



Avaya Workforce Engagement

System Administration Guide

May 20, 2026
Revision 1.68

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya LLC. All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

C o n t e n t s

About this guide	9
Introducing system administration	19
System Administration overview	20
System Administration workflow	21
Additional Suite Administration Documentation	21
License and product activation for a system license	23
About licensing and product activation	24
Licensing workflow for a system license	24
Licensing terms	26
License activation	27
Get the license registration key (RK)	27
Activate a license	27
Activate the products	30
Update product licenses	33
License expiration and renewal	34
General system settings	35
Configure General system settings	36
System-wide configuration options	36
Language selection	55
Set up Mapbox	57
Enable Google Open ID	58
Media Types	60
Feature Settings	61
Configure sign out and authentication method	61
Configure mobile authentication	62
Configure application startup messages	64
Configure the limits for user sessions	67
Change Request Management feature settings	67
Enable or disable voice signature capture	68
Voice Signature configuration reference	70
Configure Common Cloud Services	70
Workflow: Configure Common Cloud Services Secrets	71
Configure the Operations Manager URL	74
Enable Insights in WFO	75

Configure Net Staffing	76
Configure Campaigns	77
Configure SCIM User Provisioning	77
Limiting the number of concurrent WFO sessions	80
Set a limit for concurrent WFO sessions	80
Modify the limit on concurrent WFO sessions	81
Remove the limit on concurrent WFO sessions	83
Integration and adapters	84
About the Integration Service	85
Integration Server architecture	85
Integration Server features	86
Integration Server packages	87
Adapters and interfaces	87
Navigating to the Integration Servers	88
Integration packages and server monitoring	90
Typical integration packages	91
Integration server package components	93
Extenders and converters	93
Timers	94
Data source configuration	95
About data sources	96
Creating and editing data sources	97
Creating data sources	98
Creating Application data sources	99
Configure a Microsoft Teams child data source	116
Creating Dialer data sources	118
Creating LAN (Screen) data sources	127
Creating Operations data sources	129
Creating OutSourcer data sources	130
Creating Phone data sources	132
Create a Radio data source	145
Creating Trader data sources	149
Editing a data source	153
Creating a parent-child relationship between data sources	153
Viewing the data sources summary	154
Importing data source configuration	155
Exporting data source configurations	156
Deleting a data source	157
Working with data source groups	158
Creating or editing a data source group	158

Uploading data source groups	161
Skills mapping	162
Creating or editing skills mapping	162
Activity mapping	163
Creating and editing activity mapping	163
Map employees to data sources	165
Selecting employees for employee mapping	165
Creating and editing employee mappings	166
Creating and editing reason codes	168
Create and edit reason codes	168
Uploading reason codes from a file	169
Working with operations in Workforce Management	171
Transformation Operations	171
WIT Configuration	175
Cache features	178
Configuring and viewing the system cache	179
Using the cache for programming diagnostics	179
Viewing server cluster configuration	180
Troubleshooting server cluster configuration	180
Using the cache from an external URL	181
Cleaning the cache	182
System administration for suite servers	183
Overview of suite server system administration tasks	184
Changing System Accounts	185
Change passwords for existing MSA or DMSA accounts	186
Change the Password of the Existing MSA or DMSA Account	186
Change the MSA of DMSA Account to a Different Windows Account	189
Important Account Details	190
Use Multiple MSAs	190
DMSA/MSA Account Change Workflow	191
Change the DMSA/MSA Accounts (step-by-step)	192
Change the SQL Services account	200
Change the SQL Services account password	200
Change the Enterprise Manager Agent application user accounts	201
Create, edit, or delete an EMA user account	202
RM and EMA User Management create/edit account screen reference	203
Change the Import Manager application user accounts	204
Change the System Account (DB Realm)	205
Change the System Account (Windows Authentication)	206
Change the WebLogic Administrator Account Password (DB Realm)	207

Workflow: Change the WebLogic 12.x Administrator Account (Windows Authentication)	208
Back up the WebLogic 12.x Files Needed to Restore the Existing Account or Password	208
Change the WebLogic 12.x Administrator Account to a Different User Account (Windows Authentication)	209
Change the WebLogic 12.x Admin Account Password (Windows Authentication)	216
Restore the Existing WebLogic 12.x Admin Account User Name or Password	220
Workflow: Change the WebLogic 14.x Administrator Account (Windows Authentication)	221
Back up the WebLogic 14.x Files Needed to Restore the Existing Account or Password	221
Change the WebLogic 14.x Administrator Account to a Different User Account (Windows Authentication)	222
Change the WebLogic 14.x Admin Account Password (Windows Authentication)	227
Restore the Existing WebLogic 14.x Admin Account User Name or Password	229
Change the SSObind account	231
Replace the Keytab file	231
Create TAS user group and TAS user accounts	232
Changing server computer names, domains, and workgroups	233
Overview	234
Understand the workflow for changing computer names, domains, and workgroups	235
Computer name and domain change workflow	235
Step 1: Establish trust between the current domain and the target domain	237
Step 2: Change the computer name, domain, or workgroup of an individual server	239
Changing multiple servers	239
Step 2 procedures	240
Verify the server meets the requirements	241
Stop and disable the Integration Server Service	241
Perform the prerequisite steps for clustered framework applications servers	242
Back up the SSRS Encryption Key	245
Change the Management Services Account and Database Management Account for the server	246
Change the Windows computer name/domain/workgroup membership on the server	247
Run the SQL Server Change Computer Name application to rename an SQL Server	248
Ensure that SSRS can access the Reporting Services database	250
Restore the SSRS Encryption Key	251
Generate and install new TLS Server Certificates	252
Ensure the Recorder Archive Service log on account can run in the new domain or new workgroup	252
Run the ChangeComputerName.cmd script	253
Change the server name on the server Settings screen	255
Change the SQL server name on server role Settings screens	255
Update DPA with new Recorder server name	257

Review the alarms and restart services	257
Remove the old Integration Server name from BPMAINDB	259
Restart the IP Analyzer	259
Change the configuration of any affected desktop applications	260
Perform the steps to complete the changes for clustered Framework Application servers	262
Restart Recorder services from Recorder Manager	264
Review alarms and restart services	264
Determine what to do next	265
Step 3: Break the trust between the original domain and the new domain	267
Before performing the step 3 procedures	267
Step 3 procedures	267
Configure the required accounts in the new Windows domain	268
Create the five required Windows accounts	268
Complete the changes for the new MSA and DMSA accounts	269
Complete the SSO configuration for servers in the new domain	275
Create the Windows accounts required by WebLogic and SSO	275
Run the Weblogic Configuration Tool for SSO configuration	275
Change user names to reflect the new domain	276
Break the trust between the original domain and the new domain	277
Changing ports	278
Change the Tomcat Server Ports	279
Change WebLogic port to a port other than 7001	283
Adjust the Framework Applications Server Settings	283
Change the WebLogic server listening port	284
Adjust system properties	286
Verify successful change to WebLogic ports	286
Disabling TCP/IP and IP monitoring services	287
Disable TCP/IP and IP Monitoring services workflow	288
Disable Windows TCP/IP services	288
Disable the Monitoring services	290
Restart application servers after disabling services	291
Confirm the TCP/IP service is disabled	291
Sanity tests after disabling services	292
Rollback the configuration changes workflow	293
Enable the TCP/IP service	293
Enable IP monitoring	294
Restart application servers after rolling back configuration changes	294
Confirm the TCP/IP service is enabled	295
Sanity tests after rolling back configuration changes	295

Full-text search	296
Full-text search overview	297
Workflow: Full-text search deployment	298
Enable full-text search	298
Activate the Full-Text Search license	299
Configure and manage stopwords and stoplists for full-text search	301

About this guide

This guide provides instructions for the initial configuration of servers and system accounts. It describes how to configure system settings, adapters, data sources, and cache features. It also provides information on managing system log files for maintenance and troubleshooting.

Intended audience

This guide is designed for:

- Employees and Business Partner professional services staff responsible for planning and setting up systems.
- Customers' IT staff responsible for system maintenance.

Document revision history

Revision	Description of changes
1.68	In <i>Enable Insights in WFO</i> : • Updated the description and changed the Data Insights Bot URL. • Changed Workforce Engagement (WFE) references to Workforce Optimization (WFO), and removed the availability limitation.
1.67	In <i>Creating Application Data Sources</i> : • Added NICE CXone Kafka Authentication section. • Added Global Audio URL to Cisco WebEx Contact Center for real-time audio capture. • Added Post-call Cloud Settings section.
1.66	In Feature Settings, added <i>Configure SCIM User Provisioning</i> .
1.65	In Feature Settings, added <i>Enable Insights in WFE</i> .

Revision	Description of changes
1.64	In <i>Create an Application Data Sources</i>: - For Amazon Connect, renamed the section Amazon Connect Settings to Amazon Kinesis Stream Settings. - For Amazon Connect, added the Amazon Connect Multi-Party Call Mode check box. - For Genesys Cloud, added the Amazon Kinesis Stream Settings section for configuring Kinesis Data Stream and EventBridge.
1.63	Updated the workflow topics for changing the WebLogic administrator account and changing the account password to support WebLogic 12.x and WebLogic 14.x: - See Workflow: Change the WebLogic 12.x Administrator Account (Windows Authentication) - See Workflow: Change the WebLogic 14.x Administrator Account (Windows Authentication)
1.62	- In <i>Configure Common Cloud Services Secrets settings</i>, added key rotation settings for Identity V1 and V2. - In <i>Creating Application Data Sources</i>, added: Specific Switch Type for a Generic Application Data Source. Ring Central to the step related to configuring a Proxy service.
1.61	Updated the following topics to include Application data sources: - Exporting data source configurations - Importing data source configurations
1.60	Updated <i>Register WFO client on the authorization server</i> and <i>Configure Common Cloud Services Secrets settings</i> for Verint Identity V2.
1.59	Changed the heading from <i>Change the Management Service Account and Database Management Account: Change the Password of the Existing MSA or DMSA Account</i>.
1.58	In <i>Creating Application data sources</i>, added Cisco Webex Calling. In <i>Creating Phone data sources</i>, added a note on reassigning data sources. In <i>Creating Application data sources</i>, for Generic Application, in the Associated Installations section, you can select a Recorder Integration Service for real-time media capture.
1.57	In <i>Creating Application data sources</i> for Amazon Connect, Zoom Meetings, and Zoom Phone systems, added a new Proxy Settings section for configuring a proxy host.

Revision	Description of changes
1.56	For the 1112 release: In <i>General system settings > Feature Settings > Change Request Management feature settings</i> , updated the settings related to viewing request validation alerts.
1.55	In License and product activation for a system license chapter, added a new topic about license expiration and renewal.
1.54	In <i>Change Request Management feature settings</i> , added a description of the new feature setting, Maximum date range (in months) when filtering employee requests .
1.53	In <i>Creating application data sources</i> : • Under Advanced Settings, added the SIPREC.StationCountryCode key. • Added Microsoft Dynamics Authentication Settings. • Added Google UJET settings
1.52	In <i>Change the Tomcat Server Ports</i> , updated the Tomcat Shutdown port.
1.51	In <i>Creating Application data sources</i> , added the settings for Ring Central.
1.50	Added new data source options for redaction and morphing to the following topics: • Creating Application data sources • Creating Dialer data sources • Creating Phone data sources • Create a Radio data source • Creating Trader data sources
1.49	In <i>Creating application data sources</i> : • Updated the Zoom Authentication settings for Zoom Phone and Zoom Contact Center. • Under Advanced Settings, added steps for the Twilio WEBSOCKET_TARGET_URL key.
1.48	In <i>Change the Password of the Existing MSA or DMSA account</i> , added a note informing users to refer to the SQL Server Installation and Upgrade Guide if DB permissions were assigned manually.
1.47	Minor editorial revisions.
1.46	In <i>Creating Application data sources</i> , added settings for ZoomPhone.

Revision	Description of changes
1.45	In the <i>General system settings</i> chapter, under <i>Feature Settings</i> and <i>Change Request Management feature settings</i> , under the subtopic, Available options to address issues , added a description of the Maximum requests returned by the V2 Get My Requests API setting.
1.44	Added the topic "Datasource groups upload summary."
1.43	Minor changes.
1.42	In the topic "Configure application startup messages," in the "Display Message" settings, changed the value "Once" to "Every Day."
1.41	<i>Enable or disable Agent Voice Signature Capture</i> : Added a new section describing Agent Voice Signature Capture.
1.40	The description of the "Minimum Session Length" option, which is available for several data source types, is modified.
1.39	In the "Creating application data sources" topic, added descriptions for the "Snowflake Database Authentication" settings. These settings are available for the Conversational data source subtype.
1.38	Minor changes.
1.37	Minor changes.
1.36	Minor changes.
1.35	- Deleted RSA KMS content in the "Changing multiple servers" topic. - In the "Creating Application data sources" topic, a note is added about the External Recorder data source sub-type. - In the "Creating Dialer data sources" topic, it now states that you can associate an Avaya Proactive Outreach Manager (POM) dialer data source to an Avaya OneCloud application data source.
1.34	In the "System Wide Configuration" topic, in the "Reports" section, changed the description of the "Request Timeout (minutes)" setting.
1.33	Added documentation for the Twilio data source settings to the "Creating an Application data source" topic.
1.32	Added documentation for the "Maximum Allowed Extensions" setting in the "Creating Dialer data sources" and "Creating Phone data sources" topics.
1.31	Changed documentation for the "Password Minimum Length" and the "Password Maximum Length" settings.
1.30	A topic named "Configure the Operations Manager URL" is added to the "General system settings" chapter.

Revision	Description of changes
1.29	- Added a step for configuring the "Cisco WebEx Contact Center Authentication" settings to the "Creating Application data sources" topic. - In the "Register WFO client on authorization server" topic, added API scope in the information to include in an access request. - Added the chapter "Disabling TCP/IP and IP monitoring services".
1.28	Removed duplicate content in the "Reports" section of the "System-wide configuration options" topic.
1.27	In the "Configure mobile authentication" topic, in the table of OpenID Method properties, added "Auth0" to the available Identity Provider (IdP) options.
1.26	Updates for 15.2 2021R1: - Added a note to the topic "Creating application data sources" stating that the Lync application datasource sub-type is no longer supported. - In the "Feature Settings" section, added a topic titled "Workflow: Configure Common Cloud Services." - In the "Creating application data sources" topic, added descriptions of new settings for the Amazon Connect data source sub-type. - In the "Creating application data sources" topic, added descriptions of new settings for the Five9 data source sub-type.
1.25	- In the "Licensing workflow for a system license" topic, moved note from step 1 to step 4. - In the "Licensing terms" topic, stated that a Registration Key (RK) has 36 hexadecimal digits rather than 32. - In the "Activate the products" topic, edited the note beneath step 11. - In the "Activate the products" topic, edited the note beneath step 14. - In the "Activate the products" topic, changed the instructions for "Uploading licenses for an application server cluster."
1.24	In the "Change the password of the existing MSA or DMSA account" procedure, added a new step 4 instructing users to stop and start the Watchdog and WFO_ProductionDomain_ProductionServer services.
1.23	In the "Activate a license" topic, changed the URL to the license activation web application to https://licensing.verint.com/LicenseActivator/Activate.aspx .

Revision	Description of changes
1.22	Updates for 15.2 2020R1: • In the "Creating and editing Reason Codes" topic, it is noted that Reason Codes must be uniquely named. • In the "About licensing and product activation" topic, it is noted that in a multi-tenant enabled environment, each tenant requires its own license. • In the "Upgrade or update existing License Reference Number (LRN)" topic, a reference to the "playback redaction" license is changed to the "sensitive data masking" license. The playback redaction license is now called the sensitive data masking license. • Documented the privileges that are required to configure each of the screens available from the "Feature Settings" menu. • Removed the step indicating the user needs to select a specific tenant when configuring each of the screens available from the "Feature Settings" menu. Tenant Administrators will not see a Tenant drop-down menu on these screens. • In the <i>System-wide configuration options</i> topic, deleted the Request Management section with the two settings. The Enable Time Off Waitlists setting was moved to the Settings page (located on the Organization Management menu, under Request Management). The Allow Creation of Blackout Days for Organization setting is no longer valid. Now, Blackout days are another type of Special days named Time Off Not Allowed. For more information about these changes, see the Request Management Guide. • Added description of the new "Default Employee for Interactions" setting available on the Phone, LAN (Screen), Dialer, and Application data sources. • Added description of the Export button for the Audit Viewer. You can now export an audit trail to a CSV file. • In the "System-wide configuration options" topic, in the "Reports" section, documentation is added for the "Enable custom reports deployed by service provider user to tenant user" setting.
1.21	Added descriptions of configuration settings for the NENA i3 application data source sub-type.

Revision	Description of changes
1.20	Updates for 15.2 HFR7 714 The <i>System-wide configurations options</i> topic, Request Management section was updated with the following changes: • Shift Bidding Background Task Interval (minutes) setting was deleted because it is no longer needed. To update an auction schedules or employees list, the Update Schedules option is available on the Schedules page. (This page is located on the Request Management menu, under Schedule Auctions.) • Count Only Time Off Activities With Accrual Toward Organization Allotment setting was deleted because it is no longer needed. Two settings on the Activity Details page determine whether an activity uses a time off pool: Deduct from Daily Pool setting and Deduct from Interval Pool setting. (The Activity Details page is located on the Work Administration menu, under Activities.) • Time Off Request Types Enabled setting was renamed to Time Off Hours Request Options and moved to the Settings page. (This page is located on the Organization Management menu, under Request Management.) More information is available in the Workforce Management Request Management Guide.
1.19	It is noted in the "Change WebLogic port to a port other than 7001" topic that the procedure should be performed only by authorized services and support representatives.
1.18	Updates for 15.2 HFR7: • In the "Language selection" topic, added explanation of the language used for the login page and the language used for WFO applications • Changed instances of "Text Capture" to reflect new name "Interaction Capture" • Added topic "Upgrade or update existing LRN"
1.17	Changed the Related information reference in the "Create the Windows accounts required by WebLogic and SSO" topic.
1.16	• Added the topic "Media Types" that was previously included in the <i>WFM Administration Guide</i>. • Added the topic "Cleaning the cache."

Revision	Description of changes
1.15	- Corrected the URL for the security utility. Replaced IP address with <localhost>. - Added permanent licenses to notes about which licenses are updated. - Added topic "Get license registration key (RK)." - Updated note in "Perform the prerequisite steps for clustered framework application servers" so that users did not miss a step.
1.14	Added topic "Media Types" that was previously included in the <i>WFM Administration Guide</i> .
1.13	Updates for V15.2 HFR5: - Changes to the licensing activation process - Licensing changes related to Identity Authentication and Fraud Detection. - New Web Authentication tab under Feature Settings - User Session Limits under Feature Settings - Added DB Authentication setting for the System User account - Updated terminology for system accounts and default admin user accounts. - Reformatted the General Settings content for legibility
1.12	Removed recommendation for number of concurrent sessions and put "1000000" as the limit in the sample SQL.
1.11	Updates for V15.2 HFR4: - Added sections on limiting concurrent user sessions. - Removed mention of Interactive Intelligence, which is now owned by Genesys. - Removed procedure for configuring FIS adapter for License Usage Reports because the SaaS Usage - Report Dump adapter is no longer available.

Revision	Description of changes
1.10	Updates for V15.2 HFR3: - Added new topic "Configure usage terms and conditions." - In the <i>Change the SQL server name on server role Settings screens</i> topic, added a note to modify the SQL instance name key value in servers that have disabled server roles. - Specified "RSA KMS" server where applicable. - Information pertaining to system audit and logging features was removed from this guide and published in the <i>System Monitoring, Logs, and Alarms Guide</i>. - Updated with new document template.
1.09	- Updated N+N Double Consolidation setting to Keep duplicate recording for the data source configuration settings. - Restored the topic, <i>Configure FIS adapter for the License Usage Report</i>. This provides the manual configuration procedure, if the FIS adapter has <i>not</i> already been enabled. - Removed master-slave terminology in General Settings.
1.08	- Removed fields from the System Settings page that were removed from the UI. - Removed the topic, "Configure FIS adapter for the License Usage Report." This configuration is now automated. - All authentication content has been moved from this document to the <i>Authentication Configuration Guide</i>. - Added content for new field on the System Settings page, Enable Account Locking for Superuser. - Added OpenID mobile authentication content in Features Settings.
1.07	Clarified the download location of the <i>FTS scripts</i> in VerintConnect.
1.06	Revised the "Keep Maximum Number of Unmanaged Instances per report" description.
1.05	- Following DMSA password update, added a step to assign DB permissions automatically using the <i>Database Permissions Configuration Tool</i>, or manually. - Updated the folder path of the <i>SSOKeyTabFile</i>.

Revision	Description of changes
1.04	Updates for HFR1: • Chapter 9 - Change System Accounts: Added new section: Create TAS user group and TAS user accounts • New chapter: Chapter 13 - Text Analytics Services: Virtual IP configuration for LB
1.02	Revised guidance on segments marked for session auditing, now available to view in under five minutes.
1.01	Edited the <i>Full Text Search</i> section.
1.00	The following changes are new for this release: • Video Recording Mode configuration settings are described for both the Phone and Dialer Data Sources. • A new Phone data source configuration setting named "Enable N + N Double Consolidation" is documented.

Introducing system administration

This section provides an overview of the system administration tasks performed using the suite's System Management module.

Topics

System Administration overview	20
--------------------------------------	----

System Administration overview

You can perform system administration tasks that affect the entire suite, using the System Management module. Applications that can be administered from this module include:

- Workforce Management
- Interactions and Analytics
- Recorder
- Scorecards
- eLearning
- Coaching
- Customer Feedback

During the initial phase following installation, configuration, and license and product activation, there are a number of initial system administrative tasks that may be required to set up these applications to support end-user functionality.

Some tasks, such as updating licenses and general settings, continue to be performed from this module as our customers upgrade or add features to their system.



The System Management module is a core component used for all of the system. In addition to system administration tasks specific to the Framework Applications, this module also is used to complete configuration tasks, administration tasks, and tasks common to the entire suite, such as configuring the log files and the audit trail functionality.

Related information

Workforce Optimization Technical Overview

System Administration workflow

Topic	Information
License and product activation for a system license (page 23)	1. Update license information as required.
General system settings (page 35)	2. Configure, as required, system settings for all Framework Applications and the Framework GUI. 3. Configure, as required, the Audit Trail.
Integration and adapters (page 84)	4. Overview of how to access the Integration server and configure adapters, which control the data sources used by Framework Applications, and the integration of the various applications and systems within the system. All integration and adapter configuration must be complete before one can create and configure Workforce Management and Scorecards data sources. Note: Much of the adapter configuration is completed 'under the covers' during the initial installation and configuration process. Detailed descriptions of how to configure each adapter are found in the suite of Adapter Guides included with customer DVDs.
Data source configuration (page 95)	5. Describes the following: a. Creating and editing data sources (page 97) b. Creating or editing a data source group (page 158) c. Skills mapping (page 162) d. Activity mapping (page 163) e. Creating and editing reason codes (page 168) f. Working with operations in Workforce Management (page 171)

Additional Suite Administration Documentation

Your installation disks and our external library of documentation contain all the guides required to learn how to administer and use our products.

The guides listed below are administration guides, which provide further information on administration topics in the system:

- Coaching Administration Guide
- Customer Feedback Administration Guide
- eLearning Administration Guide

- Enterprise Manager Configuration and Administration Guide
- User Management Guide
- Interactions and Analytics Administration Guide
- Recorder Configuration and Administration Guide
- Scorecards Administration Guide
- Workforce Management Administration Guide
- Workforce Management Adapter Guides [suite of guides for all adapters]

License and product activation for a system license

To use WFO, you need to activate a customer license and to then activate the product.

Topics

About licensing and product activation	24
License activation	27
Activate the products	30
License expiration and renewal	34

About licensing and product activation

Licensing for all products is unified across the system.

Licensing is centrally managed, and is designed to allow the system to monitor license usage, statistics and violations reporting.



If you operate in a multi-tenant enabled environment, each tenant can be assigned its own license. For information about licensing and product activation in a multi-tenant environment, see the *Multi-tenant SaaS Service Provider Reference Guide* (Tenant license management).

These are the outcomes of successful license and product activation:

- **Configuration:** The installer sets up the customer's hierarchy and configures the server roles associated with the products for which the customer purchased the license.
- **User management:** Roles and privileges related to selected products are activated, depending on the licensing.
- **User interface:** Modules and pages are visible depending on the products that were activated.

Related topics

[Licensing workflow for a system license \(page 24\)](#)

[Licensing terms \(page 26\)](#)

[Activate the products \(page 30\)](#)

[Update product licenses \(page 33\)](#)

Related information

Licenses and License Mappings reference

Hierarchy setup and server role configuration (*Enterprise Manager Configuration and Administration Guide*)

Roles and privileges (*User Management Guide*)

Licensing workflow for a system license



If you operate in a multi-tenant enabled environment, each tenant can be assigned its own license. For information about licensing and product activation in a multi-tenant environment, see the *Multi-tenant SaaS Service Provider Reference Guide* (Tenant license management).

1. New (unsigned) license creation during Fulfillment:

- a. The licensing process begins with an initial unsigned license file that is generated after a customer order is placed. The license is then stored with a unique license reference number (LRN). In a multi-tenant SaaS environment, this license is obtained by the Service Provider

Administrator.

- b. For each order of the current release, customers receive a license letter that includes the LRN for that order through e-mail.
2. **Installation:** The customer's solution is installed. For details on installation, see the *Installation Guide*.

i During installation, the URL address is established, and a default administrator ID and password are created. You use this information to sign in to WFO during product activation.

If you do not know the sign in ID and password, request these details from your application consultant.

3. **License registration key generation:** During installation, a license registration key (RK) is generated. The RK is available on the license management page.
4. **License activation:** Upon completion of installation, the installer activates the license using the license web application. Both the unique license reference number (LRN) for the order and the registration key (RK) are required for the activation. This creates an active (signed) license file. If there were multiple orders and thus multiple LRNs, each LRN needs to be activated separately.

i During the license activation process, software items associated with a new LRN are merged with the latest activated license already in the customer's system. Permanent and term licenses that contain an explicit expiration date are merged. Pilot and temporary licenses are not merged.

If there are multiple LRNs related to multiple orders, each LRN must be activated separately to achieve the final aggregated license file.

5. **Product activation:** To activate products, the installer signs in, and in the **License** administration page, uploads the newly activated license document and restarts the server.

Related topics

[Activate a license \(page 27\)](#)

[Licensing terms \(page 26\)](#)

[Activate the products \(page 30\)](#)

Licensing terms

Term	Description
License (license file)	An XML-based file that contains the list of applications and quantities that a customer is licensed to use for a specific system. There are two versions of this file: • Unsigned License: a license file to which a registration key has not yet been applied, and which thus is not a valid license for use in an installed system. This file is created during Fulfillment. • Activated (or Signed) License: a license file that contains its systems registration key in encrypted format, and is secured so that it is linked to the specific system and cannot be tampered with or used in another system. Licenses are activated following installation.
License Generation	The process of generating an unsigned license using the license generator application. This process occurs during Fulfillment.  The license generator is also used to update existing licenses.
License Reference Number (LRN)	During the Fulfillment process, a unique number is generated for each license.
Registration Key (RK)	A unique identifier of a specific installed Enterprise system, generated during the installation process. This key is linked to the installed software and is generated during the system installation process. This key has 36 hexadecimal digits in the form of xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx used to identify a specific system that was installed, and linked, to system software or hardware
License Activation	The process of converting an unsigned license to a signed (activated) license using the license activation portal. This process occurs following installation.
Product Activation	The process of uploading the activated license to the installed system in order to activate the products for which the customer purchased the license. This process occurs after license activation, using the License administration screen within the suite portal.

License activation

Following installation of a solution, you need to activate the license using the license activation application, which is a web-based application available for access twenty-four hours, 7 days a week.

To activate a license you need:

- A valid License Reference Number (LRN).
- The license Registration Key (RK).

Related topics

[Get the license registration key \(RK\) \(page 27\)](#)

[Activate a license \(page 27\)](#)

Get the license registration key (RK)

To activate the license, you need the license registration key (RK) that is generated during system installation.

Procedure

1. In a browser window, enter the URL of the system.
 - For a system with database authorization, use the following URL format:
http://<server name>/wfo/
 - For a system with Security Assertion Markup Language (SAML), use the following URL format:
http://<server name>/wfo/control/adminsignin
2. From the sign-in page, enter the administrator user name and password. (On a new system, the installation process defined the default administrator credentials.)
3. Select **Sign in**.
4. Go to **System Management**. Under **Licensing Management**, select **System Licensing**.
The **License Data** page shows the **Registration Key**, **License Registration Number (LRN)**, **Customer Name**, and **Customer ID**.
5. Make note of the registration number (LRN) and registration key (RK).

Related topics

[Activate a license \(page 27\)](#)

Activate a license

1. Go to the license activation web application at this URL:
<https://licensing.verint.com/LicenseActivator/Activate.aspx>
The **License Activation** page opens.

Please fill in registration key (rk) details:

License Reference Number (LRN)

License Agreement

You are about to activate a license key for use with a Verint Systems, Inc. software product. All such use is subject to the terms and conditions of the license agreement executed by the end user, or if no agreement has been executed, by the license terms and conditions included with the product. Any unauthorized use of a license key (including, without limitation, use of a key licensed by another party or multiple use of the same key) is strictly prohibited, is subject to both criminal and civil penalties, and will be prosecuted to the fullest extent permitted under applicable law. Additionally, if the installation and activation of the product is not done by Verint Systems, Inc. or a certified partner of Verint, you may incur additional fees and/or any warranty or support terms may be void.

License Reference Number (LRN)

Enter the 36-character Registration Key (RK) including hyphens

For upgrade from v15.1 enter the RK of the 15.1 system being upgraded if different from target system RK, otherwise leave blank.

- In the **License Reference Number (LRN)** text box, type the LRN.
- Select **Go**.
- To accept the license agreement, click **Accept**.
- In the **Enter the 36-digit Registration Key (RK) including hyphens** box, type the unique RK for the system.
- For side-by-side upgrades from 15.1 to 15.2 where the source system has a different RK than the target, enter the RK for the source system.
- Select **OK**.

The next page displays the license information for this LRN.



If there was a previously activated LRN, the activation site displays its LRN number, and the merged license information for both LRNs.

- Verify the information on the page and select **OK**.
- On the next page, enter your contact details.

License Reference Number (LRN)

End User Contact Name

End User Telephone Number

End User Contact Email

- Select **OK**.

The activation is complete. The page refreshes again, showing the XML file that you need to activate your licensed products.

```
<?xml version="1.0" encoding="UTF-8"?>
<BR-licenses LRN="L013F64D250FB-3516" activateDate="06/21/2013" customerSysId="N/A" expiresInDays="-1" format="2.0" product="Workforce
Optimization Suite" release="11.1.0">
  <license>SO 11112222</license>
  <item displayName="Express Reporting (Cognos)"
    name="ExpressReports">
    <max-seats>150</max-seats>
    <signature>9BMlpYHkZuKM/VdpI2564outeTVZjwCMjLa6gqo9ybtEouorEoKKUBVFCpnz2RHDMnFuc7h&#xd;
    aPUQWjHnBL3aD4jcxssSKYUwrgqbJJz1LZ5XVSHKPO2ePT538Wu/f3G8b9/5uWFRq6R75dR7Sa&#xd;
    FgUvYzBaZufwKpfsPSyHVLKZhmgaNevgyby&#xd;
  </signature>
  <item displayName="Standard Reporting (Cognos)" - 93-530-3049" name="Reports">
    <max-seats>150</max-seats>
    <signature>9BMlpYHkZuKM/VdpI2564outeTVZjwCMjLa6gqo9ybtEouorEoKKUBVFCpnz2b2Q1HuKo7O&#xd;
    nR+XGwHrGvM3EpN+7BKYup3yu0ub4gIvGwJh5HvhyyfFhsuM8/SluaREsxEbYrN8FP+Cwcf&#xd;
    F3L8yVtLnVbV8lYhL4GmUHPM2aczhvgKXZ76XcChg0PPQeOaET+R6wMxw==&#xd;
  </signature>
  <item displayName="Performance Management Basic Scorecards - 93-530-3091" name="AdvisorEssential">
    <max-seats>150</max-seats>
    <signature>9BMlpYHkZuKM/VdpI2564outeTVZjwCMjLa6gqo9ybtEouorEoKKUBVFCpnz29KEvWDuk+0&#xd;
    E4I2SUSG28TtCpRTE+evvovTdeVHYHn8BjPAe1KXLSghgbof1VPDTo6Imbeo1LpduWaz&#xd;
    q0pQaoQepocp672atwDU4pLxHeBjP4VXQaJGL2RjyE4OyXn3HJawqm7aOxi7Emm2MJ&#xd;
  </signature>
</BR-licenses>
```

11. Do one of the following:
 - a. On the activation page, select **Download** and save the XML license file to your hard drive.
 - b. You do not have to download and save the file immediately. After activation, an email is sent to the address you provided. The email confirms your details and includes the file attachment for your license. Open and save the attachment to your hard drive.
12. Activate your products using the license file.

Related topics

[Activate the products \(page 30\)](#)

Activate the products

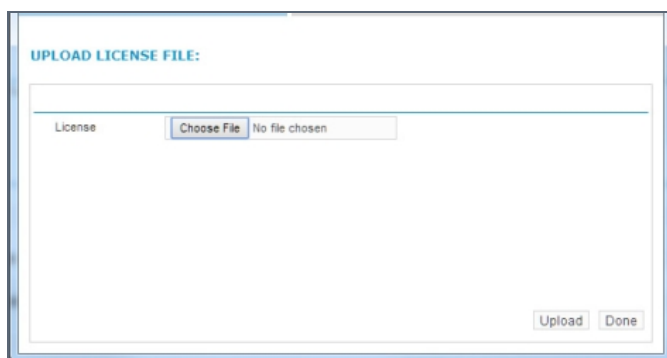
After installation, activate each licensed product.



If the new license uploaded to an old system has new or additional features, those features will not be activated until the old system is upgraded. To make the new features available on the upgraded system, you must upload the new license again.

Procedure

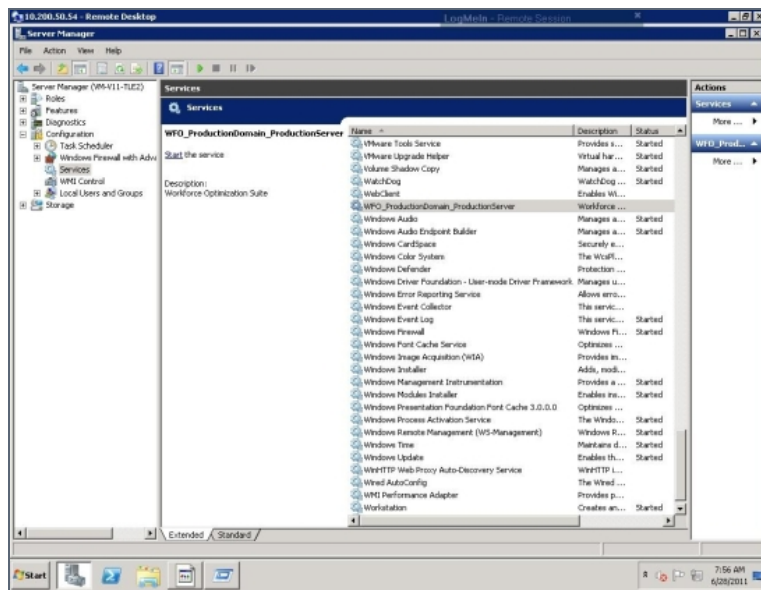
1. In a browser window, enter the URL of the system.
 - For a system with database authorization, use the following URL format:
http://<server name>/wfo
 - For a system with Security Assertion Markup Language (SAML), use the following URL format:
http://<server name>/wfo/control/adminsignin
2. From the sign-in page, enter the administrator user name and password. (On a new system, the installation process defined the default administrator credentials.)
3. Select **Sign in**.
4. Go to **System Management**. Under **Licensing Management**, select **System Licensing**.
The **License Data** page shows the **Registration Key**, **License Registration Number (LRN)**, **Customer Name**, and **Customer ID**.
5. For an existing installation that requires an updated license:
 - Verify the number of maximum units for each licensed product.
 - Review the customer information.
6. Select **Upload License**.



7. From the **Upload License File** page, select **Choose File**.
8. Select the XML activated license file that you saved to your hard drive during the license activation process.
9. Select **Upload**.
After the upload completes, a message displays on the **Upload License File** page instructing you to restart all application servers.
10. Restart the WebLogic service on the primary application server. Wait for it to be accessible from a browser running locally. The URL to access is <http://localhost/wfo/ui/signout>. This process takes

approximately 15 minutes. After accessibility is confirmed, start all the remaining application servers:

- Go to **Start > Run** and, in the **Run** page, type **services.msc**.
- In the Windows **Services** window, restart the WebLogic service. The service name is **WFO_ProductionDomain ProductionServer**.



After restarting the WebLogic service, the **License Data** page displays the list of all the product features associated with the customer license. To expand product features, select the arrow next to a feature name.

LICENSE DATA Automation						
Registration Key (R1) License Registration Number (R1) Customer Name Customer System ID CPAF401-6317-4621-801-6186432P7340 LS170701642-C-04 Automation Automation						
* Name	Max Employees	Max Normal Employees	Max Channels	Max Sites	Max Servers	
ACD Monitoring	1,000,000	1				
Ad-hoc Reporting	1,000,000					
A-Frame Name'd Employees Unit of Measure	1,000,000					
Back Office - User Tracking	1					
Back Office - Managing Productivity and/or Capacity	1					
Back Office WFM (Ad-Fax)	1,000,000					
Churnback	1,000,000					
Cost Center Indefiniteness - 10-530-8794	1,000					
Costs and Process Analytics	1,000,000					
Advanced Desktop Analysis - 10-530-8722	1,000,000					
Desktop Application Tracker for Desktop Application-Adherence	1					
Desktop Analytics and Automation - 10-530-8738	1,000					
Desktop Analytics and Automation - 10-530-8733	1,000					
Desktop Configs	1,000					
Desktop Biometric Notifications	1,000					
Enterprise Facilities Management (EFL) - 10-530-8733 or 10-530-8734 or 10-530-8738	1,000					
Express Adherence	1,000					
Express Adherence - 10-530-8826	1,000					
Desktop Application Adherence	1,000,000					
Desktop Reporting	1,000,000					
Standard Reporting	1					
Forecasting and Scheduling - 10-530-8716	1,000					
Interaction Data - Agent Manager - 10-530-8716	1,000					
Interaction Data Export Manager (monthly recorded hours) - 10-530-7716	1,000					
Interaction Data Platform - 10-530-8884	1,000,000					
Concurrent User Traces	1,000,000					

On the page, you see the following types of features displayed:

- Product features displayed in **bold** font and checked by default.
Bold features are licensed. If you do not have a license for a product feature, it does not appear on this page.
- More features displayed in *italic* font.

Features displayed in an italic font do not require a license; some are checked by default and some are not. These additional features are only visible if you have a license for the parent feature.

Product features can be arranged in a hierarchical order as follows:

- If a feature at a lower level in the hierarchy is enabled, then all the ones above it are enabled as well.
- If a feature at a higher level in the hierarchy is unavailable, then the features below it are unavailable as well.

11. To expand the product feature list for more items, click the arrows beside feature names.



An example of an extra feature is Dashboards.

12. To customize the product list and activate more features available to you, select the check box beside each available item.
13. For Identity Authentication and Fraud Detection (IAFD) customers, ensure that you have the appropriate licensing for the Voice Biometrics Library that you intend to use.
 - IAFD customers *not* using the Fusion Passive Biometrics Library: No additional product activation for the Voice Biometrics Library is required.
 - IAFD customers using the Fusion Passive Biometrics Library: Under **IAFD**, verify that the check box for **Fusion Passive Biometrics Library** is selected.



Activate the Fusion Passive Biometrics Library license only when you have not previously used Identity Authentication and Fraud Detection *and* you explicitly planned to use the Fusion Passive Biometrics Library.

14. To remove or revoke certain license items, click inside the check box next to the item you want to remove to clear the check box. After the application server is restarted, these items are no longer available for use in the system.



When you remove or revoke certain license items, you may get a message that warns you that while you can remove the item, once you stop and restart the application server, its removal may cause the system not to function as it is supposed to.

15. After you complete product activation, use Enterprise Manager to build the hierarchy required for the customer organization. You also need to configure the server roles for activated products.

Uploading licenses for an application server cluster

When uploading licenses for a hierarchy setup that includes application server clusters, you *must* do the following:

1. Sign in to one of the application servers.
2. Upload the license.
3. On all of the application servers in the cluster, do the following (the first time the license is uploaded, only one application server exists in the cluster).

- a. Stop the **Watchdog** service and the **WFO_ProductionDomain_ProductionServer** service on each server in the cluster one by one. These services must be stopped on all application servers before proceeding to step b.
- b. Start the **Watchdog** service and the **WFO_ProductionDomain_ProductionServer** service on primary server only. Wait for it to be accessible from a browser running locally. The URL to access is <http://localhost/wfo/ui/signout>. This process takes approximately 15 minutes. After accessibility is confirmed, start all the remaining ones in the cluster.

If any application servers need to be added to the cluster, add those application servers as described in the *Enterprise Manager Configuration and Administration Guide*.

Related information

Site organization, server setup, and server role configuration (*Enterprise Manager Configuration and Administration Guide*)

Verify licenses (*Identity Authentication and Fraud Detection Setup Guide*)

Update product licenses

1. Sign in to the web application.
2. Go to **System Management**. Under **Licensing Management**, select **System Licensing**.
3. Follow the directions to upload the updated license, as described under [Activate the products \(page 30\)](#).
4. When prompted, restart the **WFO_ProductionDomain_ProductionServer** service.

License expiration and renewal

A license can be Permanent (with no expiration) or with an expiration (Term license or Temporary).

The Licensing Management page shows all the available licenses that the customer has, and for non-permanent licenses the Expiration column displays the date when the license expires. If the license expires within 30 days, the expiration date shows in orange color. On the day of expiration, the license expires at 12:00 AM GMT.

Name	Expiration	Max Employees	Max Named Employees	Max Channels	Max Sites	Max Servers
ACD Monitoring	07/01/2024	1				
Ad-hoc Reporting	07/01/2024					
A-Enable Named Employees Unit of Measure	07/01/2024	1				
Automated Verification - Audio Quality Statistics - 83-630-7707	07/01/2024	1				

When the license expires, user access to all system functions, including reports and access through mobile applications, is unavailable. Access is unavailable for all users, including the first user account. However, users with System Administrator privileges can access the Licensing Management page (so that they can load a new license) and to license usage reports (to check historical license compliance).



Data collection and processing are not guaranteed when the system operates with an expired license.

Renew a License

You can upload a new license from the License Management page. Follow the instructions to upload the updated license, as described under [Activate the products \(page 29\)](#).

After the new license is loaded, users will regain the same privileges they had before expiration (subject to the new license).

Related topics

[Get the license registration key \(RK\) \(page 27\)](#)

[Activate a license \(page 27\)](#)

General system settings

You set system-wide options, such as licensed languages, password policy, and general settings for Scorecards and Workforce Management in System Management.
The options that are available depend on product licenses applied.



Many of these settings are straightforward. However, others can impact the speed and stability of the system and should be changed only by a qualified individual. Check with Technical Support before making changes.

Topics

[Configure General system settings](#) 36

[Media Types](#) 60

[Feature Settings](#) 61

[Limiting the number of concurrent WFO sessions](#) 80

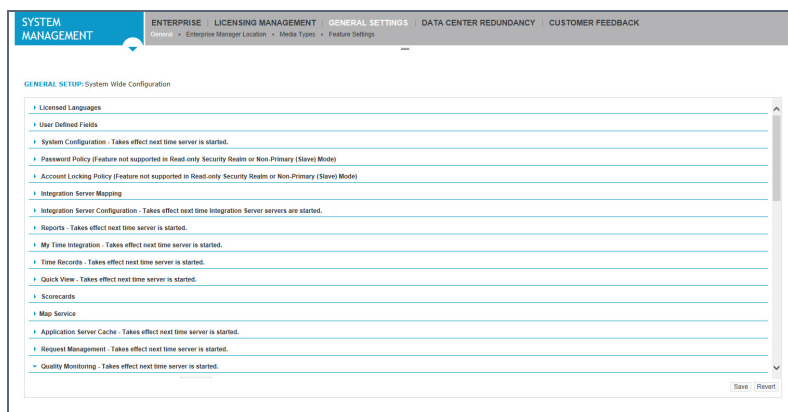
Configure General system settings

You set system-wide options, such as licensed languages, password policy, and general settings for Scorecards and Workforce Management in System Management.

The options that are available depend on product licenses applied.

Procedure

1. Go to **System Management** Under **General Settings**, select **General**.



2. Scroll down the page to the area to configure.
3. Expand the section as needed to view the available options.

Related topics

[System-wide configuration options \(page 36\)](#)

System-wide configuration options

System-wide options, such as licensed languages, password policy, and general settings for Scorecards and Workforce Management affect all components within the system.

The options that are available depend on product licenses applied.

Licensed languages

Shows the list of languages for which your product is licensed. Any language selected is available for use. The actual language used depends on the languages supported by the browser.

User Defined Fields

To include information unique to your environment, you can define up to 10 custom fields. You do not have to define 10, but you must define the fields consecutively. These fields are displayed in the employee profiles in **User Management**, **My Profile** modules and in Forecasting and Scheduling.



If your company has the Organization Scoped UDF feature activated, set up user-defined fields on the **User Defined Fields** page in **Organization Management**.

System configuration

 The web server must be rebooted before changes to these parameters take place.

Parameter	Description
Application Context Path	The context path that the current application is using. The application uses this path to embed links within a URL to allow a user to select the link and sign back in. This field is automatically populated. If you are using a firewall or load balancer, verify that this setting is correct.
Sign-in Screen Message	Optional: Any message entered here appears when users sign in to the system.
Return Server Hostname instead of IP to Client	When selected, the system returns a host name instead of an IP address to Forecasting and Scheduling for load balancing. This flexibility has been added for use with the Single Sign-On (SSO) feature.
JavaScript Load Error Detection	Enables a diagnostic tool to run to detect JavaScript loading errors (typically caused by network congestion). Only turn on this setting when requested by Technical Support.
Is System Configured to Support SSO (Trusted Login)	The Single Sign-On (SSO) feature enables user authentication using Windows sign-in credentials. To use SSO, a user must have a system user account with the same user name as the Windows user name.  If you are enabling Google OpenID Settings, be sure that this check box is selected. This setting ensures the Forecasting and Scheduling feature functions properly. When this setting is selected, the sign-in page has a Trusted Login check box. When the Trusted Login box is selected, the user name and password fields are not available. When users select Sign In, they are authenticated automatically using Windows credentials. If a user clears Trusted Login, the user name and password fields are enabled. The user can then enter any valid user name and password to sign in to the application.
Is in Non-Primary Mode	Primary Mode is the default for editing user information, such as user name, password, and account status, on the Users page and the My Profile section. In non-primary mode, another server, which is now the primary server, maintains user information. The user information is synchronized to the non-primary server. When non-primary mode is enabled, user information, employee names, email addresses, end dates, and switch IDs cannot be edited. In addition, Import, Create, Terminate, and Delete buttons, and the [Register] and [Reset Password] buttons on the sign-in page are also unavailable.

Parameter	Description
Is External Authentication Token Supported	Specifies whether external tokens are supported.
External Token Authentication Server URL	Specifies the URL of the external authentication server used to authenticate an external token.

Password policy

Password policies include settings to protect user accounts and dictate what is permitted when users create passwords. These settings apply also to the System Account.

 This feature is supported for DBRealm only.

Setting	Description
Activate Password Policy	If your security realm is modifiable, such as DBRealm, enabling this setting enforces the password policy as customized using the remaining parameters in this section. Default: Not enabled
Validate Policy On Login	When enabled, the active password policy is enforced the first time that users sign in after the Activate Password Policy is enabled. When not enabled, users who have passwords that do not adhere to the active password policy can continue to use the invalid password until it is changed. Default: Not enabled
Password Minimum Length	The minimum number of characters required for a user password. Accepted values are from 8 to 30 characters. The default is 8 characters.
Password Maximum Length	The maximum number of characters allowed for a user password. Accepted values are from 8 to 40 characters. The default is 30 characters.
Password Maximum Age (days)	The number of days that a user password is valid. After the specified number of days, the password expires and the user is prompted to reset it. The expiration count resets each time a user changes the password. A value of zero keeps passwords alive forever. Accepted values are 0–180 days. Default: 30 days
Password History (number)	The number of previous passwords stored in the system for a user account. When a user tries to reset the password, the user is forced not to use any of the stored passwords. A value of zero for this field disables the password history requirement. Accepted values are 0–30. Default: 5

Setting	Description
Password Pattern	The format to which all user passwords must conform. The options available include No Pattern, Complex Pattern, and Custom Pattern. When you specify any of the three Password Pattern options, all other policy rules that were specified, such as Password Minimum Length and Password Maximum Length, also apply to the passwords. Regardless of the password pattern chosen, a user password cannot include the user's username or birth date. No Pattern - Select this option to turn off password pattern validation. This option is the default selection. The format of the password is at the discretion of the user. Users can create passwords containing any combination of uppercase English characters, lower case English characters, numbers, or special characters (~!@#\$%^&* _-+=` \(){}[];:'"<>.,?/). The password can also be made of all uppercase or lowercase, numerical or even special characters. Complex Pattern - Select this option to require passwords to include any three of the four following items: • One uppercase English character • One lowercase English character • One special character (~!@#\$%^&* _-+=` \(){}[];:'"<>.,?/) • One number For example, one user can create a password that includes one uppercase English character, one special character, and one number. Another user can create a password that includes one uppercase English character, one lowercase English character, and one number. Both passwords are valid because each password contains three of the four items. If a user creates a password that does not include three of the four items, a message displays to the user indicating that the password must contain three of the four items. Custom Pattern - Select this option to require passwords to include the items you select from the Custom Pattern list. The selectable items in the Custom Pattern list include: • One uppercase English character • One lowercase English character • One special character (~!@#\$%^&* _-+=` \(){}[];:'"<>.,?/) • One number For example, if you select one uppercase English character and one number, all passwords must include those two items. If a user creates a password that does not include the specified items, a message displays to the user indicating that the password must contain the specified items.

Account locking policy

Administrators can define settings for locking user accounts after authentication fails.



This feature is supported for DBRealm only.

Setting	Description
Activate Account Locking Policy	When enabled, a user account status can be automatically switched to locked based on the other settings listed in this section. If a user account is locked, clearing this setting does not necessarily unlock the account. The User Management policy also affects the account. Users with locked accounts cannot access the system unless both this policy and the User Management policy are unlocked. Default: Not enabled
Enable Account Locking for System Account	When enabled, the Account Locking Policy is applied to the System account when the policy is activated. If the Account Locking Policy is activated, but this option is not selected, the lockout threshold, inactivity, or other locking parameters do not affect the System account. If the Account Locking Policy is activated and the Enable Account Locking for System Account option is selected, the Lockout Threshold also applies to the System account. If the System account is locked because of multiple failed sign-in attempts, it is unlocked automatically after the Lockout Duration period has elapsed. The default Lockout Threshold is 3; the default Lockout Duration is 30 minutes. Default: Not enabled
Lockout Threshold	This parameter only applies to failed sign-in attempts. The number supplied specifies the number of consecutive failed attempts can occur before a user account is locked. The counter resets when the sign-in is successful. Once the account is locked, a system administrator can unlock it or it is automatically unlocked after the time specified by the Lockout Duration (minutes) parameter. A value of zero prevents locking of accounts from failed password attempts and gives users infinite chances to enter a password. Accepted: 0–30 Default: 3
Lockout Duration (minutes)	This parameter only applies once the user account has been locked. The number supplied specifies the number of minutes a locked-out account (because of multiple failed sign-in attempts) remains locked before being automatically unlocked. A value of zero prevents automatic unlocking of locked accounts and requires an administrator to unlock the user account. Accepted: 0–30 Default: 30

Setting	Description
Lockout Inactive User Period (days)	Specifies the number of days of user inactivity allowed to pass before a user account is automatically locked. After the inactive user account is locked, it cannot be automatically unlocked. Only an administrator must unlock it. A value of zero prevents automatic locking of inactive user accounts. Accepted: 0-180 Default: 60

System proxy settings (OpenID)

If the IDP communication server is not on the premises, a proxy server is needed to control access for token validation.



A system restart is required for these settings to take effect.

Setting	Description
Host Name	Host name or IP address of proxy server. Alphanumeric characters only.
Port Number	5-digit port number of proxy host.

Integration Server mapping

The following settings control the display of unmapped activities and reason codes.

Setting	Description
Show Unmapped Activities for Time Collection Mapping	Display activities and reason codes that are not mapped to one another.
Show Mapped Data Source Group for Queue Mapping	Displays the data source groups that are mapped to other queues, when mapping a queue to data source groups.

Integration Server configuration

The following settings affect the Integration Server cache. The Integration Server must be rebooted before changes to these parameters take place.

Setting	Description
Cache Refresh Sleep Time	Rate at which the cache is refreshed. A low value means that the cache is in sync frequently but also consumes CPU cycles. A high value loads the system to a lesser extent with a proportional risk of de-synchronization. Default: 300,000 milliseconds.
Cache Retry Count	When the system determines that the cache must be reloaded, it waits to see if the database is still being changed. It does not reload the cache until the changes have stopped. This parameter sets the number of times it checks for the system to stabilize before it gives up and reloads the cache.
Cache Retry Interval	The maximum amount of time to wait before checking to see if the cache needs to be refreshed. The system actually checks for cache changes more frequently but slows down over time until it checks at the rate specified by this parameter.

Reports

In this area, set the parameters for the SSRS server. The application server must be rebooted before changes to these parameters take place.

Setting	Description
Enable Report Trimmer	When selected, the Report Trimmer job is scheduled to run. When cleared, the report does not run, no matter what other Report Trimmer settings are. Default: Not enabled

Setting	Description
Report Trimmer Frequency (hours)	The frequency at which the Workforce Management application requests the Report Trimmer job to remove expired or excessive report instances from the system. The value 0 means that Report Trimmer does not run, even if the parameter Enable Report Trimmer has been checked. The default value for this parameter is 24. Changes to this parameter take effect the next time the application server is rebooted.  If your system has Dashboards that include a report, each time a user views a dashboard, a report instance is created for the included report. Because this process can adversely impact performance, be careful not to set Report Trimmer to remove instances faster than the report is usually scheduled to run.
Trim Expired Instances (older than N days)	Report Trimmer uses the value for this property to remove expired instances. The value 0 means that expired instances are not trimmed. The default value is 31. Changes to this parameter take effect the next time the application server is rebooted.
Keep Maximum Number of Unmanaged Instances per report	Report Trimmer uses this value to remove excessive unmanaged ("run now") instances for each report for each user. The value 0 means that unmanaged instances are not trimmed. Changes to this setting take effect immediately. The changes are applied for each user on each report the next time that user enters the Reports page and creates an unmanaged instance for that report. Default: 5
Keep Maximum Number of Scheduled Instances per Schedule	Report Trimmer uses the value for this property to trim excessive managed (scheduled) instances for each report schedule.
Trim Adhoc Orphan Reports	Ensures that ad hoc reports that were created by an employee who is no longer with the company are removed from the store on the SSRS server.
Enable custom reports deployed by service provider user to tenant user	To make custom reports deployed by the SPA (Service Provider Administrator) available for all tenants, select this option . When this feature is enabled, custom reports deployed by the SPA appear on the Reports - Setup - Access Rights screen. The privileges to view those reports can be granted to a tenant user role. This feature is available in releases 15.2 HFR7 718 and higher.

Setting	Description
Max Data-refresh Lookback (days)	The maximum number of days in the past for which a report dump refreshes data.
Dump Chunk Size	During report dump, this parameter determines the number of employees in a single report dump chunk. You do not usually need to modify this parameter. However, if users get time-out errors during a report dump, reduce the default value of 100 to eliminate the time-out.
Dump Thread Number	The number of threads to use with Report Dump. Default: 1
Dump Max Retry	When many users are running real-time reports at the same time (which triggers a report dump), database collisions sometimes occur. This setting is the number of retries that can be attempted if report generation failed. Usually, you do not need to change this value. Default: 10
Request Timeout (minutes)	How long the system waits before timing out a report request. The default setting is 30. When running reports from the WFO application, reports containing large data sets can time out. In this case, ask your system administrator to increase the setting of this parameter. Some experimentation with this setting can be required to determine the proper setting for a particular report. If you change this setting to a value greater than 30, you must also change the report time out setting on the SSRS report server. The default report time out setting for the SSRS server is 1800 seconds/30 minutes. Change the setting on the SSRS server to match the value for this setting to prevent the SSRS server from timing out.
Status Polling Frequency (seconds)	The frequency at which the current report data is requested.
Use Live Data For Adherence Reports	Reports are typically run against data that is prepared at regular intervals, typically once a day. However, if this option is checked, adherence reports also process data that has been entered in the system since then. These reports are referred to as real-time reports.

My Time integration

Enables a special Client-Side integration with Kana.

Only change these settings at the request of Technical Support.

Time records

These settings affect the behavior of the **Tracking** module. The web server must be rebooted before changes to these parameters take place.

Setting	Description
Automatically Close If Last Event Is Longer Than (minutes)	The duration in minutes of the last event in a time record before Workforce Management automatically closes it.
Automatically Merge Time Records	Workforce Management merges adjacent time records.
Automatically Merge Time Records If The Time Interval Between Them Is Less Than (minutes)	Workforce Management merges time records that have less than this time between them.
Lookback Interval (minutes)	To improve performance, you can limit how far back in time Workforce Management looks for time records. Set the look back interval to the longest-anticipated event for this system. Default: 480 Example: There is an organization where: • The earliest shift end time is 3:00 PM EST. • The latest shift end time is 11:00 PM EST. • The longest event allowed is 300 minutes (five hours). If an agent has activity past the time limit, the Time Record Auto Close adapter is triggered when the time limit is reached. In this case, the earliest that the Time Record Auto Close adapter can run is 4:00 AM EST. The calculation is based on the length of the longest event (five hours) after the latest shift end time (11:00 PM). The length of time that the Time Record Auto Close adapter then needs to look back is: $((\text{Hours from midnight when the Time Record Auto Close adapter runs}) + (\text{time from the earliest shift end to midnight})) * 60 = (\text{four hours} + \text{nine hours})$ or $13 \text{ hours} * 60 = 780 \text{ minutes}$.
Eliminate Zero Duration Entries	When enabled, events with zero duration are deleted.

Quick view

Setting	Description
Show Organization Column	When selected, a column showing the agent organization is shown on the Quick View page.

Scorecards

The configuration settings affect the way that Scorecards processes data.

Settings	Description
%Met - Count Only People With Scores	If checked, only those employees with scores are used in the % Met calculation. In addition, the list of under-performing employees only contains employees with scores.
Convert Null Values to Zeros.	When the value of a KPI formula is calculated, some source measures can have null values. This situation typically occurs when there is no data in the source. This setting causes the calculation engine to treat null values in the source measure as zero. Example: A KPI uses the formula $bm1+bm2$, where $bm1$ is null. If the check box is selected, the calculation engine returns $bm2$. If the check box is not selected, the calculation engine returns a value of null, the equivalent of no score. When there is no score, the value associated with $bm2$ is not shown.
Audit Source Measures	Turns on or off the auditing of any insertions or updates of source measures entering Scorecards. The audit is stored in the table AUFACBASEMEASURE in the database BPWAREHOUSEDB.
Enable Period to Date Scorecards	Turns on or off score calculations before the end of the period. Users expect to be able to access Weekly and Monthly scores before the completion of the period. Period-to-Date scores are calculated by running the Scorecards – Calc Engine adapter for a period before all days in that period have been populated. Enabling this feature can adversely affect performance of the Workforce Optimization solution. KPIs that use source measures that are loaded on a weekly or monthly basis (and not daily) do not work with the period-to-date feature.
Enable Calculation Engine Performance Diagnostics	Turns on or off writing calculation engine performance diagnostics to the log table WHPERFORMANCELOG in the database BPWAREHOUSEDB.
Maximum number of days to recalculate (per each calc engine run)	The maximum number of days to recalculate (per each calculating engine run). Default: 5
Maximum recalculation time (in minutes)	The maximum recalculation time (in minutes). Default: 60

Settings	Description
Maximum numbers of periods	The maximum number of periods users can see in Scorecards KPI Trends view For the last drop-down. Also, the maximum number of periods users can see in the Scorecards History view on the Show list. Default: 30 Accepted: 4–30
Show “Filter Out Of Sync” warnings	Turns on or off the notification displayed when a Scorecards filter becomes invalid or inconsistent: "The current Scorecard filter has become inconsistent because of Administrator changes to the Configuration. Edit and save the current filter." Deleted KPIs, changes to access rights, and other changes can trigger this message. Editing and saving the filter creates a filter that is valid at its time of creation.
Enable Supervisor Rollup	Turns on or off aggregation of employee source measure and KPI values to the supervisor level during KPI calculation.
Number of Interactions to Retrieve	Maximum number of interactions to retrieve for the KPI Drill to Interactions feature. Default: 20 Maximum: 50
Custom Drill to Interactions <URL #> and Data Source <#>	Settings required to configure the KPI Drill to Interactions feature to work with an external system. A maximum of five custom URLs and associated data sources can be configured for the KPI Drill to Interactions feature. • Custom Drill to Interactions URL 01–URL 05: URL of an external system that Scorecards can access for interactions associated with a specific KPI. Used with Data Source 01–05. Each custom URL is available for selection when you create or edit a KPI in Organization Management. • Data Source 01–05: Data source for the URL in the associated Custom Drill to Interactions URL.
Intraday Interval Length (Minutes)	Number of minutes between each calculation of values for Intraday KPIs. Default: 60

Map service

After you activate your subscription to your third-party mapping service, Mapbox, you can map KPIs by location in a portlet.

To use the Performance Map feature, Map box must be enabled for users. If it is not set up correctly or not set up, an error message directs users to their administrator. For assistance with setup, contact your services representative.

Application server cache

Enables the cache parameters.

It is possible to set each cache to refresh at small intervals. However, refreshing large caches at small intervals can cause serious system performance issues.

Default: 0 (for no refresh)



Do not change these parameters unless at the direction of Technical Support.

Quality Monitoring

Set the default timeout for recording interactions.

Setting	Description
Interaction Recording Timeout (minutes)	Time out duration for recordings in minutes. A background process runs every 5 minutes and stops all recordings that have exceeded this setting. Default: 10

Activity display names for desktop monitoring

If you are licensed for Desktop Monitoring, you can set the names of the Actual and Desktop activity lines for the **Adherence** page.

Setting	Description
Primary Activity Display Name	The display name of the actual line on the Adherence page.
Secondary Activity Display Name	<i>This item is only displayed for Desktop Monitoring licenses.</i> Specifies the display name of the desktop activity line on the Adherence page.

EM alarm collection

You set parameters for the collection of alarm data from each Recorder Manager installation in the system. Alarm data can be collected from each Recorder Manager on a recurring basis, such as every 60 seconds and updates sent to the Enterprise Manager.

Setting	Description
Maximum Number of Threads	Maximum number of threads available to send Recorder Manager (RM) requests. Because each request to an RM is made on a separate thread, this value is also the maximum number of concurrent RM requests. Default: 10
Minimum Number of Threads	Minimum number of threads available to send RM requests. Default: 1
Thread Execution Delay (milliseconds)	The delay time (in milliseconds) between a thread completing the execution of a task and starting the execution of a new task. Accepted: 0, 50, 150, 200, 250, or 300. Default: 150

Setting	Description
Polling Enabled	Turns on or off the polling of each RM for its alarm status. Default: Selected (on)
Polling Interval (milliseconds)	The time, in milliseconds, between the polling of each RM server for its alarm status. Accepted: 30000, 60000, 90000, or 120000 Default: 30000
Disable Sending EMail on Failure	Turns on or off email notification of alarm failure. When selected, this setting turns notification off. Default: Not selected

EM reliable messaging

If you are licensed for Enterprise Manager, you can set parameters for sending messages to installations in the enterprise such as Recorders, Viewers, and Analyzers.

Setting	Description
Maximum Number of Threads	Maximum number of threads available to send Recorder Manager (RM) requests. Because each request to an RM is made on a separate thread, this value is also the maximum number of concurrent RM requests. Default: 10
Minimum Number of Threads	Minimum number of threads available to send RM requests. Default: 1
Thread Execution Delay (milliseconds)	The delay time (in milliseconds) between a thread completing the execution of a task and starting the execution of a new task. Accepted: 0, 50, 150, 200, 250, or 300 Default: 150
Message Data use the Cut command Interval (days)	The time to wait between checks for message data that is to be deleted (in days). Default: 1
Message Job Purge Interval (days)	The time to wait between checks for message jobs that are to be deleted (in days). Default: 1
Message Job Age (days)	The age of a message job (in days) before it can be deleted. Any <i>completed</i> message job older than the number of days is purged from the database. Default: 1
Scheduled Job Timer Interval (milliseconds)	Amount of time (in milliseconds) to wait between checks for scheduled jobs that are ready to be sent. Default: 60000
Viewer Web Server Timeout (milliseconds)	Amount of time in milliseconds that the adapter waits for a Viewer to process a message. Once this amount of time has passed, the adapter considers the message failed and reattempts on the next interval. Default: 300000.
Client Timeout (milliseconds)	Amount of time in milliseconds that the adapter waits before timing out a client request from Enterprise Manager. Use this setting to prevent unresponsiveness while the adapter is processing large configuration messages. Once a time-out occurs, the Configuration Status page displays the status of the message. Default: 15000

EM SQL Server Express job schedules

If you are licensed for Enterprise Manager and you use a SQL Server Express database, you can specify the schedules for database jobs. These settings are ignored if any other edition of SQL Server is running.

Setting	Description
Schedule for DB Cleanup Job	Default: The job is scheduled to run every day at midnight.
Schedule for DB Growth Job	Default: The job is scheduled to run at 12:30 AM on the last Sunday of every month.
Schedule for DB Optimize Statistics Job	Default: The job is scheduled to run every day at 06:00 AM.
Schedule for DB Optimize Indexes Job	Default: The job is scheduled to run at 01:30 AM on the last Sunday of every month.

Values to set schedules

To set the schedules, use specific values and characters with special meanings.

Field Name	Allowed Values	Allowed Special Characters
Seconds	0–59	, - * /
Minutes	0–59	, - * /
Hours	0–23	, - * /
Day-of-month	1–31	, - * ? / L W C
Month	1–12 or JAN-DEC	, - * /
Day-of-week	1–7 or SUN-SAT	, - * ? / L C #

Special characters

Special Character	Usage
*	Used to specify all values. For example, * in the Minutes field means <i>every minute</i> .
?	Is allowed for the day-of-month and day-of-week fields to indicate no specific value. This character is useful when you need to specify something in one of the two fields, but not the other.
-	Is used to specify ranges. For example, 10–12 in the Hours field means <i>the hours 10, 11, and 12</i> .
,	Is used to specify more values. For example, MON,WED,FRI in the Day-of-week field means <i>the days Monday, Wednesday, and Friday</i> .

Special Character	Usage
/	Is used to specify increments. For example: • 0/15 in the Seconds field means <i>the seconds 0, 15, 30, and 45</i>. • 5/15 in the Seconds field means <i>the seconds 5, 20, 35, and 50</i>. You can also specify / after the * character; in this case, * is equivalent to having 0 before the /.
L	Is allowed for the Day-of-month and Day-of-week fields. This character is shorthand for last, but it has a different meaning in each of the two fields. Example: The value L in the Day-of-month field means <i>the last day of the month</i>. That is, day 31 for January, day 28 for February on non-leap years, and so on. If used in the Day-of-week field by itself, it means 7 or SAT. But if used in the Day-of-week field after another value, it means <i>the last xxx day of the month</i>. For example, 6L means <i>the last Friday of the month</i>. When using the L option, it is important not to specify lists, or ranges of values, because you can get confusing results.
W	Is allowed for the Day-of-month field. This character is used to specify the weekday (Monday-Friday) nearest the specified day. Example: If you specify 15W as the value for the day-of-month field, the meaning is <i>the nearest weekday to the 15th of the month</i>. So, if the 15th is a Saturday, the trigger fires on Friday the 14th. If the 15th is a Sunday, the trigger fires on Monday the 16th. When the 15th is a Tuesday, then the trigger fires on Tuesday the 15th. However if you specify 1W as the value for Day-of-month, and the 1st is a Saturday, the trigger fires on Monday the 3rd. The trigger does not jump over the boundary of a month. The W character can only be specified when the Day-of-month field specifies a single day, not a range, or list of days.  The L and W characters can be combined for the Day-of-month expression to yield LW, which translates to <i>last weekday of the month</i>.
#	Is allowed for the Day-of-week field. This character is used to specify the nth XXX day of the month. Example: The value of 6#3 in the Day-of-week field means <i>the third Friday of the month</i> (day 6 = Friday and #3 = <i>the third one in the month</i>). Other examples: • 2#1 = the first Monday of the month • 4#5 = the fifth Wednesday of the month  If you specify #5 and five of the specified days in the month, no firing occurs.
C	Is allowed for the Day-of-month and Day-of-week fields. This character is shorthand for <i>calendar</i>. Values are calculated against the associated calendar, if any. If no calendar is associated, then C is equivalent to having an all-inclusive calendar. A value of 5C in the Day-of-month field means <i>the first day included by the calendar on or after the 5th</i>. A value of 1C in the Day-of-week field means <i>the first day included by the calendar on or after Sunday</i>.



The allowed special characters and the names of months and days of the week are not case-sensitive.

Examples of schedule expressions

Expression	Meaning
0 0 12 * * ?	Run at 12 p.m. (noon) every day.
0 15 10 ? * *	Run at 10:15 a.m. every day.
0 15 10 * * ?	Run at 10:15 a.m. every day.
0 15 10 * * ? *	Run at 10:15 a.m. every day.
0 15 10 * * ? 2005	Run at 10:15 a.m. every day during the year 2005.
0 * 14 * * ?	Run every minute, starting at 2 p.m. and ending at 2:59 p.m., every day.
0 0/5 14 * * ?	Run every five minutes, starting at 2 p.m. and ending at 2:55 p.m., every day.
0 0/5 14,18 * * ?	Run every five minutes, starting at 2 p.m. and ending at 2:55 p.m., AND fire every five minutes, starting at 6 p.m. and ending at 6:55 p.m., every day.
0 0-5 14 * * ?	Run every minute starting at 2 p.m. and ending at 2:05 p.m., every day.
0 10,44 14 ? 3 WED	Run at 2:10 p.m. and at 2:44 p.m. every Wednesday in the month of March.
0 15 10 ? * MON-FRI	Run at 10:15 a.m. every Monday, Tuesday, Wednesday, Thursday, and Friday.
0 15 10 15 * ?	Run at 10:15 a.m. on the 15th day of every month.
0 15 10 L * ?	Run at 10:15 a.m. on the last day of every month.
0 15 10 ? * 6L	Run at 10:15 a.m. on the last Friday of every month.
0 15 10 ? * 6L	Run at 10:15 a.m. on the last Friday of every month.
0 15 10 ? * 6#3	Run at 10:15 a.m. on the third Friday of every month.



Pay special attention to the effects of **?** and ***** in the **Day-of-week** and **Day-of-month** fields.

eLearning settings

This setting is only available when you are licensed for eLearning.

Setting	Description
Assign Lessons No More Than Once Every (days)	The frequency with which lessons are assigned.

Scheduled alerts job configuration

Setting	Description
Times to retry before de-activating job	The number of times that the system attempts to run the scheduled job before it removes it from the job queue. Default: 3
Time interval for reactivating job (in hours)	The amount of time that the system waits before resuming attempts to run a job that was deactivated due to failed attempts. Default: 1

Google OpenID settings

If Workforce Optimization is registered with Google, and users in your organization have appropriate privileges, they can use Google credentials, rather than WFO credentials, to sign in to WFO.

Setting	Description
Enable Registration using Google OpenID	Turns on and turns off the ability to use Google authentication to access WFO. The feature must be fully configured to be operational.
Authorization URL Access-Token URL Call-back URL Client ID Client Secret Key	The values for these settings are provided when you register WFO with Google.

i To ensure that Forecasting and Scheduling functions properly, when you enable this setting, be sure that you also enable the setting **Is System Configured to Support SSO (Trusted Login)**.

Related topics

[Set up Mapbox \(page 57\)](#)

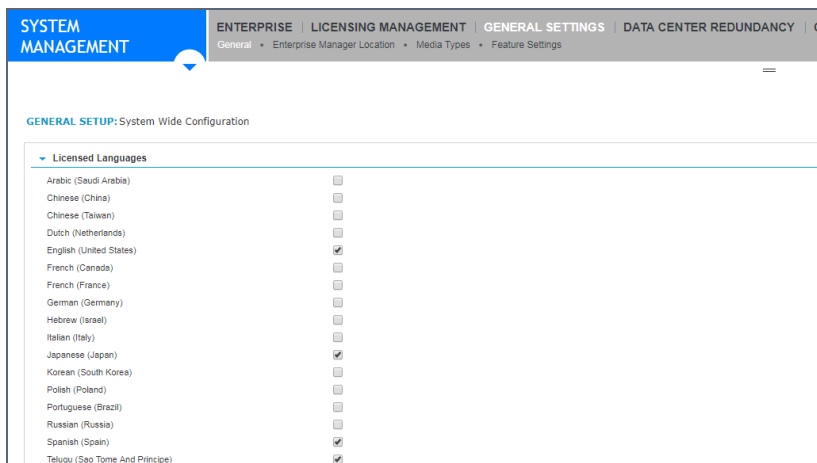
[Enable Google Open ID \(page 58\)](#)

Language selection

Workforce Optimization supports languages other than US English. The language used for the Sign-in page depends on the language selected for the browser and the licensed languages selected on the **General Setup** page. The language used for an application depends on the language that is selected from the My Preferences options.

Available languages

Licensing determines the languages that are available for use on a system. The licensed languages are listed on the **General Setup** page.

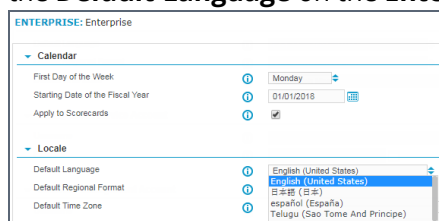


Languages selected on this page determine the languages available for selection on the following pages:

- **Sign-in** page - The language selected by default when the user accesses the Sign-in page is determined by the language specified in the user's browser. The language specified in the user's browser must match one of the languages selected on the **General Setup** page.



- **System Management > Enterprise > Enterprise Settings** page - A system administrator specifies the **Default Language** on the **Enterprise Settings** page when initialing configuring the system.



- **My Preferences** page - A user has the option of selecting a language from the **General** settings of

the **My Preferences** page at any time.



Language used for Sign-in page and language used for WFO applications

The language specified in the web browser that matches a language selected on the **General Setup** page determines the language used by default on the Sign-in page.

The language specified in a user's **My Preferences** page determines the language used in the WFO applications. The default language setting for the **My Preferences** page is determined by the administrator responsible for user management. A user has the option to change the language specified on the **My Preferences** page at any time.

Language used for Sign-in page

The language used for the Sign-in page depends on the language selected for the browser and the licensed languages selected on the **General Setup** page.

When a user accesses the Sign-in page, WFO compares the languages configured in the browser with the list of licensed languages. WFO performs this comparison in the order in which the languages are defined in the browser. For example, assume English (United States) is the first language defined in the browser and Japanese is the second language defined in the browser. In this scenario, WFO first compares English (United States) to the list of licensed languages, and if there is no match, it compares Japanese to the list of licensed languages. The Sign-in page displays in the first browser language that matches a licensed language.

If the browser language is not country and locale specific (for example, English), WFO matches the language part only if there is one supported locale for that language selected as a licensed language. For example, if English is the browser language, and either English (United States) or English (Great Britain) is selected as a licensed language, WFO matches the browser language to the selected licensed language, and displays the Sign-in page in that language. However, if both English (United States) and English (Great Britain) are selected as licensed languages, there is no match and the Sign-in page displays in the default language specified on the **Enterprise Settings** page.



If WFO cannot match the browser language with a licensed language, the Sign-in page displays in the default language selected on the **Enterprise Settings** page.

If the browser language is country and locale specific, and the exact same country and locale language is specified as a licensed language, a match occurs and the Sign-in page displays in the matching country and locale language. For example, if the browser language is English (United States), and Russian, English (United States), and English (Great Britain) are selected as the licensed languages, the Sign-in page displays in English (United States).

Language used for WFO applications

Once a user has successfully logged in, and accessed a WFO application, the WFO application displays in the language that is selected in the user's **My Preferences** page.



Example: Sign in with licensed browser language

A system is running a Chrome browser with English as the selected language. WFO is licensed for English (United States), Spanish, and Hebrew. The user's **My Preferences** language is set to Spanish. The default WFO application language on the **Enterprise Settings** page is set to Spanish.

When accessed, the WFO Sign-in page is in English (United States). The user selects Spanish and signs in. The user accesses an application and the application displays in Spanish. The user changes the **My Preferences** language to Hebrew. The application now displays in Hebrew. The user signs out. The next time the user accesses WFO, the Sign-in page is in English (United States).

Example: Sign in with non-licensed browser language

A system is running a Chrome browser with German as the selected language. WFO is licensed for English (United States), Spanish, and Hebrew. The user's **My Preferences** setting specifies English (United States). The default WFO application language on the **Enterprise Settings** page is set to Spanish.

Because the browser is set to a non-licensed language, WFO uses the default application language, Spanish, for the Sign-in screen. The user selects English (United States) and signs in. The user accesses an application and the application displays in English (United States). The user changes the **My Preferences** language to Hebrew. The application now uses Hebrew. The user signs out. The next time the user accesses WFO, the Sign-in page is in Spanish.

Set up Mapbox

To use the Performance Map feature and map KPIs by location, you must activate your subscription to the third-party mapping service, Mapbox.

If Mapbox is not set up correctly or not set up, an error message directs users to their administrator. If you need assistance with setup, contact your services representative.

Procedure

1. Get an activation code from the map service:
 - a. Go to mapbox.com.
 - b. Create an account.
 - c. Note the activation code that Mapbox provides.
2. In WFO, go to **System Management**. Under **General Settings**, select **General**.
3. Scroll down to the **Map Service** section.

The map agreement text pre-populated with the client name.
4. Select the subscription agreement check box.
5. In the text box, enter the activation code (API access token) provided by Mapbox.
6. Click **Save**.

Related topics

[System-wide configuration options \(page 36\)](#)

Enable Google Open ID

If Workforce Optimization is registered with Google and the users in your organization have the appropriate privileges, they can use Google credentials to sign in to WFO, instead of using the WFO login credentials.

You enable this feature in System Management by completing the following tasks:

1. Set Up Valid Google Email Accounts for All WFO Users.

Assign full e-mail addresses as the user names for all WFO users. These e-mail addresses must be valid Google accounts, such as user1@gmail.com.

To assign the e-mail addresses as user names, do one of the following:

- Update the **User Name** and **E-Mail** fields in the user data import form with the correct e-mail addresses, and import the user data into the User Management module.
- From the User Management module, on the **Employees > Profiles** page, configure the **User Name** and **E-Mail** fields for individual user profiles.

For more details on importing user data or configuring user profiles, see the *Workforce Optimization User Management Guide*.

A valid Google account must also be assigned to the system administration account, such as adminuser@gmail.com.

All users must have privileges assigned that allow them to sign in to WFO.

2. Register Workforce Optimization with Google.

The following describes the general steps to set up the sign in authentication process through Google.

For more detailed information on this process, see the Google link:

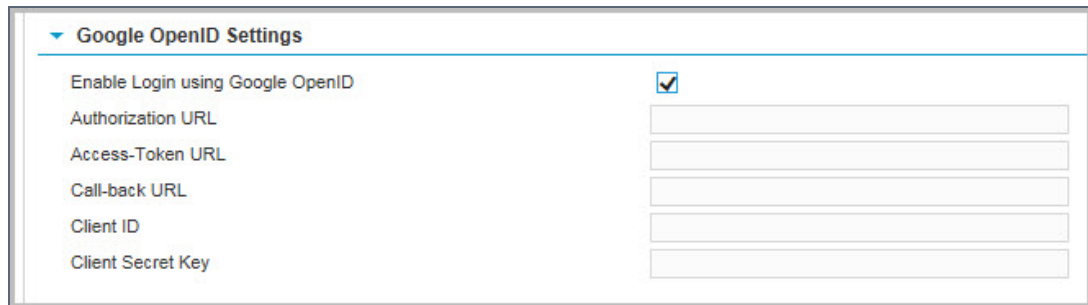
<https://developers.google.com/identity/protocols/OpenIDConnect>

- a. Go to: <https://console.developers.google.com/projectselector/apis/credentials>
- b. Follow the instructions and use the online help on this page to create a new project for Workforce Optimization.

3. Enable Google Authentication Settings in the System Management Module.

- a. Once you have registered WFO with Google, and ensured all users have appropriate email addresses and privileges, enable sign in using Google Open ID.
- b. In WFO, select **System Management > General Settings > General**.
- c. Scroll down to the bottom of the page.
- d. Select **Enable Login using Google OpenID**, and enter the following parameters:

- Authorization URL
- Access-Token URL
- Call-back URL
- Client ID
- Client Secret Key



The screenshot shows a configuration panel titled "Google OpenID Settings". It contains a list of settings with corresponding input fields or checkboxes:

Google OpenID Settings	
Enable Login using Google OpenID	☒
Authorization URL	
Access-Token URL	
Call-back URL	
Client ID	
Client Secret Key	

The parameter information is provided when you register WFO with Google.

Once enabled, when users go to the WFO URL, they are automatically redirected to Google authentication page, where they enter their Google e-mail address and password.



To ensure that Forecasting and Scheduling functions properly, when you enable this setting, ensure that you also enable the Is System Configured to Support SSO (Trusted Login).

Related topics

[System-wide configuration options \(page 36\)](#)

Media Types

The settings on the **Media Types** page under **General Settings** in **System Management** specify the time units for media types, which are used in Forecasting and Scheduling.

Use the drop-down selector to select seconds, minutes, or hours for each media type.

Current media types include:

- Callback
- Chat
- Email
- Face-to-Face
- Fax
- Operations
- Phone
- Phone Outbound
- Project
- Resolution
- Social Post-this is a deferred media type
- Voice-over-IP

Related topics

[System-wide configuration options \(page 36\)](#)

Feature Settings

Use the options on the **Feature Settings** page to manage web and mobile authentication, specify usage terms and conditions, set user session limits, and change Request Management settings to address specific performance and request processing issues.

Related topics

[Configure sign out and authentication method \(page 61\)](#)

[Configure mobile authentication \(page 62\)](#)

[Configure application startup messages \(page 64\)](#)

[Configure the limits for user sessions \(page 67\)](#)

[Change Request Management feature settings \(page 67\)](#)

[Enable or disable voice signature capture \(page 68\)](#)

[Configure Common Cloud Services \(page 70\)](#)

[Configure Common Cloud Services Secrets settings \(page 72\)](#)

[Configure the Operations Manager URL \(page 74\)](#)

[Enable Insights in WFO \(page 75\)](#)

[Configure SCIM User Provisioning \(page 77\)](#)

Configure sign out and authentication method

Only available in multi-tenant systems. On the **Web Authentication Method** tab, customize sign out and authentication for each tenant.

The system provides default sign out and time out messages that include a link to the sign in page. You can assign custom messages and include a specific URL, such as to the IdP, with the message.

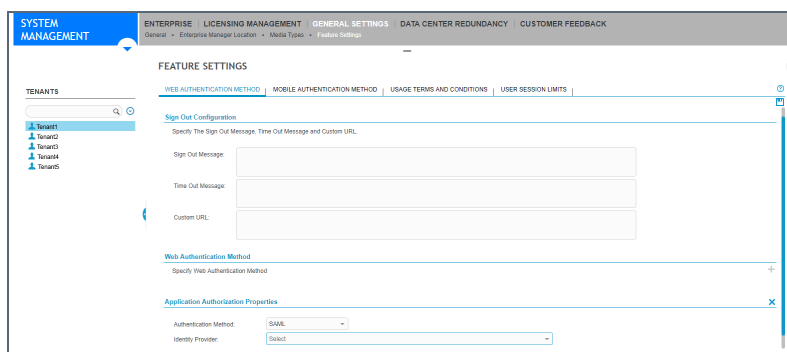
You can also assign the primary authentication method and provider for each tenant.

Before you begin

- A multi-tenant license must be applied.
- Tenants must be created.
- A SAML IdP must be configured in Weblogic for each tenant who is to use SAML authentication.
- You must have the **Configure Tenant** privilege to perform this procedure (available at **Framework - Tenant - View Tenant - Configure Tenant** on the Roles Setup screen).

Procedure

1. Go to **System Management**. Under **General Settings**, select **Feature Settings**.
2. Select the **Web Authentication Method** tab.



3. Optional: Enter text for a **Sign Out Message** and **Time Out Message**.
 4. Optional: Enter a **Custom URL**. A link to this URL is displayed with the sign out and time out messages.
 5. Select the **Add** icon .
 6. Select the **Authentication Method**.
 7. Select the **Identity Provider**. The list includes all providers configured in Weblogic.
 8. Select the **Save** icon .
- To remove a defined authentication method for a tenant, select the **Remove Configuration** icon .

Related topics

[General system settings \(page 35\)](#)

Configure mobile authentication

The Verint Mobile Gateway provides an interface between a Verint solution (for example, WFO) and the mobile client applications (iOS or Android-based). To ensure secure sign-in to mobile applications, each mobile application must be authenticated.

Form authentication

By default, the authentication method is Form, which requires users to enter credentials unique to this system.

OpenID authentication

Although Form authentication is the default for a new system, you can define other methods that use the OpenID authentication protocol. When OpenID authentication is defined:

- The user logs on to the Mobile Client Application and is directed to an Identity Provider (IdP).
- The IdP performs authentication and redirects the user back to the mobile client application with an IdP token.

- The access token grants the user permission to sign in to the application, without sending their credentials.
- The access token is switched to a session token once the sign-in is complete.

Before you begin

You must have the **Configure Mobile Authentication Method** privilege to complete this procedure. (This privilege is available at **Framework - System Management - Configure Feature Settings - Configure Mobile Authentication Method** on the Roles Setup page.)

Procedure

1. Go to **System Management**. Under **General Settings**, select **Feature Settings**.
2. Select the **Mobile Authentication Method** tab.
3. Select an authentication method. The default authentication method is **Form**.
4. Configure the **Application Authentication Properties** for the authentication application.
5. To save the page settings, click the **Save** icon in the upper right corner of the page.

Application Authentication Properties settings

Each authentication application defined must include specific settings. The settings required depend on the selected authentication method.

Form Method

Property	Description
Method	The default authentication method for a new system or tenant is Form . The Form authentication method requires the user to provide credentials in the Sign In page that are checked against credentials stored and managed in the application.
Provider	When the selected Method is Form, this field defaults to DB Realm .

OpenID Method

Property	Description
Method	Options are Form or Open ID . The default authentication method for a new system or tenant is Form . Open ID directs authentication to an Identity Provider (IdP) that holds the user credentials.
Provider	The Identity Provider (IdP) that holds the user credentials. When the selected method is Open ID, this field defaults to Azure AD. Available options are Auth0, Azure AD, Generic, Google, Okta, PingFederate, OneLogin and ADFS . If the name of your IdP does not appear in the list, select Generic . The Generic option allows you to configure any other OIDC provider that follows the OIDC 1.0 standards.

Property	Description
Username claim	The claim in the id_token that provides a value for the user name in WFO. For Azure, this is the UPN (User Principal Name); for Google OpenID, this is the email address. Okta uses <i>preferred_username</i>. • Custom - Select this check box to use a custom claim name. The custom claim name is used to validate the ID token used in the authentication of the user with the WFO application. When this option is selected, the username claim becomes a free text field limited to 100 characters. • User authenticates with different username - Select this option to have the mobile client use an alternate username to authenticate with the IdP. In this scenario, the mobile client uses a different username to authenticate with the IdP than is used to authenticate with the WFO application.
Discovery Document URL	The system uses the Discovery Document URL to retrieve the various end-points, required to validate the IdP Access token. For Example: <code>https://login.microsoftonline.com/{IdP_tenant}/.well-known/openid-configuration</code>. The Discovery Document URL, and the jkws_uri that is obtained from the Discovery URL response, must be accessible from the application server.
Application ID	A unique ID assigned to the authentication application when it is registered with the IdP. For example, 6731de76-14a6-49ae-97bc-6eba6914391e or 0oabucvyc38HLL1ef0h7.
Bundle ID	The Bundle ID or Package Name is a string that the (IdP) uses to validate the identity of the invoking application. The Bundle ID for each authentication application that you create must be unique, and according to guidance in the OIDC customer requirements, for example, <code>com.verint.teamview</code>
Redirect URI	The URI that the IdP uses to redirect back to the mobile application following a successful signin attempt. For example: <code>com.verint.workview://oauthredirect</code> or <code>com.verint.teamview://oauthredirect</code>.
Actions	The Delete icon removes the current row,

Related information

Configure mobile with DB Realm authentication (*Authentication Guide*)

Configure mobile OpenID method authentication settings (*Authentication Guide*)

Verint Mobile Gateway (*Technology, Security & Network Integration Deployment Reference Guide*)

Configure application startup messages

You can create two types of messages which are sent to all users at application startup: a Terms and Conditions message and an Announcement message.

Terms and conditions message

You create a Terms and Conditions message to specify the usage terms and conditions that a user must review and accept to access the system. Once configured, a Terms and Conditions message displays to the user when the user logs in. You can also configure the Terms and Conditions message to reappear to the user at specific time intervals.

A user has the option to click an Accept or Decline button at the bottom of the Terms and Conditions message. If the user declines the terms and conditions, the user account is locked and the user cannot access the application.

Announcement message

You can create an Announcement message when you want to send any kind of announcement to all users. Once configured, an Announcement message displays to each user when the user logs in. A user has the option to select an OK button or a Show Me Later button at the bottom of the Announcement message. If the user selects the Show Me Later button, the message displays to the user again the next time the user logs in.

If you compose an Announcement message, you can preview the message to see how it will appear to end users.



If you create both a Terms and Condition message and an Announcement message, the Terms and Condition message displays to the user first. If the user accepts the Terms and Conditions message, the Announcement message then displays to the user.

Before you begin

You must have the **Configure Application Startup Messages** privilege to perform this procedure. (This privilege is available at **Framework - System Management - Configure Feature Settings - Configure Application Startup Messages** on the Roles Setup page.)

Procedure

1. Go to **System Management**. Under **General Settings**, select **Feature Settings**.
2. Select the **APPLICATION STARTUP MESSAGES** tab.
3. The **Response Options** setting defaults to the setting that is appropriate for the selected Message Type and cannot be changed.
 - If you selected the **Terms and Conditions** Message Type, the **Accept/Decline** value appears in the **Response Options** drop-down list. With this setting an Accept button and a Decline button appear to users at the bottom of the Terms and Conditions message.
 - If you selected the **Announcement** Message Type, the **OK/Show Me Later** value appears in the **Response Options** drop-down list. With this setting, an OK button and a Show Me Later button appear to users at the bottom of the Announcement message.
4. If you selected the **Terms and Conditions** Message Type, a **Display Message** drop-down list appears in the user interface. Use the **Display Message** drop-down list to set how often the terms and conditions message is displayed to the user. Your options include:
 - None
 - Every Day
 - Every Month

- Every Three Months
 - Every Six Months
 - Every Twelve Months
5. In the **Message** text box:
- If you selected the **Terms and Conditions** Message Type, enter the Terms and Conditions message to be displayed.



When **None** is selected as the frequency to display the Terms and Conditions message, the **Message** text box is unavailable.

- If you selected the **Announcement** Message Type, enter the Announcement message to be displayed.
6. If you selected the **Announcement** Message Type, click the **Preview** button to see how your message will appear to users. (The **Preview** feature is not available for the **Terms and Conditions** Message Type.)
7. Do one of the following:
- To save the message and have it presented to the user at the next user login, click the Save Configuration icon . If you created a **Terms and Conditions** message, and configured a **Display Message** interval, the message will display to the user again at the configured time interval.
 - To disregard any previous actions taken by the user, and have the message saved and presented to the user at the next user login, click the Reset Messages and Save icon .

Inserting hyperlinks into a message (on-premises deployments only)

If you want to include a hyperlink in a Terms and Conditions or Announcement message, you can do so by inserting a record into the BPCONFIG table of the BPMAINDB database. Specifically, insert a record in the BPCONFIG table with the key '**system/validDomainNames**'. The values for the key should be domain names (such as www.verint.com). Separate multiple domain names with a colon. For example, you could enter www.verint.com:www.cnn.com as the key values. When you enter absolute URLs that include these domain names in the Message text box (such as http://www.verint.com), they will be hyperlinks in the message that is presented to the user. If you enter an absolute URL in the Message text box that includes a domain name that is not entered as a value for the '**system/ValidDomainNames**' key, the text will not be hypertext (clickable) in the message that is presented to the user.

Note that the domain name value specified in the **system/validDomainNames** key must be strictly matched. For example, if "verint.com" is specified as the key value, and "www.verint.com" is used in the message text, "www.verint.com" is not considered a valid domain and will not appear as a hyperlink. You must specify "www.verint.com" as the key value for it to be a valid domain and appear as a hyperlink in the message.

Related information

Modifying User names, Passwords, and Account Status (*User Management Guide*)

Configure the limits for user sessions

Although unlimited by default, you can limit the number of concurrent sessions per user. You can limit the number of IP addresses from which the user can sign in and the number of sessions per IP address.

- When the number of IP addresses is exceeded, all sessions from the oldest IP Address are timed out.
- When the number of sessions is exceeded, the oldest session is timed out.

Before you begin

You must have the **Configure User Session Limits** privilege to perform this procedure. (This privilege is available at **Framework - System Management - Configure Feature Settings - Configure User Session Limits** on the Roles Setup page.)

Procedure

1. In **System Management**, under **General Settings**, go to **Feature Settings**.
2. Select the **User Session Limits** tab.
3. Enter the limits:
 - **Maximum Number of Different IP Addresses:** The limit for the number of different IP addresses from which the user can sign in. Leave blank to indicate "no limit."
 - **Maximum Number of Sessions Per IP Addresses:** The limit for the number of sessions for each IP address from which the user has signed in. Leave blank to indicate "no limit."
4. Select Save Configuration .

Related topics

[Limiting the number of concurrent WFO sessions \(page 80\)](#)

Change Request Management feature settings

Request Management feature settings control where request validation alerts are shown for managers and employees, the maximum number of requests shown on the Employee Requests page for managers, and how request processing is performed. Except for the *Maximum requests per page* setting, all settings affect performance.

When a system is initially configured, do not change the performance settings. Only consider making changes to these settings when specific, serious issues with system performance and request processing occur. These issues can occur when an extremely high volume of requests is submitted in a short time.



These settings are not available in a multi-tenant environment.

Available options to address issues

Settings related to viewing request validation alerts include the following:

- Determine whether the **Alerts** checkbox is selected and alerts are displayed on the Request List page by default upon login. When navigating to this page, you can select or unselect the **Alerts** checkbox to view alerts. To improve system performance, it is highly recommended to select the following option for this setting: **Alerts not selected and no alerts are displayed by default upon login**.
- For managers, you can limit net staffing validations and keep the other validations visible on both the request list and request details.
- For managers, lowering the maximum number of requests that can be viewed on their request list, the Employee Requests page. This option applies when the default number of 30 was already changed to a much higher number.
- Configure the maximum number of employee requests returned by the V2 Get My Requests API. By default, the **Maximum requests returned by the V2 Get My Requests API** setting is zero (0), which represents an *unlimited* number of requests. To *limit* the number of requests, select any value from **1-2000** for this setting.
- To limit the date range used on the Employee Requests page, configure a specific number of months for the setting, **Maximum date range (in months) when filtering employee requests**. By default, the **Maximum date range (in months) when filtering employee requests** setting is zero (0), which represents an *unlimited* number of months. To limit the date range, select any value (other than zero) for this setting.
- Using queues for auto processing in any or all request types. Processing requests in a queue frees up resources for other processes in WFO. Example: Use this option for shift bidding when you expect an extremely high volume of shift bid request to be submitted in a short time.
- Using sequential processing for time off pools. The default option provides faster processing. However, the sequential processing option improves staffing accuracy when a high volume of requests are submitted in a short time for the same time off pool.

Procedure

1. Go to **System Management**. Under **General Settings**, select **Feature Settings**.
2. Select the **Request Management** tab.
3. Change the defaults that are needed to address your issues.



Before making any changes, contact Technical Support.

4. Select the **Save** icon .

Enable or disable voice signature capture

Speaker separation uses voice signatures, a form of biometrics identification, to identify speakers in interactions recorded in a mono channel telephony environment.

In System Management, in the Voice Signature tab, enable or disable voice signature capture for all agents in your organization:

- If you enable voice signature capture, you can disable the setting for individual agents in User Management.
- If you enable voice signature capture and then disable it, captured voice signatures are deleted, and the accuracy of identifying speakers drops for mono channel telephony environments.



Voice signature capture is now configurable, and disabled by default for all agents. Previously, voice signature capture was not configurable, and enabled by default for all agents.

After this update, you have the option to delete previously collected voice signatures. This option is only available if you have not yet enabled or disabled voice signature capture, or have not previously deleted voice signatures.

Before you begin

- You must have the **Manage Agent Signature Configuration** privilege.
- Make sure you understand the impact of enabling or disabling voice signature capture. See [Voice Signature configuration reference \(page 70\)](#).

Procedure

1. Go to **System Management**. Under **General Settings**, click **Feature Settings**.
2. Click **Voice Signature**.

3. To enable voice signature capture, select **Enable voice signature capture**.
Voice signatures are captured for all agents in your organization.
4. To disable voice signature capture after it has been enabled, clear the **Enable voice signature capture** check box.
All voice signatures are deleted, and voice signature data is no longer collected.
5. To delete all existing voice signatures, select **Delete existing voice signatures** (Only available if you have not previously enabled or disabled voice signature capture, or have not previously deleted agent voice signatures).
6. Select **Save**

Related information

Agent voice signature (*User Management Guide*)

Voice Signature configuration reference

The following table describes the available settings in the Voice Signature tab.

First-time access	Enable voice signature capture	Delete existing voice signatures	Status
Yes	Selected	Selected	Capture starts from scratch.
Yes	Selected	Not selected	For existing users, capture continues from where it left off. For new users, capture starts from scratch.
Yes	Not selected	Selected	Capture is disabled, and existing voice signatures are deleted.
Yes	Not selected	Not selected	Capture is disabled. Existing voice signatures continue to be used for speaker separation.
No	Selected	Not available	Capture starts from scratch.
No	Not selected	Not available	Capture is disabled, and existing voice signatures are deleted.

Configure Common Cloud Services

From the Common Cloud Services screen, you can configure Common Cloud Services Secrets or Operations Manager URLs.

- [Workflow: Configure Common Cloud Services Secrets \(page 71\)](#)

Any application that requires a WFO service to "dial out" to a cloud instance requires a set of credentials to authenticate the service. You configure these credentials in the "Configure Secrets" section of the Common Cloud Services screen.

- [Configure the Operations Manager URL \(page 74\)](#)

In a multi-tenant enabled environment, you can configure the URL that opens the Operations Manager application. The SPA can configure separate URLs for the SPA and for each tenant.

- [Enable Insights in WFO \(page 75\)](#)

Data Insights Bot dashboards provide insights into trends, activities, and performance based on the product data available. In WFO, users can view their Data Insights Bot dashboards under Insights, while WFO administrators can manage access through user roles.

To display Verint Data Insights Bot dashboards, Workforce Optimization (WFO) requires a URL for Data Insights Bot. The URL is region-specific and determined by the location of the customer's dashboard data.

Related topics

[Feature Settings \(page 61\)](#)

Workflow: Configure Common Cloud Services Secrets

Any application that requires a WFO service to "dial out" to a cloud instance requires a set of credentials to authenticate the service. The customer must first register the application or service, subscribe to the cloud service to access, and then configure the credentials in the "Configure Secrets" section of the Common Cloud Services.

Workflow

1. [Register WFO client on the authorization server \(page 71\)](#)
Work with Verint Support to get the WFO applications and cloud services you need registered and subscribed with Verint Identity.
2. [Configure Common Cloud Services Secrets settings \(page 72\)](#)
On the Customer Configuration Settings (CCS) page, enter the authentication credentials for the Verint Identity Service. Once the service is active and properly configured, the customer's client application (machine) can use these settings to access the Verint Cloud API or service.

Register WFO client on the authorization server

Work with Verint Support to get the WFO applications and cloud services you need registered and subscribed with Verint Identity.

Procedure

- Give Verint Support the following information:
 - The *name of the WFO application or service* that requires access to the cloud application or service. Example: Automated Verification > WFE
 - The *names of the cloud application or service* to access. Example: WFE

Verint Support will register your applications, subscribe you to the required cloud services, and return the following information to you:

- **Application (client) ID:** The Client ID that uniquely identifies the OAuth application registered with Verint Identity.
- **Client Secret:** The confidential string for the OAuth application that is used to authenticate your application when requesting tokens.
- ■ For Verint Identity V1—**Directory (tenant) ID:** The tenant ID (also called directory ID) of the specific Microsoft Entra (formerly Azure Active Directory) instance (or "tenant") where the Client application is registered.
- ■ For Verint Identity V2—**Open ID Config URL:** The URL that points to the OpenID Provider Configuration Document for the Identity Service V2 compliance zone. This is the **host** field in the M2M credentials file.



Verint Identity V2 is being rolled out to cloud customers, and may be unavailable in your site.

What to do next

[Configure Common Cloud Services Secrets settings \(page 72\)](#)

Configure Common Cloud Services Secrets settings

On the Customer Configuration Settings (CCS) page, enter the authentication credentials for the Verint Identity Service. Once the service is active and properly configured, the customer's client application (machine) can use these settings to access the Verint Cloud API or service.

Audience: Verint Support only.

This procedure is for Verint Services personnel. Customers do not access this page.



Verint Identity V2 is being rolled out to cloud customers, and may be unavailable in your site.

Before you begin

- Ensure that the 2021R1 Cloud Configuration feature flag is enabled.
- In a multi-tenant environment, the **Configure Tenants** privilege is required to edit this page on behalf of a customer (tenant).
- Ensure that you have the **Configure Common Cloud Services** security privilege (available from the **Framework - System Management - Feature Settings** privileges on the **Roles Setup** page)
- The customer must [Register WFO client on the authorization server \(page 71\)](#)

Procedure

1. Go to **System Management**, under **General Settings**, select **Feature Settings**.
2. Select the **Common Cloud Services** tab.
3. Select a customer from the **Tenants** list on the left.
4. To activate authentication credentials, move the **Active** slider to **On**.
5. In **Identity Service**, select the version of Verint Identity in use by the tenant.

6. Configure the following fields:

- **Application (client) ID:** The Client ID that uniquely identifies the OAuth application registered with Verint Identity.
 - **Client Secret:** The confidential string for the OAuth application that is used to authenticate your application when requesting tokens.
 - For Verint Identity V1—**Directory (tenant) ID:** The tenant ID (also called directory ID) of the specific Microsoft Entra (formerly Azure Active Directory) instance (or "tenant") where the Client application is registered.
 - For Verint Identity V2—**Open ID Config URL:** The URL that points to the OpenID Provider Configuration Document for the Identity Service V2 compliance zone. This is the **host** field in the M2M credentials file.
7. To configure automatic rotation of the **Current** and **Backup** keys:
- a. Select the **Rotatable** check box. Once selected, the following options become available:
 - b. **Rotation schedule date:** Enter the date when key rotation should begin.
This date must be at least equal to the full rotation period. For example, if the rotation period is 90 days, the rotation schedule date must be 90 or more days from today.
 - c. **Rotation period (days):** Specify the number of days between each key rotation. The default and recommended value is 90 days.
 - d. **For V1 only — Scope URL:** Provide the URL that defines the scope of the key. This typically corresponds to the resource or service that the key applies to.
 - e. **For V1 only — Environment name:** Enter the environment and region segment of Verint's API Gateway URL.
Commonly used production systems include: identity/au, identity/ca, identity/eu, identity/sg, identity/uk, identity/us.
 - f. To validate these settings against the authentication platform, click  **Validate** in the upper right corner of the page.
8. To save these settings, click  **Save** in the upper right corner of the page.

Related topics

[Workflow: Configure Common Cloud Services Secrets \(page 71\)](#)

[Understanding key rotation timing and recovery \(page 73\)](#)

Understanding key rotation timing and recovery

Learn how key rotation timing works for Identity V1 and V2 and how the system handles swap failures.

 Identity V2 is being rolled out to cloud customers, and may be unavailable in your site.

When configuring key rotation for the Common Cloud Services (CCS) **Secrets** settings, you schedule rotation by setting the:

- **Start date**, which is when the next key rotation is planned to occur.
- **Period**, which defines how often the system rotates the keys, measured in days.

At the halfway point in the rotation cycle, the system tries to swap the current and backup keys.

If the swap fails, the system retries until successful, then recalculates the next rotation date based on the actual swap completion date.

Example: Key rotation gets delayed when swap fails

The following example shows how a failed swap affects the rotation schedule.

- **Rotation period:** 90 days
- **Scheduled rotation start date:** January 1
- **Swap date:** February 15 (45 days after January 1)

The swap fails due to a configuration issue.

The system continues retrying the swap.

On February 20, the swap succeeds.

The system recalculates the next rotation schedule based on February 20 as the new halfway point.

- **Revised rotation start date:** April 5 (45 days from February 20)

Related topics

[Workflow: Configure Common Cloud Services Secrets \(page 71\)](#)

[Configure Common Cloud Services Secrets settings \(page 72\)](#)

Configure the Operations Manager URL

In a multi-tenant enabled environment, the Service Provider Administrator (SPA) can configure the URL that opens the Operations Manager application. The SPA can configure separate URLs for the SPA and for each tenant.

An **Operations Manager** option appears in the main navigation menu of the WFO application for a user who has any of the Work Manager privileges. When the SPA configures an Operations Manager URL, a user clicks the **Operations Manager** option in the main menu and then clicks **Operations Manager** again on the screen that opens to access the Operations Manager application.

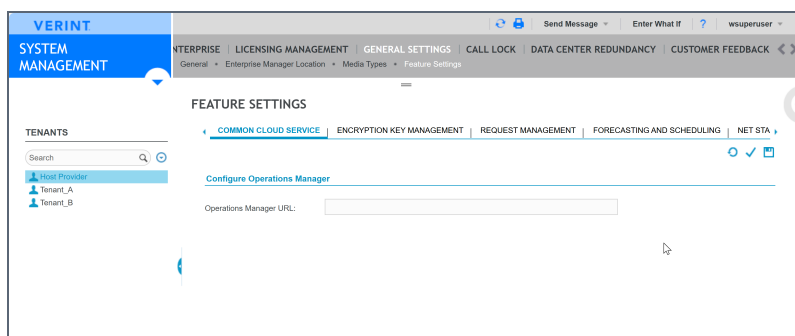
If no Operations Manager URL is configured, and a user clicks on the **Operations Manager** option to open the Operations Manager application, a message displays stating "Operations Manager is not configured. Contact your administrator."

Before you begin

Make sure you have the **Configure Operations Manager URL** security privilege (available from the **Framework - System Management - Feature Settings** privileges on the Roles Setup page)

Procedure

1. Go to **System Management**. Under **General Settings**, select **Feature Settings**.
2. Select the **Common Cloud Services** tab.



3. From the list of **Tenants** on the left, select the tenant for whom you are configuring the Operations Manager URL.
4. In the **Configure Operations Manager** section, in the **Operations Manager URL** field, enter the URL to open the Operations Manager application.
5. To save the settings, click  **Save** in the upper right corner of the page.
An **Operations Manager** option now appears in the main navigation menu of the WFO application. Users can click the **Operations Manager** option in the main menu and then click **Operations Manager** again on the screen that opens to access the Operations Manager application.

Enable Insights in WFO

Data Insights Bot dashboards provide insights into trends, activities, and performance based on the product data available. In WFO, users can view their Data Insights Bot dashboards under Insights, while WFO administrators can manage access through user roles.

To display Verint Data Insights Bot dashboards, Workforce Optimization (WFO) requires a URL for Data Insights Bot. The URL is region-specific and determined by the location of the customer's dashboard data.

Before you begin

Ensure that:

- The customer tenant is licensed for and enabled to use Data Insights Bot.
- You have the correct Insights URL for the customer's region.
- You are signed in with an administrator-level account that has **View and Edit Common Cloud Services** privileges.

Procedure

1. Go to **System Management**; under **General Settings**, select **Feature Settings**.
2. Select the **Common Cloud Services** tab.
3. Select a customer from the list of **Tenants**.
4. In the **Insights URL** field, enter the URL. The URL has the format:
https://region.datainsights.verintcloudservices.com
where *region* identifies the country or region for the customer's data.

Each customer uses a specific Data Insights Bot URL. Example for the United States:

`https://use1.datainsights.verintcloudservices.com`

5. Select  **Save** in the upper right corner of the page.

Related topics

[Configure Common Cloud Services \(page 70\)](#)

Configure Net Staffing

In Queue Analytics, the Net Staffing statistic allows managers to know how much they are short or surplus on staffing, allowing them to manage VTO and Shift requests efficiently.

The calculation for Net Staffing can be configured to be based on Headcount Staffing or Dedicated Staffing.

- **Headcount Staffing:** Number of agents qualified to work on a particular queue for a particular interval. When viewing an aggregation, it is the number of hours.
- **Dedicated Staffing:** The total contribution made by agents to a queue. Unlike Headcount staffing, where an agent is counted as 1 for each queue they are skilled for, Dedicated staffing only counts a fraction of an agent, depending on the amount they are estimated to contribute to the queue. For example, if an agent is skilled for four queues, their contribution may be split over the four queues.



In Reports, Net Staffing is still based on Headcount staffing, regardless of choice made for Net Staffing Calculation.

Procedure

1. Go to **System Management**. Under **General Settings**, select **Feature Settings**.
2. Select the **Net Staffing** tab.
3. For **Net Staffing Calculation** select either *Headcount Staffing* or *Dedicated Staffing*.

Related information

Track queue performance (*Forecasting & Scheduling Guide*)

Configure Campaigns

In Calendar, if an employee is moved between organizations, the scheduling period ID on any shift assignments or events may become invalid, if the organizations are not associated with the same campaign. The scheduling period IDs must be updated to a scheduling period for the organization the employee has been moved to, or is pooling for. You can use the *Enable auto update of SP ID when employees are moving organization* option, to determine whether the SP IDs get automatically updated, or if you must do it manually. If this option is set, then the SP IDs get updated automatically when an employee is moved between organizations.



When *Enable auto update of SP ID when employees are moving organization* is enabled, it covers all campaigns and organizations.



Enable auto update of SP ID when employees are moving organization is currently being rolled out to cloud customers. It may not be available in your site just yet.

Procedure

1. Go to **System Management**. Under **General Settings**, select **Feature Settings**.
2. Select the **Campaigns** tab.
3. To have the scheduling period ID automatically updated on shift assignments, select *Enable auto update of SP ID when employees are moving organization*.

Related information

Shift assignment settings (*Forecasting & Scheduling Guide*)

Configure SCIM User Provisioning

The Provisioning Settings page allows an administrator to configure the settings required for WFO to provision users from an identity provider using the SCIM protocol.

Part of the configuration is the selection of other employee fields that can only be managed through the SCIM API. Fields synchronized with SCIM are not editable through the WFO user interface or user management API.



The *Configure user details synchronized over SCIM* settings are currently being rolled out to cloud customers. It may not be available in your site just yet.

Setting	Description
JWT Token	The JSON Web Token (JWT) token is required for authentication when your identity provider connects to the WFO application using the SCIM protocol during the provisioning process. When you create a token, you can set its expiry date. You can also revoke any of the existing tokens from this page at any time.
Configure user details synchronized over SCIM	When WFO is configured for user provisioning using an identity service, the following fields are read-only in the WFO user interface and only manageable through SCIM: • Username • First Name • Last Name In addition to those fields, you can also select any of the following user details fields to be synchronized with SCIM: • Desktop Messaging Username • City • Employee Number • Start Date • Zip/Postal Code • Address 1 • Country • End Date • State • Cell Phone • Email • Home Phone • Work Phone

Related information

Identity Service provisioning configuration (On-premises environment) (*User Management Guide*)

Limiting the number of concurrent WFO sessions

The number of concurrent WFO sessions is unlimited, by default. You can set a limit, though, to manage the number of concurrent WFO sessions on each application server.

You can limit the number of concurrent WFO user sessions on an application server. Or you can include "system user" sessions, and limit the total number of concurrent WFO sessions. System user sessions are those sessions that internal system requests create.

By default, system user sessions are not included in the count of concurrent WFO sessions.

If the number of concurrent WFO sessions reaches the configured limit, any requests that require the creation of a new session receive a response with the HTTP status code "503 Service Unavailable."

Related topics

[Set a limit for concurrent WFO sessions \(page 80\)](#)

Set a limit for concurrent WFO sessions

To set a limit for the number of concurrent WFO sessions, you modify the BPCONFIG table in the BPMAIN database.

There are two parameters you can set:

- **MaxSessionLimitForWFO.** Limits the number of active sessions that can be created for WFO on the server.
- **IncludeSystemUserForSessionLimit.** Includes or excludes the WFO system user sessions in the total session count. Only used when MaxSessionLimitForWFO is greater than 0. Possible values are true and false. The default is false. (The system user is not included in the total session count.)

Procedure

1. In SQL Server Management Studio , open a query window in the BPMAINDB database.
2. To limit the number of concurrent sessions, run the following query:

```
DECLARE @MaxSessionCount varchar(50)
SET @MaxSessionCount = '1000000' -- Update the Max session count here
IF EXISTS(SELECT 1 FROM BPCONFIG WHERE NAME='system/MaxSessionLimitForWFO')
BEGIN
    PRINT 'Setting system/MaxSessionLimitForWFO value to : ' + @MaxSessionCount
    UPDATE BPCONFIG SET VALUE=@MaxSessionCount WHERE
    NAME='system/MaxSessionLimitForWFO'
END
ELSE BEGIN --Get the next key for these new rows
    DECLARE @nextkey INT
    EXEC Bp_nextkey 'BPCONFIG',@nextkey output,1
    PRINT 'Setting system/MaxSessionLimitForWFO value to : ' + @MaxSessionCount
    INSERT INTO BPCONFIG(ID,NAME,VALUE) values
    (@nextkey,'system/MaxSessionLimitForWFO',@MaxSessionCount)
END
```


3. To include the system user sessions in the total session count, run the following query:


```
DECLARE @IncludeSystemUser varchar(50)
SET @IncludeSystemUser = 'false' -- Update the include System User in session count here
IF EXISTS(SELECT 1 FROM BPCONFIG WHERE NAME='system/IncludeSystemUserForSessionLimit')
BEGIN
PRINT 'Setting system/IncludeSystemUserForSessionLimit value to : ' + @IncludeSystemUser
UPDATE BPCONFIG SET VALUE=@IncludeSystemUser WHERE
NAME='system/IncludeSystemUserForSessionLimit'
END
ELSE BEGIN --Get the next key for these new rows
DECLARE @nextkey INT
EXEC Bp_nextkey 'BPCONFIG',@nextkey output,1
PRINT 'Setting system/IncludeSystemUserForSessionLimit value to : ' + @IncludeSystemUser
INSERT INTO BPCONFIG(ID,NAME,VALUE) values
(@nextkey,'system/IncludeSystemUserForSessionLimit',@IncludeSystemUser)
END
```
4. Restart the WFO_ProductionDomain_ProductionServer service.

Related topics

[Limiting the number of concurrent WFO sessions \(page 80\)](#)

[Modify the limit on concurrent WFO sessions \(page 81\)](#)

Modify the limit on concurrent WFO sessions

To modify the limit for the number of concurrent WFO sessions, update the session limit keys in the BPCONFIG table in the BPMAIN database.

Update the values

You can change the value configured for MaxSessionLimitForWFO. A value of 0 sets the maximum number of sessions to "unlimited."

Update the value of IncludeSystemUserForSessionLimit to include (true) or exclude (false) the system user sessions in the total session count. If MaxSessionLimitForWFO is 0, the value for this parameter is ignored.

Procedure

1. In SQL Server Management Studio , open a query window in the BPMAINDB database.
2. To update the maximum number of concurrent sessions, run the following query:


```
DECLARE @MaxSessionCount varchar(50)
SET @MaxSessionCount = '1000000' -- Update the Max session count here
IF EXISTS(SELECT 1 FROM BPCONFIG WHERE NAME='system/MaxSessionLimitForWFO')
BEGIN
PRINT 'Setting system/MaxSessionLimitForWFO value to : ' + @MaxSessionCount
UPDATE BPCONFIG SET VALUE=@MaxSessionCount WHERE
NAME='system/MaxSessionLimitForWFO'
END
ELSE BEGIN --Get the next key for these new rows
```

```
DECLARE @nextkey INT
EXEC Bp_nextkey 'BPCONFIG',@nextkey output,1
PRINT 'Setting system/MaxSessionLimitForWFO value to : ' + @MaxSessionCount
INSERT INTO BPCONFIG(ID,NAME,VALUE) values
(@nextkey,'system/MaxSessionLimitForWFO',@MaxSessionCount)
END
```

3. To change the tracking to include (or exclude) the system user sessions in the total session count, run the following query:

```
DECLARE @IncludeSystemUser varchar(50)
SET @IncludeSystemUser = 'false' -- Update the include System User in session count here
IF EXISTS(SELECT 1 FROM BPCONFIG WHERE NAME='system/IncludeSystemUserForSessionLimit')
BEGIN
PRINT 'Setting system/IncludeSystemUserForSessionLimit value to : ' + @IncludeSystemUser
UPDATE BPCONFIG SET VALUE=@IncludeSystemUser WHERE
NAME='system/IncludeSystemUserForSessionLimit'
END
ELSE BEGIN --Get the next key for these new rows
DECLARE @nextkey INT
EXEC Bp_nextkey 'BPCONFIG',@nextkey output,1
PRINT 'Setting system/IncludeSystemUserForSessionLimit value to : ' + @IncludeSystemUser
INSERT INTO BPCONFIG(ID,NAME,VALUE) values
(@nextkey,'system/IncludeSystemUserForSessionLimit',@IncludeSystemUser)
END
```

4. Restart the WFO_ProductionDomain_ProductionServer service.

Related topics

[Set a limit for concurrent WFO sessions \(page 80\)](#)

[Limiting the number of concurrent WFO sessions \(page 80\)](#)

Remove the limit on concurrent WFO sessions

To remove the limit for the number of concurrent sessions, delete the session limit keys in the BPCONFIG table in the BPMAIN database.

If you remove the MaxSessionLimitForWFO key, the value for the IncludeSystemUserForSessionLimit key is ignored.

Procedure

1. In SQL Server Management Studio , open a query window in the BPMAINDB database.
2. To remove the limit on the number of concurrent WFO sessions, run the following query:

```
DELETE FROM BPCONFIG where NAME= 'MaxSessionLimitForWFO'
```

```
DELETE FROM BPCONFIG where NAME= 'IncludeSystemUserForSessionLimit'
```
3. Restart the WFO_ProductionDomain_ProductionServer service.

Related topics

[Set a limit for concurrent WFO sessions \(page 80\)](#)

[Limiting the number of concurrent WFO sessions \(page 80\)](#)

Integration and adapters

This chapter provides an overview of the suite’s integration service, server packages and their components.

The following content is only meant to provide an overview of the integration service.
For details on the Integration server and adapters see the following:

- The adapter online help: navigate to **Integration Management > Integration Server > Integration Server**, and click **Help**.
- The Workforce Optimization solution’s suite of Adapter guides: these guides are shipped with each customer’s installation DVDs.

Topics

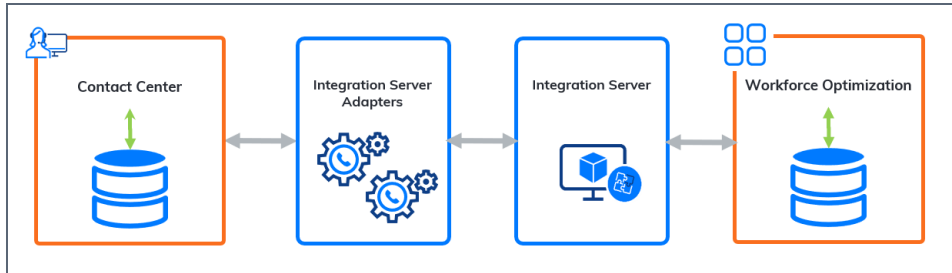
About the Integration Service 85

Integration packages and server monitoring 90

Integration server package components 93

About the Integration Service

The System Management module gives you access to the Integration Server, an open integration platform that provides seamless information flow between contact center data sources and applications, and the Workforce Optimization Solution, and other applications within the system.



The Integration Service consists of the following main software components:

- The Integration Server, which resides on a server machine.
- The System module within the suite. This module configures the server.
- Integration packages, adapters, and interfaces for the most common types of ACDs. These include Time Collection, Historical Time Collection, Agent Sync, Scorecards Agent Stats, and Contact Statistics. Integration Server also provides generic adapters and interfaces that you can use as a framework to create custom adapters and integration packages.

The Integration Server supports data exchange using a variety of protocols including file based (XML or fixed format), all major database protocols, and a variety of proprietary based CRM and telephony protocols. In addition to integrating with the suite, Integration Server provides the functionality to manage integration with ACDs, CTIs, and email systems.

Related topics

[Integration Server architecture \(page 85\)](#)

[Adapters and interfaces \(page 87\)](#)

[Navigating to the Integration Servers \(page 88\)](#)

[Extenders and converters \(page 93\)](#)

[Timers \(page 94\)](#)

Integration Server architecture

The Integration Server provides the following services:

- Framework services for managing integration tasks (in the form of integration adapters and interfaces). These services include security, licensing, database access, workflow management, error detection and recovery, logging and alerts, and Watchdog and scheduling services.
- Monitoring the status of adapters and interfaces (example, connection to the ACD).

- Controlling adapters and interfaces (start, stop).
- Supplying configuration information to adapters and interfaces.
- Passing data from the adapters and interfaces to the suite database.

Related topics

[Integration Server features \(page 86\)](#)

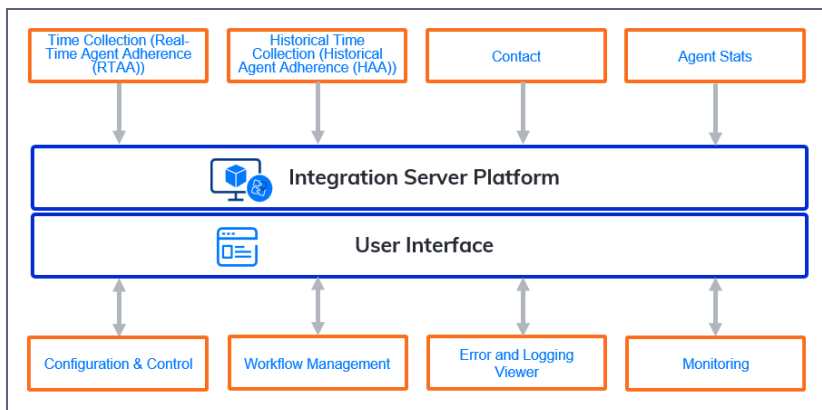
[Integration Server packages \(page 87\)](#)

Integration Server features

Integration Server provides several advantages by integrating call center components.

A single installation of Integration Server can simultaneously integrate multiple Automatic Call Distributors (ACD), Computer Telephony Integration (CTI) Servers, Report Servers, and Intelligent Routers within the Workforce Optimization Solution server which accesses and imports agent information, monitors agent adherence, and synchronizes agent data from multiple sources.

In addition, the Integration Server includes error detection and logging features, and reporting for easy troubleshooting, and the ability to manage the adapters and interfaces except for the parts which reside on the source systems. The illustration below shows a basic block diagram of Integration Server.



The Integration Server simultaneously supports a variety of technologies, including:

- Remote configuring and monitoring
- Simultaneous support of multiple types of data sources
- Historical data import
- Dynamic report importing workflow management
- Diagnostics
- Enhanced error logging with user-configurable viewer
- Automatic startup as a service

- Extensible, including custom solutions
- Multi-contact support
- Multi-contact adapters
- Time Collection (Real-Time Agent Adherence (RTAA))
- Historical Time Collection (Historical Agent Adherence (HAA))
- Data Junction
- Agent configuration
- Agent performance data import

Integration Server packages

The integration server, once installed, includes all available integration packages. While all available integration packages are listed, only those for which your organization purchased a license can be configured for your system.

Each integration package contains a set of integration components that are designed to do a specific integration task, including retrieving and manipulating the specified data from the data source. Integration components can be either predefined (come as part of the package) or user specified.

Integration package components include the adapters, interfaces, and timers that are configured for your system.

Adapters and interfaces

All Integration Server adapters and interfaces are currently designed to run on the same machine as the Integration Server.

Each adapter is managed by an adapter manager (one for each adapter instance). All adapter managers are configured on the Integration Server. An adapter manager sends commands or configuration information from the Integration Server to the adapter, and the adapter sends event information to the Integration Server through the Adapter Manager. Each adapter is a separate process.

A description of how to configure individual adapters is provided in these key areas:

Related topics

[Navigating to the Integration Servers \(page 88\)](#)

[Integration packages and server monitoring \(page 90\)](#)

[Integration server package components \(page 93\)](#)

Navigating to the Integration Servers

In the web application, navigate to **Integration Management > Integration Server > Integration Servers** to display the list of integration packages.

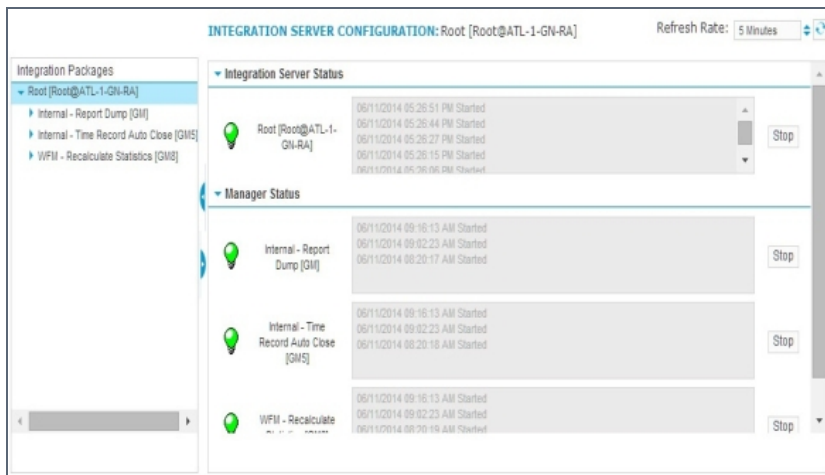


The screenshot shows the 'Integration Management' web application. The top navigation bar includes 'INTEGRATION MANAGEMENT', 'INTEGRATION SERVER', 'DATA SOURCES', and 'SCORECARDS SOURCES'. The 'INTEGRATION SERVER' tab is selected, and the sub-tab 'Integration Servers' is active. Below the navigation bar, the 'INTEGRATION SERVERS:' section displays a table with the following data:

Server Name	Fully Qualified Server Name	RMI Port	Version
ATL-1-GN-CFA	ATL-1-GN-CFA.lab.local	45731	11.2.0.2890

At the bottom of the table, there are three buttons: 'Edit Configuration', 'Refresh Cache', and 'Export Cache'.

To access the Integration Server you want to view or edit, select the server and click **Edit Configuration**. The Integration Server Configuration page opens.



The screenshot shows the 'INTEGRATION SERVER CONFIGURATION: Root [Root@ATL-1-GN-RA]' page. The page has a 'Refresh Rate: 5 Minutes' dropdown at the top right. On the left, there is a sidebar with 'Integration Packages' including 'Root [Root@ATL-1-GN-RA]', 'Internal - Report Dump [GMI]', 'Internal - Time Record Auto Close [GMS]', and 'WFM - Recalculate Statistics [GMS]'. The main content area is divided into two sections: 'Integration Server Status' and 'Manager Status'. Each section contains a list of tasks with their status (indicated by a light green bulb icon), start times, and a 'Stop' button. The 'Integration Server Status' section shows tasks for 'Root [Root@ATL-1-GN-RA]' starting at 06/11/2014 05:26:51 PM. The 'Manager Status' section shows tasks for 'Internal - Report Dump [GMI]', 'Internal - Time Record Auto Close [GMS]', and 'WFM - Recalculate' starting at 06/11/2014 09:16:13 AM.

Integration Configuration Page overview

The Integration Server is the highest level component in the hierarchy shown in the Integration Package pane.

When the top level (Integration Server) is selected on the left (this level is also referred to as root level), you also see the machine name displayed near the top of the right window.

The content and structure of the Integration Server is controlled by a set of pages.

Monitor: At the Integration Server level, the Monitor page is used to check the status of the server and integration packages. It also allows you to control the operation of the Integration Server and the integration packages.

Configure: At the Integration Server level, the Configure page is used to set up the description of the Integration Server. It also displays the number of integration packages for which you are licensed, and allows some advanced configuration parameters to be set.

Workflow: At the Integration Server level, the Workflow page is used to configure the Integration Server with one to 15 integration packages.

Stop/Start: This button is used to stop the related integration component. Click the button to stop the process. When the process is stopped, a red stop-sign icon appears on the left of the page in line with the process. When you stop a sub task, the server and all other sub tasks remain active. However, when you stop the server, you also stop all of the server's packages.

Status Light: A status light appears to the left of the server or a package. If a red or yellow light is displayed, go to the log and read the message to determine the cause. A red light means that the latest status message shows an error. A yellow light means that there has been an error within the last ten messages. The status light will turn green when there is no error in the last ten messages.

Integration packages and server monitoring

An integration package is a set of integration components bundled together to act as a unit. Together, these components accomplish the specific task that the package was designed to do.

An integration package can be either generic or vendor-specific.

For instance, you might have one or more integration packages which collect contact statistics from your data source(s). You will have several integration packages which are designed to accomplish specific tasks within the Workforce Management package.

Integration packages can be started/stopped in the same way as the server.

To make the integration package run on an ad hoc basis, you can click **Import Now** to cause the package to run on demand.

Monitor page

At the package level, the Monitor page displays the status of the package and its components. You can also use this page to control the operation of the package.

Configure page: At the package level, you use the Configure page to set the description of the package and to set the path to the data source. You also use it to configure the plug-ins.

Data Source page

Not all packages use the Data Source page. For those that do, you use the Data Source page to select the system, ACD, and other values, from which the Integration Server will retrieve employee information. You select the data source from a pull-down list. You can also enter a short description of the data source, and add a new data source or rename a data source.

Workflow page

At the Package level, you use the Workflow page to set up the task managers and configure them with a set of integration functions/components arranged in a specific order. You can set up the integration tasks and their components in a workflow in various ways as needed to correctly convert and import the file into the database.

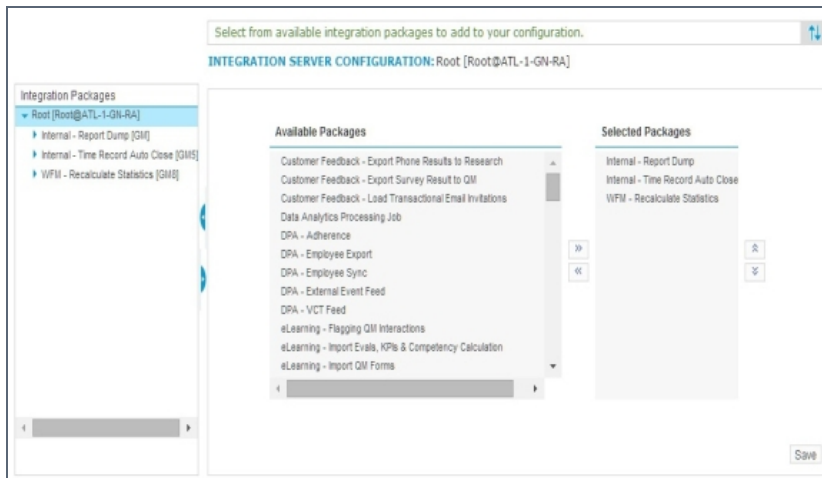
Related topics

[Navigating to the Integration Servers \(page 88\)](#)

[Typical integration packages \(page 91\)](#)

Typical integration packages

To view the list of available packages, and those already selected for your solution, click the Workflow page.



If your Workforce Optimization system configuration includes such server roles as the Framework Database server role or the QM Database server role, certain adapters are added automatically to your integration server.

For example:

- If the Framework Database server role was configured for your system, the Report Dump and Recalculate Statistics adapter are automatically added.
- If the QM Database server role was configured for your system, the Unified User Management adapter is automatically added.

These adapters ensure that your system functions correctly.

If you plan to make changes that affect these adapters on your integration server, contact your application consultant.

Some typical packages that are included for a Workforce Management solution include:

- **Report Dump:** Runs queries and populates data tables to accelerate report calculations.
- **Time Record Auto Close:** Closes time records that have been open beyond the acceptable limits.
- **Staffing Calculator:** Calculates actual staffing based on time records.
- **Data source specific CSI integrations:** Collects actual contact center statistics (like contact volume, AHT, service level, and other statistics) from the specific data source at regular intervals.
- **Data source specific Time Collection integrations:** Collects actual employee state data (like login, logout, wrap-up, not ready, and other data) from the specific data source through a real time data stream.

There are many other integration packages available, including packages to export schedules, employee data, or time records into files, and packages to collect employee performance statistics for scorecards. Note that integration packages are also sometimes called Adapters.

Each integration package (adapter) has its own user guide. These are available in the Adapters folder on the Documentation DVD that was shipped with your software.

Related information

Comprehensive listing of packages and how to configure them (*Workforce Management Administration Guide*)

Integration server package components

Every integration server package includes the following components that manage the function that the selected integrated package performs within the system.

- Batch extender (or other extenders and converters)
- Timer

Related topics

[Extenders and converters \(page 93\)](#)

[Timers \(page 94\)](#)

Extenders and converters

Each integration package has a batch extender component, which starts the processes that perform a specified task and then exits. The process is triggered by the adapter manager. When you select an integration's batch extender component, the Configure page displays on the right panel.

CONFIGURE: Auto Close Adapter [BatchExtender6]

Integration Packages

- Root [Root@ATL-1-GN-RA]
 - Internal - Report Dump [GM]
 - Internal - Time Record Auto Close [GMS]
 - Auto Close Adapter [BatchExtender6]**
 - Timer [Timer7]
 - WFM - Recalculate Statistics [GMS]

Properties

Description: BatchExtender6

Local Adapter ☒ Remote Adapter ☐

Timeout (sec): 36000

Command Line: java.exe -jar Plugins\AutoClose\AutoClose.jar

Working Directory:

☒ Integration Server Adapter

Advanced Configuration

Extender Configuration

Adapter Configuration

Key	Value
LOOKBACK_DAYS	30
VERSION_INFO	
USER_NAME	Auto Close Adapter

Save

On this page you can set the command line to run the process and the maximum time to run. For some of the integration packages, the extender command line is straightforward. Others will have additional configuration parameters, such as an offset.

The timer component triggers the integration package which in turn, starts the batch extender which runs the process.

When the Batch Extender completes, it sends a Completed indicator to Integration Server.

If the Batch Extender fails, it sends a Failed indicator to Integration Server.

In either case, the status is displayed on the Monitor page of the package.

When the Batch Extender component times out while the process is still running, the Batch Extender shuts down the process and sends a Failed error message.

Related topics

[Navigating to the Integration Servers \(page 88\)](#)

Related information

Extenders and converters (*Workforce Management Administration Guide* and individual adapter guides)

Timers

Timers are clocks that trigger the integration package to run. Most integration packages are established to run on timers when installed. (Continuous Extenders do not since they run continuously.) Whenever possible, you should avoid setting the same time for multiple integration packages.

Data source configuration

This section describes how to configure data sources.

Topics

About data sources	96
Creating and editing data sources	97
Working with data source groups	158
Skills mapping	162
Activity mapping	163
Map employees to data sources	165
Creating and editing reason codes	168
Working with operations in Workforce Management	171

About data sources

Data sources are used with various applications within the system and Workforce Optimization Suite, such as Workforce Management, Scorecards, Quality Monitoring and Interactions and Analytics.

Data sources are third-party systems, such as private branch exchanges (PBXs) and CTI Middleware Servers, that generate employee state, device state, and data change events.

When used with the Recorder application, these make business decisions on the interactions to record based on the events supplied by the Integration Service. They also provide business views of interactions based on different logic. Data sources consist of phone systems with associated employee IDs and extensions. Data source also use email systems, Recorder pages, and more.

Creating data sources

Before you can associate users to data sources, you must first create the data sources.

Related topics

[Creating and editing data sources \(page 97\)](#)

[Creating data sources \(page 98\)](#)

[Editing a data source \(page 153\)](#)

[Creating a parent-child relationship between data sources \(page 153\)](#)

[Importing data source configuration \(page 155\)](#)

[Exporting data source configurations \(page 156\)](#)

[Deleting a data source \(page 157\)](#)

Configuring skills mapping, employee mapping and reason codes associated with data sources

Once a data source is created, from the System Management's **Data Sources** area, and depending on the type of data source you had created, you can create and edit data source groups, skills mappings, activity mappings, employee mappings and reason codes.

Related topics

[Creating or editing a data source group \(page 158\)](#)

[Creating or editing skills mapping \(page 162\)](#)

[Creating and editing employee mappings \(page 166\)](#)

[Create and edit reason codes \(page 168\)](#)



For each data source type, a different set of additional configurable features may be shown. For example, with some data source types, such as **Phone**, once you have created the data source, you can then create and edit data source groups, employee mappings and reason codes.

Creating and editing data sources

Data source configuration pages are entered in one of two ways:

Integration Management module

This module generally contains data sources that are used in WFO/Interactions applications:

- Phone (also used with Recording Management)
- Operations
- Outsourcer
- Quality
- Text Analytics

Recording Management module

This module contains data sources used with Recording Applications.

- Phone
- Dialer
- LAN
- Radio
- Trader
- Application

Depending on licensing and your system configuration, you can create the following types of data sources:

- **Dialer:** This data source is associated with another primary Phone data Source to allow predictive dialing of phone numbers automatically, depending on the availability of employees and the response from called party numbers. Dialer switches thus increase the amount of time an employee spends communicating instead of waiting. Before you create this data source, you must create a Phone data source (see below).

See [Creating Dialer data sources \(page 118\)](#).

- **LAN (Screen): Used for screen captures (also sometimes referred to as screen recording).**

See [Creating LAN \(Screen\) data sources \(page 127\)](#).

- **Operations: When licensed for Workforce Management, used for Financial Services Operations data, particularly for volume arrivals and events.**

See [Creating Operations data sources \(page 129\)](#).

- **Outsourcer:** For contact centers that share calls across their own sites and outsourced centers, this data source allows outsourcers' schedules to be imported back into the contact center's model allowing an increased level of coordination.

See [Creating OutSourcer data sources \(page 130\)](#).

- **Phone:** To set up voice recording you must create a phone data source. A phone data source encapsulates information related to the target to be recorded, specifically the switch type, and the seating arrangement of employees using the phones within the call center.

See [Creating Phone data sources \(page 132\)](#).

- **Radio:** This data source is used with Recording applications.

See [Create a Radio data source \(page 145\)](#).

- **Application:** This data source is used with Recording applications.

See [Creating Application data sources \(page 99\)](#).

- **Text Analytics:** A Text Analytics Data Source is used to support text analytics projects for interactions.

- **Trader:** A Trader Data Source is used to support call recording in a financial trading environment.

See [Creating Trader data sources \(page 149\)](#).

If you are licensed for Recorder applications, entering data source information allows your CTI server to be recognized by the data source and thereafter be configured by Recorder Manager or Enterprise Manager.

If you are working with Phone or LAN data sources, you can also export and import configurations for these data sources to an external file that can be imported into another system:

- **Exported** data includes Extensions, Associations, and Groups (for a Phone data source), and Workstations, Groups, and Workstation Associations (for a LAN data source).
- **Imported** data includes Extensions, Associations, and Groups (for a Phone data source), and Workstations, Groups, and Workstation Associations (for a LAN data source). These features allow you to reuse settings from previous versions or from other sources.

Related topics

[Creating data sources \(page 98\)](#)

[Editing a data source \(page 153\)](#)

[Creating a parent-child relationship between data sources \(page 153\)](#)

[Importing data source configuration \(page 155\)](#)

[Exporting data source configurations \(page 156\)](#)

[Deleting a data source \(page 157\)](#)

Creating data sources

To create data sources, follow the instructions for each data source type. Note that once you've selected a data source type, configured it, and saved it, you cannot later edit the data source type

itself.

Related topics

[Creating Dialer data sources \(page 118\)](#)

[Creating LAN \(Screen\) data sources \(page 127\)](#)

[Creating Operations data sources \(page 129\)](#)

[Creating OutSourcer data sources \(page 130\)](#)

[Creating Phone data sources \(page 132\)](#)

Creating Application data sources

Application data sources are for capturing *voice calls, video calls, text and email messages, and video meetings* (including screen share and chat messages) from cloud platforms and multi-channel platforms.



The **Lync** application data source subtype is no longer supported. You cannot create a new **Lync** data source. Existing **Lync** data sources continue to work as is. Using **Skype** instead of **Lync** is recommended.

The **External Recorder** application data source sub type is the only sub type not associated to a Recorder Integrations Service server role. A user installing the Automated Verification 15.2 Capture Verification application creates an **External Recorder** data source to create collectors for switches recorded by a third-party recorder.

Some types of application data sources only include a subset of the following settings:

1. In Enterprise Manager, click **Recording Management**. Under **Data Sources**, click **Settings**.
2. Click **Create Data Source**.
3. As the **Type**, select **Application**.
4. As the **Switch/Sub Type**, select the type of application or server that is the source of data to be recorded.
5. Click **Select**.
6. Enter a **Name** for the data source.
7. Specify the **Organization** to which you want to associate the data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.
8. Type a **Description** (optional) for the data source.
9. Select a **Time Zone**.
10. A **Data Source Parent** option is available only for the Microsoft Teams data source Sub Type. This option does not display in the user interface if the Microsoft Teams data source is already a parent data source.

In a multi-tenant enabled environment, one recording BOT serves multiple Microsoft Azure tenants. In this scenario:

- The recording BOT is deployed inside the Microsoft Azure tenant of the service provider
- Each Microsoft Teams customer has its own Microsoft Teams Azure tenant

To support this deployment, you must configure a parent Microsoft Teams data source for the service provider tenant. Then configure separate child Microsoft Teams data sources for each of the Microsoft Teams customers.

Use the parent data source to:

- Configure the recording BOT settings
- Configure a member group with an association to an IP Recorder server role and a Recorder Adapter Proxy Service server role.

To configure the parent data source, leave the **No Parent** option selected. Then follow the instructions in this topic to configure the Microsoft Teams parent data source settings.

Use the child data source for each customer to configure Employees and their Recording Profiles. To make a Microsoft Teams data source a child data source, select the parent data source from the **Data Source Parent** drop-down.

In a multi-tenant enabled environment, a child data source can have a parent data source that is assigned to the same organization as the child, or is assigned to an organization that is a parent of the organization that is assigned to the child. The child data source can also have a parent data source that is assigned to an organization that belongs to a service provider.

In an environment that is not multi-tenant enabled, a child data source can have a parent data source that is assigned to the same organization as the child, or is assigned to an organization that is the parent of the organization that is assigned to the child.

11. Under **Recorder Settings**, do the following:

- a. For the Amazon Connect, Cisco WebEx Calling, Cisco WebEx Contact Center, Cisco WebEx Meeting Center, Conversocial, Microsoft Teams, Ring Central, Zoom, Zoom Contact Center, and Zoom Phone data sources, the **Seating Arrangement** is specified as **Free** and cannot be changed. Free Seating indicates that employees do not have permanently assigned workstations. They are assigned an Employee ID and can sign in from any location in the call center.
- b. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.
- c. Enable the **Rollback Period (minutes)** setting to ensure that an amount of additional overlapping audio is kept for a period of time, so that in the event of a disconnection it is possible to retrieve it. A rollback period is applicable to systems using Performance Mode (set in the member group) or N+N redundancy. The default value is 15 minutes, and the maximum value is 60 minutes. This setting appears only for the Lync data source sub type.

- d. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system triggers an alarm. The system also stops tracking the call from a CTI perspective, so in CTI-controlled application or performance mode environments this configuration can cause loss of recording. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.



The Integration Service runs maintenance checks every five minutes to close calls that last for more than the length of time specified as the **Long Call Duration**. An alarm indicates that a call was closed because it was too long. These maintenance checks are not run more frequently to avoid imposing an extra load on the system. Therefore it can take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.

- e. **Long Hold Duration (minutes)**— This setting allows you to specify the maximum duration of a single hold in minutes. Any holds over this duration raises an alarm. Enter any number between 1 and 1440, representing the number of minutes. The default is 30.
- f. In Delivery Recording environments, select a **Recording Resource Allocation Behavior** (in Interception Recording environments, skip to the next step). This setting appears only for the Lync data source sub type.
- **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of the data source, member group, and extension list settings.
 - **LineFirst**—The Lync Proxy service attempts to record an agent on the Recorders with which it was associated in the Member Group. If that fails, it attempts to allocate the resources to any other Recorder on that same data source. This setting is the default.
 - **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated to the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it does not record the call. By recording calls on a recorder co-located with the PBX for employees taking calls on a remote site, using this setting reduces WAN traffic.
- g. **Contact Policy Type**—This setting allows you to set the call stitching method.
- **Follow the call**—When follow the call is enabled, there is one contact that includes all audio from the beginning of the call to the end. This setting is the default.
 - **Backoffice - Contact per call**—Enables the “Back office” style of stitching, which creates sessions/interactions based on CTI calls. If one employee is on two calls at the same time (for example, a customer call and a consultation call), the system creates two sessions/interactions. This setting is used more often in trading environments rather than contact center environments.
- h. **Recorded Platform** - If you have selected **External Recorder** as the **Switch/Sub Type**, use this setting to specify the switch type.
- i. **Session Auditing Policy**—Defines the type of session/interaction that should be marked and kept in the system. “Disabled” (the default) only marks sessions/interactions with some kind of content. Two other options create a basic entry in the database for calls that occurred but were not recorded: “Missed Recordings” marks calls that ought to have been recorded, but were not, while “Full Switch” marks all sessions/interactions for which we receive CTI without recording

(for example, calls that were blocked, or interception calls that were met with a busy tone or unanswered ringtone). You can then search for these types of interactions in the Portal. You can replay an interaction when the interaction is complete. It is not necessary to wait for the entire contact to complete to replay an interaction.

- j. **Recorder Allocation based on Audio Location**—Use this setting in a SIP-based VoIP delivery environment to control how Recorders are selected to record calls. This setting ensures that each call is recorded by a Recorder local to the media gateway at which the call arrives. This setting is designed primarily for environments where recording occurs at multiple sites and each site has its own gateway.

Use this setting in conjunction with either a Gateway Side Correlation Pool member group or an IP Extension Pool member group configured for the data source. Within these member groups, you must specify the IP addresses or host names of the phones associated with the member group in the IP Network Region configuration.

The Recorder Allocation Based on Audio Location setting instructs the system to examine the IP address in a SIP message. The system then compares this address to the addresses listed in the IP Network Region settings of the Gateway Side Correlation Pool or IP Extension Pool member group associated with the data source.

If an address in the SIP message matches one of the addresses specified in the member group IP Network Region settings, the system routes the call to a Recorder associated with that member group.

The options for this setting are:

- **Inactive**—The system attempts to record the call. The system does not use an address found in a SIP message to route the call to a particular Recorder. This setting is the default.
- **From Signaling**—The system examines the SIP header section of the SIP Invite. The system compares the address found in a SIP header field (such as From, Contact, Via, or Socket) to the addresses configured in the member group IP Network Region settings. If there is a match, the system routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded.
- **From Media**—The system examines the SDP message attached to a SIP Invite. The system compares the IP addresses found in the SDP message to the addresses configured in the member group IP Network Region settings. If there is a match, it routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded. This option does not work if SIP operates in Delayed-Offer mode.

This setting works with the **Recording Resource Allocation Behavior** setting to determine recording behavior. If the **Recording Resource Allocation Behavior** setting specifies:

- **IgnoreLine**—The system acts as if the Inactive setting is selected for this setting. If either the From Signaling or From Media is selected, those settings are ignored. In this case, any Recorder associated with the data source can record the call.
- **LineFirst**—The system makes two attempts to record the call using the address obtained from the SIP message. If the system cannot route the call to a Recorder using the SIP message address, any Recorder associated with the data source can record the call.

- **LineExclusive**—If the system cannot successfully route the call to a Recorder using the address from the SIP message, the call is not recorded. In this case, the system raises an alarm.
- k. **Video Recording Mode** — Select one of the following options (this setting appears only for the Lync data source sub type):
- **Start On Trigger** - Do not record video calls for the employees associated with this data source until a recording rule is triggered or an external API command starts recording. Video recording starts whenever the call starts, but video that came before the recording trigger is deleted.
 - **Application Controlled** - Record every video call for every employee associated with this data source, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start of the call to the end.
 - **Do Not Record** - Do not record video calls for employees associated with this data source. Recording rules are ignored and cannot trigger the recording of video calls.
 - **Record** - Record all video calls for all employees associated with this data source. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
- l. **Timeout for clearing idle chats (minutes)** - This setting appears only for the NENA i3 Text data source sub type. Set the threshold (in minutes) for closing contacts for idle chats. An idle chat is a chat with no chat activity for which an End Call event has not been received. When this threshold is crossed with no chat activity, the contact for the conversation is closed and recorded. This setting supersedes the timeout setting in the Interaction Capture server role Advanced Settings. The default setting is 15 minutes. The setting can be in a range from 5 to 480 minutes.
- m. **Default Text Language** - Specify the default language assigned to text interactions when the language is not provided by the text source.
- n. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:
- **Disabled:** No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always:** Sensitive customer information is obscured.
 - **In Fallback:** Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
- o. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:

- **Disabled:** The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.
 - **In Fallback:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.
- p. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
- **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.
- q. **Alarm - Device Not Recorded Call Count** - The number of calls for a configured device that must fail to record before triggering the Device Not Being Recorded alarm. The default is one failure.
- r. **Alarm - Device Not Recorded Duration (milliseconds)** - Failed call durations under this threshold will not count against the Alarm - Device Not Recorded Call Count. The default is 15000 (15 seconds).
12. For NICE CXone, under **NICE CXone Kafka authentication**, configure the following:

Field	Description
Broker server hosts	Specify a comma-separated list of Kafka broker hostnames and ports provided by NICE CXone for event streaming.
Topic	Specify the Kafka topic name for the NICE CXone event stream consumed by this data source.
Consumer group ID	Specify the Kafka consumer group identifier provided by NICE CXone for consuming the event stream.
SASL/SCRAM username	Specify the username generated by NICE CXone for authenticating to the Kafka event stream.
SASL/SCRAM password	Specify the password associated with the SASL/SCRAM username.

13. The **Vendor and Filter** settings appear only for the NENA i3 Text data source sub-type. Under **Vendor and Filter** complete these fields:
- a. **Vendor** - Select the vendor (either VESTA or Solacom) from which this data source is expected to receive NENA i3 LogRequest events.
 - b. **Filter Element Name** - Specify the name in a name-value pair that appears in incoming LogEvent request elements. This name-value pair is used, together with the **Vendor** setting, as the filter for processing or ignoring a request. For example, enter "AgencyId". This entry is case-sensitive and must be exactly the same as the element name appearing in the LogEvent XML.

This field cannot be blank. The maximum number of characters allowed for this field is 250.

- c. **Filter Element Values** - Specify the value in a name-value pair that appears in incoming LogEvent request elements. This name-value pair is used, together with the **Vendor** setting, as the filter for processing or ignoring a request. This field supports wildcard and multiple value matching. Separate multiple values with a semicolon. For example, enter "psap1.south.la.com;*.north.la.com". This field cannot be blank. The maximum number of characters allowed for this field is 250.
14. When the customer has a proxy host for their Amazon Connect, Ring Central RingEx, Zoom Meetings, or Zoom Phone systems, in the **Proxy Settings** section, configure the following:
 - a. **Proxy**: Select this option when the tenant uses a proxy host for connection to the internet.
 - b. **Proxy Scheme**: Specify the protocol used by the proxy server to authenticate and manage client requests, such as HTTP or HTTPS.
 - c. **Proxy Host**: Enter the fully-qualified domain name (FQDN) of the proxy server.
 - d. **Proxy Port**: Enter the port number used for communications with the proxy server. The specified port cannot be in use by any other application or adapter on the local server.
 - e. **Proxy Username**: Enter the username the data source will use to authenticate with the proxy server.
 - f. **Proxy Password**: Enter the password for the specified username.
 - g. **Non Proxy Hosts**: Enter the domain names (FQDN) of the host servers that should bypass the proxy server, separated by commas. Requests to these hosts will connect directly to the internet instead of through the proxy. You can use the wildcard * to specify multiple server domains. For example, *.example.com will match all subdomains of example.com.
15. In the **Default Employee** section, specify the employee to be associated to a recording that has no employee associated to it.

There are situations where recordings will not have employees associated to them. Examples include:

- IVR recordings where there is no employee or phone device
- Back office environments where phones are shared and not associated to a specific employee

Assigning a **Default Employee for Interactions** to a data source provides a way to provide replay access to these recordings. When a **Default Employee for Interactions** is configured, any recordings made for the data source that have no explicit user associated are associated to the **Default Employee for Interactions**.

First, select the **Organization** to which the **Default Employee for Interactions** belongs, and then select one employee as the **Default Employee for Interactions**.

You cannot select an employee who has a configured end date as the **Default Employee for Interactions**. Also, you should not select an employee who will soon move or transfer to a different organization as the **Default Employee for Interactions**.

Once an employee is selected as the **Default Employee for Interactions**, an error message displays on the data source screen if the employee has been deleted, terminated, or changed to a different organization since the last time the data source was saved.

16. If you selected **Generic** as the switch subtype, expand the **Specific Switch Type** area and, in the **Specific Switch Type** field, specify the type of switch. Consult with our engineers for a list of supported switch types.
17. For a Cisco WebEx Calling data source, under **Cisco WebEx Calling Authentication**, configure the following required settings:
 - a. **Authorization API Base URL** - The base URL (without schema) of the Cisco Authorization API.
 - b. **WebEx Calling API Base URL** - The base URL (without schema) of the platform API for the cloud region where the customer's instance of Cisco WebEx Calling is located.
 - c. **Client ID**: The Client ID for the Cisco OAuth app that is registered for Verint interaction capture.
 - d. **Client Secret** - The Client Secret for the Cisco OAuth app.
 - e. **Refresh Token** - The refresh token that is used to generate a short-lived access token that allows Verint to access the WebEx Calling API.
18. For a Cisco WebEx Contact Center data source:
 - a. For real-time audio capture, in **Global Audio URL**, enter the public URL of the load balancer configured to receive real-time audio streams from Cisco WebEx Contact Center.

This value is provided during deployment of the recording solution.

Format: **https://{host}.{domain}** or **http://{host}.{domain}**

 - **host** — Load balancer hostname
 - **domain** — Domain of the load balancer URL (must match the Data Exchange Domain configured in the Cisco WebEx Service App)
 - b. For real-time and post-call audio capture, configure the **Cisco WebEx Contact Center Authentication** settings:
 - **Authorization API Base URL** — The base URL of the Cisco Authorization API used to generate access tokens for Contact Center APIs. Maximum length is 500 characters.
 - **Contact Center API Base URL** — The base URL of the Contact Center APIs. Maximum length is 500 characters.
 - **Client ID** — The client ID for the registered application that accesses the APIs. Maximum length is 500 characters.
 - **Client Secret** — The client secret for the registered application that accesses the APIs. Maximum length is 500 characters.
 - **Refresh Token** — The refresh token used to generate short-lived access tokens for the Contact Center APIs. Maximum length is 500 characters.
19. For a Cisco WebEx Meeting data source, under **Cisco WebEx Meeting Authentication**, configure the following required settings:
 - a. **WebEx Meeting API Base URL** - The base URL (without schema) of the Meeting APIs. The maximum length is 255 characters. This value cannot be empty.
 - b. **Authorization URL** - The base URL (without schema) of the Cisco Authorization API that is used to generate access tokens that allow access to the WebEx APIs. The maximum length is 255

- characters. This value cannot be empty.
- c. **Client ID** - The client ID for the registered application that will be accessing the APIs. The maximum length is 255 characters. This value cannot be empty.
 - d. **Client Secret** - The client secret for the registered application that will be accessing the APIs. The maximum length is 255 characters. This value cannot be empty.
 - e. **Refresh Token** - The refresh token that is used to generate short lived access tokens that allow access to the Meeting APIs. The maximum length is 255 characters. This value cannot be empty.
20. For Microsoft Dynamics, in the **Authentication Settings** section, enter the following:
- a. **Dynamics Omnichannel Environment URL** - Enter the base URL (without https://) for the customer's Dynamics 365 Omnichannel Organization for Customer Service environment.
Example: myOrganization.api.crm.dynamics.com
 - b. **Tenant ID** - Enter the customer's Microsoft Tenant ID (formerly call the Azure AD tenant ID).
21. For a Twilio data source, under **Amazon Kinesis Settings**, configure the following:
- a. **Twilio Events Stream Name** - This field is required only when the data source is associated to a Recorder Integration Service server role. In this field, specify the Kinesis data stream name that the Recorder Integration Service connects to for real-time agent and call events. This field is required for real-time audio and screen recording. This field is blank by default. The field can have a minimum of one character and a maximum of 1024 characters.
 - b. **Region** - You must select a region from the **Region** drop-down list. In this drop-down list, select the Amazon Web Service (AWS) region hosting the Twilio Events Kinesis Stream. This field is blank by default.
If you select the **Custom Region** option, you must specify the custom region in the **Custom Region** field that follows.
 - c. **Custom Region** - Complete this field only when you have selected the **Custom Region** option from the **Region** drop-down list. Enter only the region code for custom region, not the entire display name. An example of a **Custom Region** value is "ap-south-1" for the region "Asia Pacific (Mumbai) ap-south-1". This field is blank by default.
 - d. **Specify Application Credentials** - To enable the use of specific application credentials, select this check box. If you select this check box, you must provide the specific application credentials in the **Access Key ID** and **Access Key Secret** fields. If this check box is not selected, the default application credentials are used.
 - e. **Access Key ID** - This field is enabled only when the **Specify Application Credentials** check box is selected. When this field is enabled, enter the user-specified application access key ID. This field is blank by default. The field can have a minimum of 1 character and a maximum of 1024 characters.
 - f. **Access Key Secret** - This field is enabled only when the **Specify Application Credentials** check box is selected. When this field is enabled, enter the user-specified application access key secret. This field is blank by default. The field can have a minimum of 1 character and a maximum of 1024 characters.
 - g. **Specify IAM Role** - Select this check box to use a specific application IAM Role. If you select this check box, you must provide the specific IAM Role information in the **Role ARN** (Amazon

- Resource Name) and **External ID** fields. If this check box is not selected, no role is assumed.
- h. **Role ARN** - This field is enabled only when the **Specify IAM Role** check box is selected. When this field is enabled, enter the user-specified application IAM Role ARN. This field is blank by default. The field can have a minimum of 1 character and a maximum of 1024 characters.
 - i. **External ID** - This field is enabled only when the **Specify IAM Role** check box is selected. When this field is enabled, enter the user-specified application IAM Role External ID. This field is blank by default. The field can have a minimum of 1 character and a maximum of 1024 characters.
 - j. **Role Session Name** - When authenticating by means of an IAM role, you can explicitly configure the role session name in this field. If this name is not configured, a role session name is generated by the adapter.
22. In the **Ring Central Authentication** section, configure the following:
- a. **API Base URL** - Enter the base URL, without the schema, that is used to send the requests to the Ring Central API. The maximum length allowed is 255 characters. This field cannot be empty.
 - b. **Client ID** - Enter the unique client ID for the registered OAuth application that gives the data source access to the Ring Central APIs. The maximum length allowed is 255 characters. This field cannot be empty.
 - c. **Client Secret** - Enter the client secret for the registered OAuth application that gives the data source access to the Ring Central APIs. The maximum length allowed is 255 characters. This field cannot be empty.
 - d. **JWT Token** - Enter the JSON Web token (JWT) that is used to authenticate to the registered OAuth app. The maximum length allowed is 255 characters. This field cannot be empty.
23. **Internal use only.** The Post-Call Cloud settings are for the **External Cloud Recording Configuration** service, and apply to supported Application data sources (currently Amazon Connect). Configuration is performed by Verint Services.



The **Post-Call Cloud Settings** section is always visible on the Application data source, regardless of which recording service is deployed.

When using the **External Cloud Recording Configuration** service, you must configure the Post-Call Cloud Settings, and no adapter is required.

When using the **Recorder** service (on-premises deployments and some cloud deployments), the Post-Call Cloud Settings are ignored, even if configured. To capture post-call audio in these deployments, you must deploy and configure the appropriate adapter (for example, the **Amazon Connect Polling Adapter**).

Do not rely on the Post-Call Cloud Settings when the Recorder service is in use.

The **Post-Call Cloud Settings** include the following fields:

- **Application Name:** Specifies the DynamoDB table name provided by Verint Services for this deployment. The post-call capture service uses this value for checkpointing and post-call event tracking.

This value must exactly match the value supplied by Verint Services.

- **Record Unknown Agents:** Determines whether the system processes post-call interactions when the agent identified in the interaction record cannot be matched to a configured Verint agent.
 - When enabled, the system captures post-call audio and metadata for unmapped or unrecognized agents.
 - When disabled, these interactions are discarded.
 - **Block Fallback Audio:** Controls whether post-call audio is stored when the real-time recording is missing.
 - When enabled, the system blocks ingestion of fallback audio and saves only post-call metadata and tags.
 - When disabled, the system stores fallback audio when required.
24. In the **Twilio Account Settings** section configure the following (**Twilio Account Settings** appear only for the Twilio data source):
- a. **Account SID** - Enter the Twilio Account String Identifier (SID). The administrator gets Twilio to generate an Account SID when creating a Twilio account. The Account SID, along with the Authentication Token, are essentially a master key that can be used to perform any function available in the Twilio API. This field is mandatory when the Twilio data source is associated with an Interaction Capture or a Recorder Integration Service server role. The field can have a minimum of 1 character and a maximum of 1024 characters.
 - b. **Authentication Token** - Enter the Twilio Authentication Token. The administrator gets Twilio to generate an Authentication Token when creating a Twilio Account. The Authentication Token, along with the Account SID, are essentially a master key that can be used to perform any function available in the Twilio API. This field is mandatory when the Twilio data source is associated with an Interaction Capture or a Recorder Integration Service server role. The field can have a minimum of 1 character and a maximum of 1024 characters.
25. For a Genesys Cloud CX Application data source, configure the **AudioHook Settings**:
- a. **Organization ID** — Enter the Genesys Cloud Organization ID used for authentication.
 - b. **API Key** — Enter the API key configured in the Genesys AudioHook integration. This key is required for authentication and must match the API key you entered when creating the AudioHook integration in the Genesys portal.
 - c. **Client Secret** — Optional. Enter the client secret configured in the Genesys AudioHook integration on the Genesys portal. Enter the secret exactly as it appears in Genesys Cloud, typically as a Base64-encoded string.
- The client secret is used to generate a request signature that validates each request. If the secret does not match the value in Genesys Cloud, the system returns a 401 error and rejects the request.
- Note:** AudioHook settings are not required for text capture from digital channels in Genesys Cloud.
26. Configure Verint's response to pause and resume events from Genesys Cloud CX: Under **Genesys Platform API Settings**, select an option from the **Use Pause/Resume Events from Genesys Client** list:

- **No:** Ignore pause and resume events.
 - **Yes for Audio:** Pause and resume audio only.
 - **Yes for Audio and Screen:** Pause and resume audio and agent screen.
27. In the **Voice Stream** section, configure the following (**Voice Stream** settings appear only for the Five9 Voice Stream data source):
- a. **Trust Token** - This field is optional. The Trust Token is a shared secret configured for a given Voice Stream subscription. This token is used by the recording integration to authenticate the CTI and SIP events delivered from Voice Stream.
 - b. **Subscription ID** - The ID of the Voice Stream subscription. This ID is used as a filter parameter for Voice Stream webhook CTI events routing. The value for this ID should be copied from the Voice Stream portal where the Subscription is configured for the customer Voice Stream domain.
28. For an Amazon Connect data source, under **Amazon Kinesis Stream Settings** do the following:
- a. **Contact Trace Records Stream Name:** Required only when the data source is associated with an Interaction Capture Service server role. Enter the name of the Kinesis data stream that the Interaction Capture Service uses for post-call recording retrieval.
 - b. **Agent Events Stream Name:** Required when the data source is associated with a Recorder Integration Service server role. Enter the name of the Kinesis data stream that the Recorder Integration Service uses for real-time agent and call events. This field is required for real-time audio and screen recording.
 - c. **Region:** Choose the AWS region that hosts the Amazon Kinesis Data Stream.
If you select **Custom Region**, complete the following **Custom Region** field.
 - d. **Custom Region:** Complete this field only if you selected **Custom Region** from the **Region** list. Enter the region code, not the full display name. **Example:** **ap-south-1** for "Asia Pacific (Mumbai) ap-south-1."
 - e. **Specify Application Credentials:** Select this check box to use specific application credentials. If selected, enter the credentials in **Access Key ID** and **Access Key Secret**. If not selected, the default credentials are used.
 - f. **Access Key ID:** Enabled only when **Specify Application Credentials** is selected. Enter the application access key ID.
 - g. **Access Key Secret:** Enabled only when **Specify Application Credentials** is selected. Enter the application access key secret.
 - h. **Specify IAM Role:** Select this check box to use a specific IAM role. If selected, enter the role details in **Role ARN** (Amazon Resource Name) and **External ID**. If not selected, no role is assumed.
 - i. **Role ARN:** Enabled only when **Specify IAM Role** is selected. Enter the IAM role ARN (Amazon Resource Name).
 - j. **External ID:** Enabled only when **Specify IAM Role** is selected. Enter the IAM role external ID.
 - k. **Role Session Name:** When authenticating with an IAM role, you can enter a role session name. If not specified, the adapter generates one.

- l. **Pause/Resume Recording:** For post-call recording environments where Amazon Connect handles audio recording, select this option to pass pause and resume commands to Amazon Connect so that both screen and audio recordings are masked during the same time period.
 - m. **Amazon Connect Instance ID:** Enter the instance ID of the Amazon Connect instance. This ID is used when sending pause and resume recording commands.
 - n. **Amazon Connect Multi-party Call Mode** - Enable this option if your Amazon Connect instance supports multi-party calls and enhanced monitoring for voice. This setting must match your Amazon Connect configuration for recordings to work correctly.
29. For a Genesys Cloud CX system that uses an Amazon EventBridge, under **Amazon Kinesis Stream Settings** configure the following:
- a. **Use Amazon EventBridge:** Select this check box when Genesys Cloud events are delivered to an Amazon Kinesis Data Stream via Amazon EventBridge. When selected, other configuration options become available.
 - b. **Agent Events Stream Name:** Required when the data source is associated with a Recorder Integration Service server role. Enter the name of the Kinesis data stream that the Recorder Integration Service uses for real-time agent and call events. This field is required for real-time audio and screen recording.
 - c. **Region:** Choose the AWS region that hosts the Amazon Kinesis Data Stream.
If you select **Custom Region**, complete the following **Custom Region** field.
 - d. **Custom Region:** Complete this field only if you selected **Custom Region** from the **Region** list. Enter the region code, not the full display name. **Example:** **ap-south-1** for "Asia Pacific (Mumbai) ap-south-1."
 - e. **Specify Application Credentials:** Select this check box to use specific application credentials. If selected, enter the credentials in **Access Key ID** and **Access Key Secret**. If not selected, the default credentials are used.
 - f. **Access Key ID:** Enabled only when **Specify Application Credentials** is selected. Enter the application access key ID.
 - g. **Access Key Secret:** Enabled only when **Specify Application Credentials** is selected. Enter the application access key secret.
 - h. **Specify IAM Role:** Select this check box to use a specific IAM role. If selected, enter the role details in **Role ARN** (Amazon Resource Name) and **External ID**. If not selected, no role is assumed.
 - i. **Role ARN:** Enabled only when **Specify IAM Role** is selected. Enter the IAM role ARN (Amazon Resource Name).
 - j. **External ID:** Enabled only when **Specify IAM Role** is selected. Enter the IAM role external ID.
 - k. **Role Session Name:** When authenticating with an IAM role, you can enter a role session name. If not specified, the adapter generates one.
30. The **Zoom Authentication** settings appear only for the Zoom Phone and Zoom Contact Center data sources.
- Under **Zoom Authentication Settings**, configure the following:

- a. **Zoom REST API Base URL** - Enter the base URL, without the schema, that is used to send the requests to a Zoom API. For example, `api.zoom.us/v2`. The maximum length allowed is 255 characters. This field cannot be empty.
 - b. **Zoom Authorization URL** - Enter the URL, without the schema, of the Zoom OAuth 2.0 endpoint that is used by your server-to-server OAuth app to get access tokens. For example: `https://zoom.us/oauth/token`. The maximum length allowed is 255 characters. This field cannot be empty.
 - c. **Account ID** - Enter the unique account ID for the registered OAuth application that gives the data source access to the Zoom APIs. The maximum length allowed is 255 characters. This field cannot be empty.
 - d. **Client ID** - Enter the unique client ID for the registered OAuth application that gives the data source access to the Zoom APIs. The maximum length allowed is 255 characters. This field cannot be empty.
 - e. **Client Secret** - Enter the client secret for the registered OAuth application that gives the data source access to the Zoom APIs. The maximum length allowed is 255 characters. This field cannot be empty.
31. To capture real-time interactions from a Zoom Contact Center, in the **Stream Recording Settings** section, enter the information that was created when the audio stream integration using Websocket was set up in the customer's Zoom Contact Center:
- a. **Customer ID** - Enter the customer ID exactly as it is configured in the Zoom Integration audio stream. The ID is required for Verint to identify interactions.
 - b. **Profile ID** - Enter the profile ID exactly as it is configured in the Zoom Integration audio stream. The ID is required for Verint to identify interactions.
 - c. **API Key** - Enter the API Key exactly as it is configured in the Zoom Integration audio stream. The key determines the authenticity of messages between Zoom and Verint.
32. Select one of the following **Device IP Configuration** options and enter the corresponding **IP Address**:
- **PBX Side - Near End**—The PBX Side - Near End is the server used to send/receive the control messages to/from the extensions. If you have the same extensions in multiple data sources, you must specify an IP Address or Host Name for the signaling interface server.
Otherwise, the setting is not mandatory, but recommended.
The Recorder uses the source or destination IP addresses or host names of the signaling messages to identify the particular data source with which a call is associated. The recorder does not use any data inside the signaling itself to make this determination. For this reason, the source/destination of the IP packets presented to the Recorder *must be different for each duplicate extension*. Make sure that your network is set up in such a way as to allow for this.
Example
A proxy server in front of separate PBXs using duplicate extensions can cause IP packets to appear as though they are using the same IP address (even though the SIP signaling would indicate otherwise). This will prevent the duplicate extensions from being recorded correctly. For more details, see the section "Recording Duplicate Extensions" in the *Recorder Configuration and Administration Guide*.

- **PSTN Side - Far End**—If you are using SIP Trunk Recording, set PSTN Side - Far End as the Server Type.
This setting is only available for Avaya and Generic switch types, and if you have created a Gateway Side Correlation Pool Member Group, this setting is mandatory.
For details on this, see the “SIP Trunk Recording” section in the *Recorder Configuration and Administration Guide*, or the related online help.
33. Under **Time Zone Settings**, specify a **Local Time Tagging Mode**. Select one of the following options:
 - **Organization** - Select this option to base the time zone tagging on that of the organization. This setting is useful in scenarios where agents are working in different regions. The setting allows you to unify tagging across multiple time zones.
 - **Data Source** - Select this option to base time zone tagging on the time zone specified in step 9.
 34. The **Snowflake Database Authentication** settings appear only for the Conversocial data source.
 - a. **Account Identifier** - Specifies the account identifier for accessing the Snowflake database. This field is required. The maximum account identifier length is 255 characters.
 - b. **Username** - Specifies the username for accessing the Snowflake database. This field is required. The maximum username length is 255 characters.
 - c. **Password** - Specifies the password for accessing the Snowflake database. This field is required. The maximum password length is 255 characters.
 - d. **Database Name** - Specifies the name of the database to access. This field is required. The default setting is CONVERSOCIAL. The maximum database name length is 255 characters.
 - e. **Database Warehouse Name** - Specifies the name of the database warehouse to access. This field is required. The default setting is GBID_7. The maximum database warehouse name length is 255 characters.
 - f. **Database Schema Name** - Specifies the name of the database schema to access. This field is required. The default setting is PUBLIC_V3. The maximum database schema name length is 255 characters.
 35. The **BOT Settings MS Teams** section appears only for the Microsoft Teams child data source in a Multi-Tenant SaaS environment.
 - a. **Tenant ID** - Specify the tenant ID where the BOT registered.
 36. The **BOT Settings Authentication** section appears only for the Microsoft Teams data source. In the **BOT Settings Authentication** section do the following:
 - a. **BOT Tenant ID** - In a Multi-Tenant SaaS environment, specify the tenant ID where the BOT registered.
 - b. **BOT Application ID** - Specify the application ID created during BOT channel registration.
 - c. **BOT Application Secret** - Specify the secret created during BOT permission configuration.
 - d. **Redundant BOT Application ID** - Specify the application ID created during redundant BOT channel registration.
 - e. **Redundant BOT Application Secret** - Specify the secret created during redundant BOT permission configuration.

37. The **BOT Settings Media** section appears only for the Microsoft Teams data source. Under **BOT Settings Media** do the following:
- Media Control Internal Port** - Specify the media platform instance internal port. The default port is 8445.
 - Media Control Public Port** - Specify the media platform instance public port. The default port is 8445.
 - Media Port Range Begin** - Use this setting in combination with the **Media Port Range End** setting to define a range of 1000 ports or more for media. (You must specify a port range of at least 1000 ports for media.) The port number specified should fall within the range of 16384 to 65535. This setting specifies the port that begins the range of ports. For example, you can specify 17000 for the **Media Port Range Begin** setting and 18000 for the **Media Port Range End** setting.
 - Media Port Range End** - Use this setting in combination with the **Media Port Range Begin** setting to define a range of 1000 or more ports for media. This setting specifies the last port in the range of ports. See **Media Port Range Begin** for details.
 - Unmixed Audio** - Use this setting to request unmixed audio from Microsoft Teams. Select the check box to request unmixed audio. Do not select the check box to request mixed audio. By default, the check box is not selected and mixed audio is requested.
38. The **BOT Settings Signaling** section appears only for the Microsoft Teams data source. Under **BOT Settings Signaling** do the following:
- Default End Point Internal Port** - Specify the BOT channel registered port for an incoming call alert. The default port is 9440.
 - Default End Point Public Port** - Specify the BOT channel registered port for an incoming call alert. The default port is 9440.
 - Call Control End Point Internal Port** - Specify the Microsoft Teams to BOT signaling port for individual call session management. The default port is 10100. This port is used to create the call control listening URL.
 - Call Control End Point Public Port** - Specify the Microsoft Teams to BOT signaling port for individual call session management. The default port is 10100. This port is used to create the call control base URL, which is used to build the graph client.
 - Service Base URL** - This URL is used to build the graph client. The default setting is <http://graph.microsoft.com/beta>.
39. For a Google UJET contact center, enter the following values that originate in the Developer Settings of the customer's UJET account:
- Under **Google UJET Settings - API Credentials**:
 - **API Name**: Enter the name of the API credential created in the customer's UJET account in the Developer Settings.
 - **API Token**: Enter the token for the customer's UJET API credential.

- **REST API Base URL:** Enter the URL of the API endpoint used by Google UJET REST APIs.
Example: **https://CustomerServer.ujet.co/manager/api/v1/agents**, where *CustomerServer* is the name of the customer's UJET server.
- b. Under **Google UJET Settings - QM Call Events**:
 - **User name:** Enter the user name specified in the Session Data Export page for QM Call Events.
 - **Password:** Enter the password specified in the Session Data Export page for QM Call Events.
 - c. Under **Google UJET Settings - SIPREC Call Events**:
 - **User name:** Enter the user name specified in the Session Data Export page for SIPREC Call Events.
 - **Password:** Enter the password specified in the Session Data Export page for SIPREC Call Events.
40. Under **Associated Skype Installations**, select one or more check boxes to associate this data source with the Skype Filtering Service on a Skype Front End Server. This setting appears only for the Skype data source sub type.
The Skype Filtering Service gathers information about Skype interactions and distributes it to the following components:
 - Media Proxy, part of the Recorder platform. When an on-premises call should be recorded, the Filtering Service chooses a Media Proxy based on priority, subnets, and health status. The Media Proxy Service starts and stops proxying of Skype calls based on these requests.
 - Media Collector Service, responsible for forwarding RTP traffic from the Edge Server to one or more IP Recorders.
 - Recorder Integration Service, which uses the SIP information it receives to provide more detailed metadata and follow-the-call.
 - Interaction Capture Service, which receives and records chat-based interactions.
 41. For a custom solution that uses the Generic Application capture source, under **Associated Installations**:
 - a. Select the tenant's EDM Capture Module.
 - b. For post-call ingestion of media (such as audio, video, e-mail, chat), select the **Interaction Capture** service.
 - c. For real-time capture of media (such as audio or video), select the **Recorder Integration Service**.
 42. Under **Associated Integration Service Installations**, select the node that provides the Recorder Integration Services for this data source. This server role is required to capture real-time interactions.
A data source may only be associated with a single Recorder Integration Service server (or pair in the case of redundant Recorder Integration Service servers).



In a multi-tenant enabled environment, the tenant name associated to each Site Group, Site, and Server appears beside the Site Group, Site, and Server name on the right side of the Installations tree.

43. Under **Associated Interaction Capture Installations**, select the server role that provides the Interaction Capture services for this data source. This server role is required to ingest post-call interactions, including chat sessions. This setting does not appear for all data source subtypes.
44. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system—this should be done only in consultation with Field Engineers.
 - a. For a data source that connects to a line-side SIPREC adapter:
 - i. In **Key**, enter **SIPREC.StationCountryCode**.
This field is case sensitive; enter as shown.
 - ii. In **Value**, enter the country code configured on your stations.
Enter a single code between one and five digits long. It can include the numbers 0-9, but must omit the plus (+) sign. If your organization has stations in multiple countries, you need a data source for each country.
 - b. For a Twilio data source:
 - i. In **Key**, enter **WEBSOCKET_TARGET_URL**.
This field is case sensitive; use all capitals as shown above.
 - ii. In **Value**, enter **wss://<FQDN_LB_Frontend>/twilio/v1**,
where *FQDN_LB_Frontend* is the fully-qualified domain name of the load balancer. In the Twilio portal, you can find this URL on the **Frontend IP configuration** page. Twilio needs this URL to connect to the Verint Twilio Media Adapter.
45. Click **Save**.

Related topics

[Configure a Microsoft Teams child data source \(page 116\)](#)

Configure a Microsoft Teams child data source

Configure a Microsoft Teams child data source for each Microsoft Teams customer that has its own Microsoft Teams Azure tenant.

Procedure

1. In Enterprise Manager, click **Recording Management**. Under **Data Sources**, click **Settings**.
2. Click **Create Data Source**.
3. As the **Type**, select **Application**.
4. As the **Switch/Sub Type**, select Microsoft Teams.
5. Click **Select**.
6. Enter a **Name** for the data source.
7. Specify the **Organization** to which you want to associate the data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

8. Type a **Description** (optional) for the data source.
9. Select a **Time Zone**.
10. Select the **Data Source Parent**. When you select a Data Source Parent, the data source you are configuring becomes a child data source. The data source parent contains the Recorder Settings configuration and the BOT recording configuration. These configurations are passed from the tenant data source to the child data source and are not configurable for the child data source.

In a multi-tenant enabled environment, a child data source can have a parent data source that is assigned to the same organization as the child, or is assigned to an organization that is a parent of the organization that is assigned to the child. The child data source can also have a parent data source that is assigned to an organization that belongs to a service provider.

In an environment that is not multi-tenant enabled, a child data source can be associated to any organization and any parent data source.
11. Under **BOT Settings MS Teams**, specify the **Tenant ID** for the Microsoft Teams customer tenant. The Tenant ID in each call request identifies the tenant to which the call belongs.
12. You cannot select an associated Recorder Integration Service server role or an associated Interaction Capture Service server role for a child data source. These associations are inherited from the parent data source. The associations are visible in the user interface after you click **Save** to save the child data source settings.
13. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system—this should be done only in consultation with Field Engineers.
14. Click **Save** to save the child data source settings.



You must configure the Employees and the Recording Profiles for the child data source.

Member group configuration when creating a new child data source or changing the child or standalone status of the data source

A Microsoft Teams data source with **No Parent** selected as the **Data Source Parent** is a standalone data source. A Microsoft Teams data source with a data source specified as the **Data Source Parent** is a child data source. A Microsoft Teams data source that does not show the **Data Source Parent** setting in the user interface is a parent data source.

Note the following regarding member group configurations when creating a new child data source, when changing a standalone data source to a child data source, and when changing a child data source to a standalone data source.

When creating a new child data source:

- The child data source is automatically assigned the same member groups as the parent data source.
- Member groups cannot be modified from the child data source.

When changing a standalone data source to a child data source:

- You must delete all member groups from the standalone data source before making the data source a child data source.
- The child data source is automatically assigned the same member groups as the parent data source.
- Member groups cannot be modified from the child data source.

When changing a data source from a child data source to a standalone data source:

- You must define the Recorder Settings and the BOT recording settings for the data source after making it a standalone data source.
- You must assign member groups to the data source after making it a standalone data source.

Related topics

[Creating Application data sources \(page 99\)](#)

Creating Dialer data sources

Dialer data sources are for capturing *voice calls* from an outbound campaign dialer.

Use the following procedure to create a dialer data source.



Unless you are using a standalone dialer deployment, you should create a phone data source before you begin. See [Creating Phone data sources \(page 132\)](#).

For more information about how Phone and Dialer data sources are used and integrated, see the *Recorder Configuration and Administration Guide*.

To create a dialer data source:

1. Navigate to **Recording Management > Data Sources > Settings** and click **Create Data Source**.
2. In the pop-up **Data Source Type** page, do the following:
 - a. From the **Type** drop-down list box, select **Dialer**.
 - b. From the **Switch/Sub Type list box**, select a switch/sub-type.



The data source types available to you are dependent on licensing.

- c. Click **Select**.
3. Type a **Name** for the data source.
 4. Specify the **Organization** to which you want to associate the data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.
 5. Type a **Description** for the data source (optional).

6. Under **Recorder Settings**, do the following:

a. Specify a **Seating Arrangement**—*Fixed, Free, or Hybrid*:

- **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension.
- **Free** seating, the default, indicates that employees do not have permanently-assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
- **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.

b. In a multi-tenant enabled (cloud) environment, the Service Provider Administrator (SPA) can specify a **Maximum Allowed Extensions** value for this data source. The Maximum Allowed Extensions setting limits the number of extensions a Tenant Administrator can create for the data source. This setting allows a SPA to prevent tenants from creating more extensions than their assigned capture capacity supports.

If this setting is not set and the data source currently has no extensions associated with it, this setting defaults to 1000 at the time a Tenant Administrator creates the first extension.

In an upgrade scenario, a data source may already have extensions assigned to it. In this scenario, when a Tenant Administrator adds extensions, the system updates this setting to 120% of the existing number of extensions or 1000, whichever is higher. For example, if 2000 extensions are associated with the data source at the time of the upgrade, this setting defaults to 2400 when a Tenant Administrator adds extensions.

This setting does not limit the number of extensions a SPA can create. For example, if the setting is 1000, a SPA can create more than 1000 extensions. If the SPA creates more extensions than this setting specifies, the Tenant Administrator cannot create any extensions.

If a Tenant Administrator configures the maximum number of allowed extensions, the SPA can increase this number to allow the Tenant Administrator to create additional extensions. Before increasing this setting, the SPA should verify that the tenant's environment has the resources necessary to handle the increased load.

c. To save the last employee's settings after the computer is shut down, select the **Persist Agent State on Shut Down (minutes)** check box. Specify the amount of time in minutes for which you want to save the employee's settings. The default is 600 minutes (10 hours).

Data from within this time period is not loaded, while data after this duration has passed, is loaded. Note that if the CTI adapter is down, the following occurs:

- If unselected, all agents on the data source are logged out right away.
- If selected, all agents on the data source are logged out once the number of minutes specified by **Persist Agent State on Shut Down (minutes)** has expired.

d. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.

- e. Enable the **Rollback Period (In minutes)** to ensure that a recording is kept for a certain amount of time before deletion, so that in the event of a disconnection it is possible to retrieve it. The default value is 15, and the maximum value is 60.



A rollback period is applicable only to Performance Mode (set in the IP Extension Pool member group) and N+N redundancy.

- f. RTP detection is enabled in Performance and Liability fallback modes to prevent audio loss. Coordination between the Integration Service and RTP, using the following settings, ensures that there will only be one recording for a given call:
- **Start Overlay (In milliseconds)**—This threshold indicates the longest amount of audio (from before CTI starts) that will be associated to that CTI call. Anything over this threshold will be treated as VOX.
 - **End Overlay (In milliseconds)**—This threshold indicates the longest amount of audio (after CTI ends) that will be associated to that CTI call. Anything over this threshold will be treated as VOX.
- g. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system will trigger an alarm. The system will also stop tracking the call from a CTI perspective, so in CTI-controlled application or performance mode environments this may cause loss of recording. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.



The Integration Service runs maintenance checks every five minutes to close handset calls that last for more than the length of time specified as the **Long Call Duration**. An alarm indicates when a call is closed because it was too long.

Since these maintenance checks are not run more frequently in order to avoid imposing an additional load on the system, it may take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.

- h. **Long Hold Duration (minutes)**—Indicates the maximum duration of a single hold. Any holds over this duration will raise an alarm. Enter any number between 1 and 3000, representing the number of minutes. The default is 30.
- i. **Recording Resource Allocation Behavior**—This setting is for duplicate streaming solutions, which allow you to distribute recordings across multiple recorders.
- **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of data source, member group, and extension list settings.
 - **LineFirst**—First attempts to record on the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service can't find an associated recorder it will attempt to find any connected recorder with the capacity (whether or not the extension is associated with the recorder). LineFirst provides a way to keep recorders local to the extensions/site. The Integration Service will fail over to another set of recorders if a call can't be recorded locally. If you don't want fail over to another set of recorders, use 'LineExclusive', described below. This is the default.

- **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated to the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it will not record the call.

The “least-utilized” recorder is the one with the most unused capacity. For example, if one recorder has 300 licenses and 50 calls are currently being recorded, and another recorder has with 100 licenses and 10 calls currently being recorded, the capacity left on the recorders are 250 and 90 respectively. The system will attempt to record the next duplicate streamed call on the first recorder.

- j. **Always Report Extension as Primary Extension**—If enabled, the extension field of the session will always be the primary extension on a telephone. If disabled, the extension field will contain the DN/extension that first answered the call. This only affects multiline phones. Enabled by default.
- k. **Contact Policy Type**—This setting allows you to set the call stitching method.
 - **Follow the call**—When follow the call is enabled, there will be one contact that includes all audio from the beginning of the call to the end. This is the default.
 - **Backoffice - Contact per call**—Enables the “Back office” style of stitching, which creates sessions based on CTI calls. If one employee is on two calls at the same time (for example, a customer call and a consultation call), the system creates two sessions. This is used more often in trading environments rather than contact center environments.
- l. **Record Extensions for Internal Calls**—This setting applies to trunk side environments (such as the Avaya switch in trunk-side environment), and hybrid systems where the same data source is used for TDM recording and IP recording (one data source and two member groups). Select this check box to allow the recording of internal calls on selective recording resources.
- m. **Raise Alarm for Out Of Service Devices**—If enabled, the Integration Service will raise alarms for any devices that go out of service. This is currently only available for Cisco JTAPI and Genesys adapters.
- n. **Alarm - Device Not Recorded Call Count**—The number of calls for a configured device that must fail to record before triggering the DeviceNotRecording alarm. The default is 1.
- o. **Alarm - Device Not Recorded (milliseconds)**—Failed call durations under this threshold will not count against the Device Not Recorded Call Count. The default is 15 seconds.
- p. **Enable Nailup Algorithm**—This setting is selected by default, and is used by the Integration Service to identify nailup calls (otherwise, manual configuration of dialer trunks may be required).
- q. **Session Auditing Policy**—Defines the type of session that should be marked and kept in the system. “Disabled” (the default) will only mark sessions with some kind of content. Two additional options will create a basic entry in the database for calls that occurred but were not recorded: “Missed Recordings” will mark calls that should have been recorded, but were not, while “Full Switch” will mark all sessions for which we receive CTI without recording (for example, calls that were blocked, or interception calls that were met with a busy tone or unanswered ringtone). You may then search for these types of sessions in Search and Replay. Recorded employee segments marked by means of auditing will appear in playback once all Sessions in the related Contact are closed, after a delay of up to five minutes.

- r. **Recorder Allocation Based On Audio Location**—Use this setting in a SIP-based VoIP delivery environment to control how Recorders are selected to record calls, and ensure that each call is recorded by a Recorder local to the media gateway at which the call arrives. This setting is designed primarily for environments where recording occurs at multiple sites and each site has its own gateway.

Note that this setting must be used in conjunction with either a Gateway Side Correlation Pool member group or an IP Extension Pool member group configured for the data source. Within these member groups, you must specify the IP addresses or host names of the phones associated with the member group in the IP Network Region configuration.

The Recorder Allocation Based on Audio Location setting instructs the system to examine the IP address in a SIP message and compare this address to the addresses listed in the IP Network Region settings of the Gateway Side Correlation Pool or IP Extension Pool member group associated with the data source.

If an address in the SIP message matches one of those specified in the member group IP Network Region settings, the system will route the call to a Recorder associated with that member group.

The options for this setting are:

- **Inactive**—The system attempts to record the call, but does not use an address found in a SIP message to route the call to a particular Recorder. This is the default setting.
- **From Signaling**—The system examines the SIP header section of the SIP Invite. The system compares the address found in a SIP header field (such as From, Contact, Via, or Socket) to the addresses configured in the member group IP Network Region settings. If there is a match, the system routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting will determine how the call is recorded.
- **From Media**—The system examines the SDP message attached to a SIP Invite. The system compares the IP addresses found in the SDP message to those configured in the member group IP Network Region settings. If there is a match, it routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded. This option does not work if SIP operates in Delayed-Offer mode.

Note that this setting works in combination with the **Recording Resource Allocation Behavior** setting to determine recording behavior. If the **Recording Resource Allocation Behavior** setting specifies:

- **IgnoreLine**—The system acts as if the Inactive setting is selected for this setting. If either the From Signaling or From Media is selected, those settings are ignored. In this case, any Recorder associated with the data source can record the call.
- **LineFirst**—The system makes two attempts to record the call using the address obtained from the SIP message. If the system cannot successfully route the call to a Recorder using the SIP message address, any Recorder associated with the data source can record the call.
- **LineExclusive**—If the system cannot successfully route the call to a Recorder using the address from the SIP message, the call is not recorded. In this case, the system raises an alarm.

- s. **Video Recording Mode**— Select one of the following options:
- **Start On Trigger** - Do not record video calls for the extensions associated with this data source until a recording rule is triggered or an external API command starts recording. Video recording starts whenever the call starts, but video prior to the recording trigger is deleted.
 - **Application Controlled** - Record every video call for every extension associated with this data source, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start to the end of the call.
 - **Do Not Record** - Do not record video calls for extensions associated with this data source. Recording rules are ignored and cannot trigger the recording of video calls.
 - **Record** - Record all video calls for extensions associated with this data source. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
- t. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:
- **Disabled:** No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always:** Sensitive customer information is obscured.
 - **In Fallback:** Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
- u. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:
- **Disabled:** The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.
 - **In Fallback:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.
- v. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
- **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.
7. In the **Default Employee** section, specify the employee to be associated to a recording that has no employee associated to it.

There are situations where recordings will not have employees associated to them. Examples include:

- IVR recordings where there is no employee or phone device
- Back office environments where phones are shared and not associated to a specific employee

Assigning a **Default Employee for Interactions** to a data source provides a way to provide replay access to these recordings. When a **Default Employee for Interactions** is configured, any recordings made for the data source that have no explicit user associated are associated to the **Default Employee for Interactions**.

First, select the **Organization** to which the **Default Employee for Interactions** belongs, and then select one employee as the **Default Employee for Interactions**.

You cannot select an employee who has a configured end date as the **Default Employee for Interactions**. Also, you should not select an employee who will soon move or transfer to a different organization as the **Default Employee for Interactions**.

Once an employee is selected as the **Default Employee for Interactions**, an error message displays on the data source screen if the employee has been deleted, terminated, or changed to a different organization since the last time the data source was saved.

8. Select one of the following **Device IP Configuration** options and enter the corresponding **IP Address**:

- **PBX Side - Near End**—The PBX Side - Near End is the server used to send/receive the control messages to/from the extensions. If you have the same extensions in multiple data sources, you must specify an IP Address or Host Name for the signaling interface server.

Otherwise, the setting is not mandatory, but recommended.

The Recorder uses the source or destination IP addresses or host names of the signaling messages to identify the particular data source with which a call is associated. The recorder does not use any data inside the signaling itself to make this determination. For this reason, the source/destination of the IP packets presented to the Recorder *must be different for each duplicate extension*. Make sure that your network is set up in such a way as to allow for this.

Example

A proxy server in front of separate PBXs using duplicate extensions can cause IP packets to appear as though they are using the same IP address (even though the SIP signaling would indicate otherwise). This will prevent the duplicate extensions from being recorded correctly.

For more details, see the section “Recording Duplicate Extensions” in the *Recorder Configuration and Administration Guide*.

- **PSTN Side - Far End**—If you are using SIP Trunk Recording, set PSTN Side - Far End as the Server Type.

This setting is only available for Avaya and Generic switch types, and if you have created a Gateway Side Correlation Pool Member Group, this setting is mandatory.

For details on this, see the “SIP Trunk Recording” section in the *Recorder Configuration and Administration Guide*, or the related online help.

9. If Scorecards is part of your package, expand the **Scorecards Settings** area and type the **Contact Viewer Server Name**, **Contact Viewer Server Port**, **Contact Viewer URL**. For more details, refer to your Scorecards documentation.

10. Configure **SIP Call Tracking** to achieve session tracking and recording of signaling only calls (non-CTI), typically seen with Interactive Voice Response (IVR).
 - **Track Signaling Calls** - Select this setting to enable session tracking for signaling only calls (non-CTI). To disable session tracking for signaling only calls, clear the check mark from this setting. (If you disable the setting, neither of the settings below is applicable). This setting is disabled by default.
 - **Separate CTI and Signaling API Commands** - If you select this setting, API commands sent during a signaling or CTI session are applicable only within that session. If a command is sent during an IVR call, and the call then transitions to an agent, the command is cleared. If a command is sent during an agent call, and then the call transitions to IVR, the command is also cleared. If the agent performs operations such as consult, transfer, or conference, any command sent within the agent portion is still applicable to all the portions of the agent call within the contact.
 - **Signaling Recording Mode** - Defines the behavior applied to the correlation line on a tracked signaling call. This setting also exists in the Recorder configuration and in that context controls the baseline behavior. Use this setting to control the signaling portion of the call specifically. For example, to capture all signaling recordings, select **Record** as the value.

If you clear the check mark from this setting, API commands will apply to the entire contact, including any agent calls.

 - **Track Signaling Calls** - Select this setting to enable session tracking for signaling only calls (non-CTI). To disable session tracking for signaling only calls, clear the check mark from this setting. (If you disable the setting, neither of the settings below is applicable). This setting is disabled by default.
 - **Separate CTI and Signaling API Commands** - If you select this setting, API commands sent during a signaling or CTI session are applicable only within that session. If a command is sent during an IVR call, and the call then transitions to an agent, the command is cleared. If a command is sent during an agent call, and then the call transitions to IVR, the command is also cleared. If the agent performs operations such as consult, transfer, or conference, any command sent within the agent portion is still applicable to all the portions of the agent call within the contact.

If you clear the check mark from this setting, API commands will apply to the entire contact, including any agent calls.

 - **Signaling Recording Mode** - Defines the behavior applied to the correlation line on a tracked signaling call. This setting also exists in the Recorder configuration and in that context controls the baseline behavior. Use this setting to control the signaling portion of the call specifically. For example, to capture all signaling recordings, select **Record** as the value.
11. If applicable, expand the **Associated Integration Service Installations** area and select the server that is providing Integration Services for the recorder for which you are configuring this data source.



In a multi-tenant enabled environment, the tenant name associated to each Site Group, Site, and Server appears beside the Site Group, Site, and Server name on the right side of the Installations tree.

12. Click **Save**.

13. For **Associated Data Sources**, you can associate a phone data source to any dialer data source sub type. You can also associate an Avaya Proactive Outreach Manager (POM) dialer data source to an Avaya Experience Platform application data source.

 If you are using a standalone dialer, you can skip this step.

You associate the phone data source to a dialer data source to associate the PBX/ACD (that is, the phone data source you created earlier) to the dialer data source.

You associate an Avaya POM dialer data source to an Avaya Experience Platform application data source to support the Avaya Experience Platform CaaS product. This association supports tenants that have purchased dialer capabilities as part of their OneCloud product set.

To associate a phone or Avaya Experience Platform data source to a dialer data source, do the following:

- a. Under **Associated Data Sources**, click **Add**.
- b. Under **Data Source**, select a phone data source or the Avaya Experience Platform application data source.

 In a multi-tenant enabled environment, the phone data source selected here must be associated to the same tenant as the dialer data source. If the phone data source is not associated to the same tenant as the dialer data source, an error message displays when you click **Save** to save the dialer data source.

- c. For a phone data source, specify a **Dial Code**, **Discard Digits** and **New Prefix** value. These fields define the transformation of the dialer extensions into ACD extensions. For example, if the dialer extension is 551234, and the ACD is 81234, enter "55" as the Dial Code, "2" under Discard Digits (that is, the total number of digits to be discarded), and the Prefix, "8". In this example, any 55xxxx, would translate to 8xxxx.

For an Avaya Experience Platform data source, leave the **Dial Code**, **Discard Digits** and **New Prefix** fields empty.

With the exception of the Avaya POM dialer data source, you can associate multiple phone data sources with the dialer data source. It is important to note that the combination of the phone extension plus the dialer code must be unique. (For example, if the dialer codes are 21 and 211, and the associated extensions are 12 and 2 respectively, this creates a conflict.)

You can only associate one data source to the Avaya POM dialer data source. You can associate either an Avaya Experience Platform application data source or an Avaya Communication Manager phone data source to the Avaya POM data source.

14. If applicable, expand the **Associated Integration Service Installations** area and select the server that is providing Integration Services for the recorder for which you are configuring this data source.
15. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. This should only be done in consultation with our field engineers.
16. Click **Save**.

Related topics

[Editing a data source \(page 153\)](#)

[Deleting a data source \(page 157\)](#)

Creating LAN (Screen) data sources

You must first create a Phone data source on the **Settings** page, before you can create a LAN (Screen) data source.

1. In **Recording Management > Data Sources > Settings**, click **Create Data Source**.
2. In the pop-up **Data Source Type** page, from the **Type** drop-down list box, select **LAN (Screen)**, then click **Select**.
3. Type a **Name** for the data source.
4. Specify the **Organization** to which you want to associate the data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

5. Type a **Description** for the data source (optional).
6. Under **Recorder Settings**, select one of the following under **Seating Arrangement**:
 - **Free** seating, the default, indicates that employees do not have permanently-assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
 - **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension.
 - **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.



If you select **Fixed** or **Hybrid** seating, you will be required to set the Workstation that employees are assigned to. This is similar to assigning an extension to an employee for Phone data sources.

The **Workstation** column then displays on the LAN data source page.

7. Under **Recorder Settings**, select the appropriate **Session Auditing Policy** setting. This setting defines the type of session that should be marked and kept in the system. "Disabled" (the default) will only mark sessions with some kind of content. Two additional options will create a basic entry in the database for screen sessions that occurred but were not recorded: "Missed Recordings" will mark screen sessions that should have been recorded, but were not, while "Full Switch" will mark all sessions for which we receive CTI without recording (for example, calls that were blocked). You may then search for these types of sessions in Search and Replay. Recorded employee segments marked by means of auditing will appear in playback once all Sessions in the related Contact are closed, after a delay of up to five minutes.
8. **Long Call Duration** - This setting allows you to specify the length of a screen recording, in minutes, after which the system will trigger an alarm. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where screen recordings exceed this number of minutes. The default is 120.



The Integration Service runs maintenance checks every five minutes to close screen recordings that last for more than the length of time specified as the **Long Call Duration**. An alarm will indicate that a call was closed because it was too long. These maintenance checks are not run more frequently in order to avoid imposing an additional load on the system. Therefore it may take up to five minutes to close a long screen recording after it has passed the defined **Long Call Duration** threshold.

9. To prevent the retention of very short screen recordings, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.
10. In the **Default Employee** section, specify the employee to be associated to a recording that has no employee associated to it.

There are situations where recordings will not have employees associated to them. Examples include:

- IVR recordings where there is no employee or phone device
- Back office environments where phones are shared and not associated to a specific employee

Assigning a **Default Employee for Interactions** to a data source provides a way to provide replay access to these recordings. When a **Default Employee for Interactions** is configured, any recordings made for the data source that have no explicit user associated are associated to the **Default Employee for Interactions**.

First, select the **Organization** to which the **Default Employee for Interactions** belongs, and then select one employee as the **Default Employee for Interactions**.

You cannot select an employee who has a configured end date as the **Default Employee for Interactions**. Also, you should not select an employee who will soon move or transfer to a different organization as the **Default Employee for Interactions**.

Once an employee is selected as the **Default Employee for Interactions**, an error message displays on the data source screen if the employee has been deleted, terminated, or changed to a different organization since the last time the data source was saved.

11. Under **Associated Integration Service Installations**, select the server that is providing Integration Services for this recorder, if applicable.



In a Multi-Tenant SaaS environment, the tenant name associated to each Site Group, Site, and Server appears beside the Site Group, Site, and Server name on the right side of the Installations tree.

12. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system.
13. Click **Save**.
14. Click the **Workstations** page, then do the following:

- a. Click **Create**.
- b. On the **New Workstations** page, specify the Phone data source associated with this LAN data source. To specify the Phone data source, click beside the **Phone Data Source** drop-down list, and select the Phone data source. Complete the rest of the information on this page, and the other LAN (Screen) data source pages as required.
- c. Select the Phone data source that you plan to associate with this LAN (screen) data source, and complete step 3 of the procedure: [Creating Phone data sources \(page 132\)](#).

Once you have completed the above steps, the LAN (Screen) data source is properly configured, and you can use it for screen recording in your system.

Related topics

[Editing a data source \(page 153\)](#)

[Deleting a data source \(page 157\)](#)

Related information

Configuring the LAN (Screen) data source (*Recorder Configuration and Administration Guide*)

Creating Operations data sources

If you are licensed for the Operations features, an Operations data source is one of the possible data sources you can create.

To create an Operations data source:

1. In **Integration Management > Data Sources > Settings**, click **Create Data Source**.
2. In the pop-up **Data Source Type** page, from the **Type** drop-down list box, select **Operations**, and then click **Select**.
3. In the **Name** text box, type a data source name.
4. If applicable, from the **Organization** drop-down list, select the organization to which you want to associate this data source.



For this feature, note the following:

- The Organization selection feature is only visible if you have the Org Scoped Data Sources license.
- By default, organizations are selected in the drop-down list in **one** of the following ways:
 - If no organization is configured for a data source, the selected organization is the default root organization.
 - When creating a new data source, the selected organization is the user's current organization assignment.
- The **Organization** drop-down list is not restricted by the user's scope, and displays all

- existing organizations.
- Child organizations inherit the parent organization's association with a data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

5. In the **Description** text box, type a description (optional).
6. Select a time zone for the data source from the drop-down menu.
7. Click **Save** to create the new data source.
8. If required, click the **Data Source Groups** page and create data source groups for the **Operations** data source.
9. Once you have set up the following, do the following:
10. To specify a transformation operation, click the **Transformation Operations** page. For details on working with this page, see [Transformation Operations \(page 171\)](#).



Operations data can be imported in many forms. These forms need to be transformed during the import process into a form that can be used in Workforce Management. For more details, see [Working with operations in Workforce Management \(page 171\)](#).

11. To specify Work Item Tracking (WIT) data that is imported from Operations data sources and define settings for custom attributes, click the **Wit Configuration** page. For details on working with this page, see [Wit Configuration \(page 175\)](#).

Related topics

[Editing a data source \(page 153\)](#)

[Deleting a data source \(page 157\)](#)

Creating OutSourcer data sources

1. In **Integration Management > Data Sources > Settings**, click **Create Data Source**.
2. In the pop-up **Data Source Type** page, from the **Type** drop-down list box, select **OutSourcer**, and then click **Select**.
3. In the **Name** text box, type a data source name.
4. If applicable, from the **Organization** drop-down list, select the organization to which you want to associate this data source.



For this feature, note the following:

- The Organization selection feature is only visible if you have the Org Scoped Data Sources license.
- By default, organizations are selected in the drop-down list in one of the following ways:
- If no organization is configured for a data source, the selected organization is the default root organization.
- When creating a new data source, the selected organization is the user's current organization assignment.
- The **Organization** drop-down list is not restricted by the user's scope, and displays all existing organizations.
- Child organizations inherit the parent organization's association with a data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

5. In the **Description** text box, type a description (optional).
6. Type an external name. This name is the name of the ACD as retrieved by the ACD vendor.
7. Click **Save** to create the data source.

Related topics

[Editing a data source \(page 153\)](#)

[Deleting a data source \(page 157\)](#)

Creating Phone data sources

To set up voice recording, create a phone data source. A phone data source encapsulates information related to the target to be recorded, specifically the switch type and the seating arrangement of employees who use the phones within the call center.

You also must create a phone data source before you can create a LAN (screen) data source.

If you are creating a LAN (Screen) data source as well, see also [Workflow for creating a Phone data source with a LAN \(Screen\) data source \(page 143\)](#).

For details on collection data sources and configuring collection data sources, see:

- [Creating Collection Data Sources \(page 143\)](#)
- [Configuring child data sources to correlate audio and CTI \(page 144\)](#)

To create a Phone Data Source

1. Depending on which system you are working in, on the left vertical menu, select **Integration Management** or **Recording Management**.
2. From there, go to **Data Sources > Settings**, and click **Create Data Source**.
3. In the **Data Source Type** page, do the following:
 - a. From the **Type** drop-down list box, select **Phone**
 - b. From the **Switch/Sub Type list box**, select a switch/sub-type.



The data source types available to you depend on licensing. Similarly, some of the following options are only applicable if you are using a specific switch, and therefore they do not appear for some of the phone data source subtypes.

- c. Click **Select**.
4. Type a **Name** for the phone data source.
 5. Specify the **Organization** to which you want to associate the data source.

In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.

A parent data source can be assigned to an organization belonging to a particular tenant or to a service provider organization.

- If the parent data source is assigned to an organization belonging to a particular tenant, the child data source must be assigned either to the same organization as the parent data source or to a suborganization under the parent data source organization.
 - If the parent data source is assigned to an organization belonging to the service provider, the child data source can be assigned to the same organization as the service provider, or to a suborganization under the parent service provider organization. The child data source can also be assigned to a particular tenant.
6. Type a **Description** of the data source (optional).
 7. Select a **Time Zone** from the drop-down list. You can specify whether tagging should be based on this time zone or that of the organization beneath it.



It is essential that the time zone is always correct on each server.

8. Specify a **Data Source Parent** to make the data source a child data source. Leave this setting set to **No Parent** to make the data source available to be a parent data source. Specify a data source parent (make the data source a child data source) in either of these scenarios:
 - You are configuring a Genesys Business Continuity environment. In this environment, you can specify a data source to act as a parent to multiple child data sources. In this scenario, you use a parent data source to configure extensions that are then shared by the child data sources. Each child data source represents a different switch (or site) where the sites are paired together to support failover. The child data source and parent data source must be of the same phone data source subtype.
 - You are creating a collection data source for gateway recording. For more information, see [Creating Collection Data Sources \(page 143\)](#) and [Configuring child data sources to correlate audio and CTI \(page 144\)](#).



A child data source must be assigned to the same organization as the parent data source or to a suborganization under the parent data source organization.

9. Under **Recorder Settings**, do the following:
 - a. Specify a **Seating Arrangement**—*Fixed, Free, or Hybrid*.
 - **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension.
 - **Free** seating, the default, indicates that employees do not have permanently assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
 - **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.
 - b. In a multi-tenant enabled (cloud) environment, the Service Provider Administrator (SPA) can specify a **Maximum Allowed Extensions** value for this data source. The Maximum Allowed Extensions setting limits the number of extensions a Tenant Administrator can create for the data source. This setting allows a SPA to prevent tenants from creating more extensions than their assigned capture capacity supports.

If this setting is not set and the data source currently has no extensions associated with it, this setting defaults to 1000 at the time a Tenant Administrator creates the first extension.

In an upgrade scenario, a data source may already have extensions assigned to it. In this scenario, when a Tenant Administrator adds extensions, the system updates this setting to 120% of the existing number of extensions or 1000, whichever is higher. For example, if 2000 extensions are associated with the data source at the time of the upgrade, this setting defaults to 2400 when a Tenant Administrator adds extensions.

This setting does not limit the number of extensions a SPA can create. For example, if the setting is 1000, a SPA can create more than 1000 extensions. If the SPA creates more extensions than this setting specifies, the Tenant Administrator cannot create any extensions.

If a Tenant Administrator configures the maximum number of allowed extensions, the SPA can increase this number to allow the Tenant Administrator to create more extensions. Before increasing this setting, the SPA verifies that the tenant's environment has the resources necessary to handle the increased load.

- c. To save the last employee's settings after the computer is turned off, select the **Persist Agent State on Shut Down (minutes)** check box. Specify the amount of time in minutes for which you want to save the employee's data logon state information. The default threshold is 600 minutes (10 hours). If the service restarts, state information within the threshold is reloaded from startup. State information beyond the threshold will not be loaded. Reloading this state information can be useful if the CTI link does not provide a snapshot capability so the recorder can learn about all the logged in states on startup. It is expected that the CTI feed supplements any state information loaded on startup. Data from within this time period will not be loaded, while data from after this duration has passed.

If the CTI adapter is down, the following occurs:

- If unselected, all agents on the data source are logged out right away.
 - If selected, all agents on the data source are logged out once the persistence period has elapsed.
- d. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.
 - e. If you are working with a system that uses Performance Mode (set in the IP Extension Pool member group) or N+N redundancy, enable the **Rollback Period (minutes)**.
This ensures that an amount of additional overlapping audio is kept for a time period, so that in the event of a disconnection it is possible to retrieve it. The default value is 15 minutes, and the maximum value is 60 minutes.



A rollback period is applicable only to Performance Mode (set in the IP Extension Pool member group) and N+N redundancy.

- f. If you are working with a system that uses Performance and Liability fallback modes, enable RTP detection to prevent audio loss. Coordination between the Integration Service and RTP, using the following settings, ensures that there will only be one recording for a specified call:
- **Start Overlay (milliseconds)**—This threshold indicates the longest amount of audio (from before CTI starts) that will be associated to that CTI call. The default is 5000 milliseconds (five seconds).
 - **End Overlay (milliseconds)**—This threshold indicates the longest amount of audio (after CTI ends) that will be associated to that CTI call. The default is 6000 milliseconds (six seconds).
- g. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system triggers an alarm. The system also stops tracking the call from a CTI perspective, so in CTI-controlled application or performance mode environments, this may cause loss of recording. Enter any number between 1 and 1440 (24 hours) —an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.
- i. **Long Hold Duration (minutes)**— This setting allows you to specify the maximum duration of a single hold in minutes. Any holds over this duration raises an alarm. Enter any number between 1 and 3000, representing the number of minutes. The default is 30.
- i. **Recording Resource Allocation Behavior**—This setting is for duplicate streaming solutions, which allow you to distribute recordings across multiple recorders.



The Integration Service runs maintenance checks every five minutes to close calls that last for more than the length of time specified as the **Long Call Duration**. An alarm indicated that a call was closed because it was too long. These maintenance checks are not run more frequently to avoid imposing an extra load on the system. Therefore, it may take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.



To use the CTI-based recorder selection feature available for Shared Interception or Avaya DMCC environments, you must select either **LineFirst** or **LineExclusive**. For details, see the *Recorder Configuration and Administration Guide*:

- For Shared inception, see the section “IP Extension Pool Member Group Settings.”
 - For Avaya, see the section “Extension Recording Resource Member Group Settings.”
- **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of data source, member group, and extension list settings.
 - **LineFirst**—First attempts to record on the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service can't find an associated recorder, it attempts to find any connected recorder with the capacity (whether or not the extension is associated with the recorder). LineFirst provides a way to keep recorders local to the extensions/site. The Integration

Service fails over to another set of recorders if a call cannot be recorded locally. If you do not want to fail over to another set of recorders, use 'LineExclusive', described below. This is the default.

- **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it will not record the call. By recording calls on a recorder co-located with the PBX for agents taking calls on a remote site, the use of this setting has the advantage of reduced WAN traffic.

The "least-utilized" recorder is the one with the most unused capacity. For example, if one recorder has 300 licenses and 50 calls are currently being recorded, and another recorder has 100 licenses and 10 calls are currently being recorded, the capacity left on the recorders is 250 and 90, respectively. The system will attempt to record the next duplicate streamed call on the first recorder.

- j. **Always Report Extension as Primary Extension**—If enabled, the extension field of the session/interaction will always be the primary extension on a telephone. If unavailable, the extension field contains the DN/extension that first answered the call. This only affects multiline phones. Enabled by default.
- k. **Contact Policy Type**—This setting allows you to set the call stitching method.
 - **Follow the call**—When follow the call is enabled, there will be one contact that includes all audio from the beginning of the call to the end. This is the default.
 - **Back office - Contact per call**—Enables the "Back office" style of stitching, which creates sessions or interactions based on CTI calls. If one employee is on two calls at the same time (for example, a customer call and a consultation call), the system creates two sessions or interactions. This is used more often in trading environments rather than contact center environments.
- l. **Raise Alarm for Out Of Service Devices**—If enabled, the Integration Service raises alarms for any devices that go out of service. This is only available for Cisco JTAPI and Genesys adapters.
- m. **Alarm - Device Not Recorded Call Count**—The number of calls for a configured device that must fail to record before triggering the DeviceNotRecording alarm. The default is 1.
- n. **Alarm - Device Not Recorded (milliseconds)**—Failed call durations under this threshold will not count against the Device Not Recorded Call Count. The default is 15 seconds.
- o. **Service Observe Fail Count Threshold**—The number of consecutive recording failures that must occur before the Integration Service attempts to reset the Service Observe connection. The default is 3.
- p. **Session Auditing Policy**—Defines the type of session or interaction that should be marked and kept in the system. "Disabled" (the default) only marks sessions or interactions with some kind of content. Two extra options create a basic entry in the database for calls that occurred but were not recorded: "Missed Recordings" will select calls that had to be recorded, but were not, while "Full Switch" will select all sessions or interactions for which we receive CTI without recording (for example, calls that were blocked, or interception calls that were met with a busy tone or unanswered ringtone). You can then search for these types of interactions in the

Portal.

Recorded employee segments marked by means of auditing will appear in playback once all Interactions in the related Contact are closed, after a delay of up to five minutes.

q. **Keep Duplicate Recording—**

For an N+N recording environment, select one of the following options:

- Select the **Keep Duplicate Recording** option when a customer's compliance recording policies require them to archive duplicate recordings of every call. To support this configuration, you must double the size of the Contact Database, the Archive Database, and the archive storage media.
- Clear the **Keep Duplicate Recording** option (default) so that the system deletes the secondary interaction after determining which copy to keep.



When N+N recording is configured, the system evaluates the interactions captured by both Recorders. It marks one as primary and the other as secondary based on several criteria, including call quality. For details, refer to *Selective Recording Configuration*.

Archive campaigns provide alternative methods for managing recordings in N+N environments. Set the N + N Dual Marking options to turn off the double-archiving of recordings, which keeps a single copy. For details, refer to *Campaign conditions*.

- r. **Recorder Allocation Based On Audio Location—**Use this setting in a SIP-based VoIP delivery environment to control how Recorders are selected to record calls, and ensure that each call is recorded by a recorder local to the media gateway at which the call arrives. This setting is designed primarily for environments where recording occurs at multiple sites and each site has its own gateway.

This setting must be used in conjunction with either a Gateway Side Correlation Pool member group or an IP Extension Pool member group configured for the data source. Within these member groups, you must specify the IP addresses or host names of the phones associated with the member group in the IP Network Region configuration.

The Recorder Allocation Based on Audio Location setting instructs the system to examine the IP address in a SIP message and compare this address to the addresses listed in the IP Network Region settings of the Gateway Side Correlation Pool or IP Extension Pool member group associated with the data source.

If an address in the SIP message matches one of those specified in the member group IP Network Region settings, the system routes the call to a recorder associated with that member group.

The options for this setting are:

- **Inactive**—The system attempts to record the call, but does not use an address found in a SIP message to route the call to a particular Recorder. This is the default setting.
- **From Signaling**—The system examines the SIP header section of the SIP Invite. The system compares the address found in a SIP header field (such as From, Contact, Via, or Socket) to the addresses configured in the member group IP Network Region settings. If there is a

match, the system routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded.

- **From Media**—The system examines the SDP message attached to a SIP Invite. The system compares the IP addresses found in the SDP message to those configured in the member group IP Network Region settings. If there is a match, it routes the call to a Recorder associated with that member group. If the system does not find a match, the **Recording Resource Allocation Behavior** setting determines how the call is recorded. This option does not work if SIP operates in Delayed-Offer mode.

This setting works with the **Recording Resource Allocation Behavior** setting to determine recording behavior. If the **Recording Resource Allocation Behavior** setting specifies:

- **IgnoreLine**—The system acts as if the Inactive setting is selected for this setting. If either the From Signaling or From Media is selected, those settings are ignored. In this case, any Recorder associated with the data source can record the call.
- **LineFirst**—The system makes two attempts to record the call using the address obtained from the SIP message. If the system cannot successfully route the call to a Recorder using the SIP message address, any Recorder associated with the data source can record the call.
- **LineExclusive**—If the system cannot successfully route the call to a Recorder using the address from the SIP message, the call is not recorded. In this case, the system raises an alarm.

s. **Video Recording Mode** — Select one of the following options:

- **Start On Trigger** - Do not record video calls for the extensions associated with this data source until a recording rule is triggered or an external API command starts recording. Video recording starts whenever the call starts, but video prior to the recording trigger is deleted.
- **Application Controlled** - Record every video call for every extension associated with this data source, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start to the end of the call.
- **Do Not Record** - Do not record video calls for extensions associated with this data source. Recording rules are ignored and cannot trigger the recording of video calls.
- **Record** - Record all video calls for all extensions associated with this data source. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.

t. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:

- **Disabled:** No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always:** Sensitive customer information is obscured.
 - **In Fallback:** Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
- u. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:
- **Disabled:** The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.
 - **In Fallback:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.
- v. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
- **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.
10. In the **Default Employee** section, specify the employee to be associated to a recording that has no employee associated to it.
- There are situations where recordings will not have employees associated to them. Examples include:
- IVR recordings where there is no employee or phone device
 - Back office environments where phones are shared and not associated to a specific employee
- Assigning a **Default Employee for Interactions** to a data source provides a way to provide replay access to these recordings. When a **Default Employee for Interactions** is configured, any recordings made for the data source that have no explicit user associated are associated to the **Default Employee for Interactions**.
- First, select the **Organization** to which the **Default Employee for Interactions** belongs, and then select one employee as the **Default Employee for Interactions**.
- You cannot select an employee who has a configured end date as the **Default Employee for Interactions**. Also, you should not select an employee who will soon move or transfer to a different organization as the **Default Employee for Interactions**.
- Once an employee is selected as the **Default Employee for Interactions**, an error message displays on the data source screen if the employee has been deleted, terminated, or changed to a different organization since the last time the data source was saved.
11. If you selected **Generic** as the switch subtype, expand the **Specific Switch Type** area and, in the **Specific Switch Type** field, specify the type of switch. Consult with our engineers for a list of

supported switch types.

- If you are using the TDM Recorder and selected the **Generic** or **Avaya** switch types, expand the **Recorder TDM Settings** area, then enter values in the following fields:
 - **Off Hook Delay (milliseconds)**—For Service Observe and Single Step Conference only, type the amount of time in milliseconds that the recorder will wait after taking a channel off-hook. Maximum of 6 characters, representing a total time of not more than 15 seconds.
 - **On Hook Delay (milliseconds)**—For Service Observe only, type the amount of time in milliseconds that the recorder will wait after putting a channel on-hook. Maximum of 6 characters, representing a total time of not more than 15 seconds. (The default is two seconds.)
 - **Service Observe String**—Service Observe is a type of three-way conference that allows the monitoring of employees on an extension. Type the dial string used to invoke the Service Observe feature on a switch. Use the characters 0–9, #, or *, to a maximum of 16 characters. (The default is 116.)
 - **Inter Digit Delay (milliseconds)**—Type the amount of time in milliseconds that the recorder waits between dialing digits on a channel. Maximum of 6 characters, representing a total time of not more than 15 seconds. (The default is 150 milliseconds.)
 - **Period Between Service Observe (milliseconds)**—Type a value in milliseconds, between 0 and 10000, to indicate the minimum allowable time between sessions of Service Observe. This setting is for Dedicated Service Observe deployments only and prevents overloading the system with simultaneous requests. The default is 250 milliseconds.
 - **Record Extensions for Internal Calls**—This setting applies to trunk side environments (such as the Avaya switch in trunk-side environment), and hybrid systems where the same data source is used for TDM recording and IP recording (one data source and two member groups). Select this check box to allow the recording of internal calls on selective recording resources. If you configure a Gateway Side Correlation Pool member group and an Extension Recording Resource member group, internal calls are recorded regardless of this setting.
 - **Record IP Trunks**—To record all other non-SIP calls using selective DMCC resources when there is no match between CTI events and configured member groups, enable this setting. If you configure a Gateway Side Correlation Pool member group and an Extension Recording Resource member group, all other non-SIP trunk calls are recorded regardless of this setting.
12. If your recorder is part of a package that includes WFM, expand the **WFM Settings** area and configure the following values:
- Specify whether you want to **Use ACD Staffing**.
 - Type an **External Name**.
 - If applicable, from the **Organization** drop-down list, select the organization to which you want to associate this data source.



For this feature, note the following:

- The Organization selection feature is only visible if you have the Org Scoped Data Sources license.
- By default, organizations are selected in the drop-down list in one of the following ways:

- If no organization is configured for a data source, the selected organization is the default root organization.
- When creating a new data source, the selected organization is the user's current organization assignment.
- The **Organization** drop-down list is not restricted by the user's scope, and displays all existing organizations.
- Child organizations inherit the parent organization's association with a data source.

- Select a **Data Source Parent**.
13. Expand the **TimeZone Settings** area, and select one of the **Local Time Tagging Mode** options from the drop-down list:
- **Organization**—to base tagging on the organization. This is useful in scenarios where employees are working in different regions, allowing you to unify tagging across multiple time zones.



If you select **Organization**, it is still necessary to specify the correct time zone for the data source as described in step 7, where you selected a time zone from the **Time Zone** drop-down list.

This is used in fallback selection for monitored extensions without an associated Employee or Profile (that is, extensions that don't belong to an employee).

- **Data Source**—to base tagging on the time-zone specified in step 5, where you selected a time zone from the **Time Zone** drop-down list.

14. Select one of the following **Device IP Configuration** options and enter the corresponding **IP Address**:



For the Broadworks data source subtype, this section is blank. You do not need to make a selection.

- **PBX Side - Near End**—The PBX Side - Near End is the server used to send/receive the control messages to/from the extensions. If you have the same extensions in multiple data sources, you must specify an IP Address or Host Name for the signaling interface server.

Otherwise, the setting is not mandatory but recommended.

The recorder uses the source or destination IP addresses or host names of the signaling messages to identify the particular data source with which a call is associated. The recorder does not use any data inside the signaling itself to make this determination. For this reason, the source/destination of the IP packets presented to the recorder *must be different for each duplicate extension*. Make sure that your network is set up in such a way as to allow for this.

For example, a proxy server in front of separate PBXs using duplicate extensions can cause IP packets to appear as though they are using the same IP address (even though the SIP signaling would indicate otherwise). This prevents the duplicate extensions from being recorded correctly.

For more details, see the topic “Recording Duplicate Extensions” in the *Recorder Configuration and Administration Guide*.

- **PSTN Side - Far End**—If you are using SIP Trunk Recording, set PSTN Side - Far End as the Server Type.

This setting is only available for Avaya and Generic switch types, and if you have created a Gateway Side Correlation Pool Member Group, this setting is mandatory.

For details on this, see the “SIP Trunk Recording” section in the *Recorder Configuration and Administration Guide*, or the related help.

15. If Scorecards is part of your package, expand the **Scorecards Settings** area and type the **Contact Viewer Server Name**, **Contact Viewer Server Port**, **Contact Viewer URL**. For more details, refer to your Scorecards documentation.
16. Configure **SIP Call Tracking** to achieve session tracking and recording of signaling only calls (non-CTI), typically seen with Interactive Voice Response (IVR).

- **Track Signaling Calls** - Select this setting to enable session tracking for signaling only calls (non-CTI). To make session tracking unavailable for signaling only calls, clear the check mark from this setting. (If you make the setting unavailable, neither of the following settings is applicable.) This setting is unavailable by default.
- **Separate CTI and Signaling API Commands** - If you select this setting, API commands sent during a signaling or CTI session are applicable only within that session. If a command is sent during an IVR call, and the call then transitions to an agent, the command is cleared. If a command is sent during an agent call, and then the call transitions to IVR, the command is also cleared. If the agent performs operations such as consult, transfer, or conference, any command sent within the agent portion is still applicable to all the portions of the agent call within the contact.

If you clear the check mark from this setting, API commands apply to the entire contact, including any agent calls.

- **Signaling Recording Mode** - Defines the behavior applied to the correlation line on a tracked signaling call. This setting also exists in the Recorder configuration and in that context controls the baseline behavior. Use this setting to control the signaling portion of the call specifically. For example, to capture all signaling recordings, select **Record** as the value.
17. If applicable, expand the **Associated Integration Service Installations** area and select the server that is providing Integration Services for the recorder for which you are configuring this data source.



In a Multi-Tenant SaaS environment, the tenant name associated to each Site Group, Site, and Server appears beside the Site Group, Site, and Server name on the right side of the Installations tree.

18. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. This should be done only in consultation with our field engineers.



For the Broadworks data source subtype, this section is blank. You do not need to make a selection.

19. Click **Save**.

Workflow for creating a Phone data source with a LAN (Screen) data source

1. Complete the procedure [To create a Phone Data Source \(page 132\)](#).
2. Create a LAN (screen) data source, as described under [Creating LAN \(Screen\) data sources \(page 127\)](#). Make sure to configure the workstations.
3. Select the phone data source that you created in step 1, and from that page, select the **Phones** page. Do the following:
 - a. On the **Phones** page, click **Create**.
 - b. Type **Extension** and select **Recording Mode** information as required.
 - c. From the **LAN (Screen) Data Source** drop-down list, select the LAN data source you created in step 2 above.
 - d. Beside the **Workstation Name** text box, click the pencil icon, and find and select the workstations you set up when creating the LAN data source.
 - e. Complete any other information required.
 - f. Click **Save**. The LAN (Screen) data source and its workstations are now set to work with the Phone data source.

For more information on configuring the **Phones** page itself, see the *Recorder Configuration and Administration Guide*.

Creating Collection Data Sources

A Collection data source is a way to represent shared gateway resources used by multiple, independent PBX sources. The Collection data source holds the gateway member group with associated recorders and acts as a “parent” data source for multiple “child” data sources. These child data sources represent the multiple PBXs that may place and receive calls through the recorded

gateways.



For collection data sources, the maximum number of child data sources you can associate with a parent is 50.

For more details, see the *Recorder Integration Guide* provided by your application consultant.

1. In the Enterprise Manager, click **Recording Management > Data Sources**.
2. Click **Create Data Source**.
3. In the Data Source Type page, select Phone as the Type, and select **Collection** from the **Switch/Sub Type** list box.
4. Click **Select**.
5. Type a **Name** for the Phone data source, and a **Description** (optional).
6. Select a **Time Zone** from the list box (the Recorder relies on the time zone for recording start and end times).



It is essential that the time zone is always correct on each server.

The time zone selected in the Collection data source applies to all child data sources.

7. From the **Data Source Parent** field, select **No Parent**. The Collection data source serves as a parent data source.
8. Enter the following **Recorder Settings**, if applicable:
 1. A rollback period is applicable to systems using Performance Mode (set in the IP Extension Pool member group) or N+N redundancy. Enable the **Rollback Period (minutes)** to ensure that an amount of more overlapping audio is kept for a period, so that during disconnection it is possible to retrieve it. The default value is 15 minutes, and the maximum value is 60 minutes.
9. Under **Associated Integration Service Installations**, select the server that provides Integration Services for this Recorder.



The integration service associated with the Collection data source applies to all child data sources.

10. Under **Device IP Configuration**, specify **Call Center SIP Trunk Interface** as the **Server Type**. Enter the **IP Address** of the Call Center SIP Trunk Interface.
11. Click **Save**.
12. Within the Collection data source, create a Gateway Side Correlation Pool member group as described in the *Recorder Configuration and Administration Guide*, and associate with it the relevant Recorders.
13. Click **Save**.

Configuring child data sources to correlate audio and CTI

To properly correlate audio and CTI events within a pool of calls, create a phone data source for each PBX and assign each phone data source to a parent collection data source.

Guidelines for child data sources

- For SIPREC only, a SIPREC adapter is associated with the parent collection data source (this adapter handles INVITE messages from the SBC).
- For all scenarios, including SIPREC, a CTI adapter for each child data source.
- Child data sources are automatically assigned to the same integration service as the parent and configured with the devices to be monitored.
- All child data sources must be the same subtype. For example, you cannot have a combination of Cisco and Avaya.
- The child data sources must not contain member groups.
- The maximum number of child data sources you can associate is 50.
- The maximum Long Call Duration value from among all the specified in child data sources is used.
- The child data source can be assigned to the same organization as the parent service provider, to a suborganization, or to a specific tenant.
- A child data source must be assigned to the same organization as the parent data source or to a suborganization.
- After the child data source is saved, it can only be reassigned to an organization of the same tenant. If you need to reassign a child data source to a different tenant, delete the existing one and create a new one.

Procedure

1. To make a data source the child of another, select the data source.
2. Under **Data Source Parent**, select the name of the collection data source created previously.
3. Click Save.

The child data source is assigned to the same organization as the parent. If required, you can reassign the child data source to another data source within this tenant's organization.

Related topics

[Creating a parent-child relationship between data sources \(page 153\)](#)

Create a Radio data source

To set up voice recording for a trunked radio system, you must create a radio data source. A radio data source provides the system with needed information about the radio source to be recorded, such as the switch type and the seating arrangement of employees using the radios.

Procedure

1. Navigate to **RecordingManagement > Data Sources > Settings**, and click **Create Data Source**.
2. In the **Data Source Type** page, do the following:

- a. From the **Type** drop-down list box, select **Radio**
- b. From the **Switch/Sub Type list box**, select a **switch/sub-type**.



The data source types available to you depend on licensing. Similarly, some of the following options are only applicable if you are using a specific switch; therefore, they do not appear in all cases.

- c. Click **Select**.
3. Type a **Name** for the radio data source.
4. Specify the **Organization** to which you want to associate the data source.
In a multi-tenant enabled environment, if the selected organization is associated with a tenant, the data source is also associated with that same tenant. In this scenario, when you click **Save** to save the data source, the tenant name of the organization that is associated with the data source is displayed in the screen heading. The data source can be associated with a particular tenant or have the **Shared** status. A data source associated with a particular tenant processes data only for that tenant. A data source that has the **Shared** status processes data for all tenants in the system.
5. Type a **Description** for the data source (optional).
6. Select a **Time Zone** from the drop-down list. You can specify whether tagging should be based on this time zone or that of the organization.



It is essential that the time zone is always correct on each server.

7. Under **Recorder Settings**, do the following:
 - a. Specify a **Seating Arrangement**—*Fixed, Free, or Hybrid*.
 - **Fixed** seating indicates that an employee has a permanently assigned workstation and is associated with a specific extension. For the Bosch data source sub-type, only the Fixed seating arrangement is available.
 - **Free** seating, the default, indicates that employees do not have permanently-assigned workstations. They are assigned an Employee ID and can log in from any location in the call center. Extensions are assigned dynamically when the employee logs in.
 - **Hybrid** seating refers to a mixed arrangement that contains both Free and Fixed seating for employees.
 - b. To prevent the retention of very short calls, specify a **Minimum Session Length (seconds)**. Active calls (from connected to closed) that are shorter than the specified value will be deleted automatically. If set to zero (0), this feature is disabled and no calls will be deleted based on this setting. The maximum value is 3600 (or one hour). This setting applies to the active duration of CTI Sessions or the entire duration of VOX Sessions. Inactive CTI Sessions can be retained using the Session Auditing Policy.
 - c. If you are working with a system that uses Performance Mode (set in the IP Extension Pool member group) or N+N redundancy, enable the **Rollback Period (minutes)**.
This ensures that an amount of additional overlapping audio is kept for a period of time, so that in the event of a disconnection it is possible to retrieve it. The default value is 15 minutes, and the maximum value is 60 minutes.

i A rollback period is applicable only to Performance Mode (set in the IP Extension Pool member group) and N+N redundancy.

- d. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system triggers an alarm. The system also stops tracking the call from a CTI perspective, so in CTI-controlled application or performance mode environments, this may cause loss of recording. Enter any number between 1 and 1440 (24 hours) —an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.

i The Integration Service runs maintenance checks every five minutes to close calls that last for more than the length of time specified as the **Long Call Duration**. An alarm indicated that a call was closed because it was too long. These maintenance checks are not run more frequently in order to avoid imposing an additional load on the system. Therefore it may take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.

- e. **Recording Resource Allocation Behavior**—This setting is for duplicate streaming solutions, which allow you to distribute recordings across multiple recorders.

i To use the CTI-based recorder selection feature available for Shared Interception or Avaya DMCC environments, you must select either **LineFirst** or **LineExclusive**. For details, see the *Recorder Configuration and Administration Guide*:

- For Shared inception, see the section “IP Extension Pool Member Group Settings”.
- For Avaya, see the section “Extension Recording Resource Member Group Settings”.

- **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of data source, member group, and extension list settings.
- **LineFirst**—First attempts to record on the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service can't find an associated recorder it will attempt to find any connected recorder with the capacity (whether or not the extension is associated with the recorder). LineFirst provides a way to keep recorders local to the extensions/site. The Integration Service will fail over to another set of recorders if a call can't be recorded locally. If you don't want fail over to another set of recorders, use 'LineExclusive', described below. This is the default.
- **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated to the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it will not record the call. By recording calls on a recorder co-located with the PBX for agents taking calls on a remote site, the use of this setting has the advantage of reduced WAN traffic.

The “least-utilized” recorder is the one with the most unused capacity. For example, if one recorder has 300 licenses and 50 calls are currently being recorded, and another recorder has with 100 licenses and 10 calls currently being recorded, the capacity left on the recorders are

250 and 90 respectively. The system will attempt to record the next duplicate streamed call on the first recorder.

- f. **Alarm - Device Not Recorded Call Count**—The number of calls for a configured device that must fail to record before triggering the DeviceNotRecording alarm. The default is 1.
- g. **Alarm - Device Not Recorded (milliseconds)**—Failed call durations under this threshold will not count against the Device Not Recorded Call Count. The default is 15 seconds.
- h. **Session Auditing Policy**—Defines the type of session/interaction that should be marked and kept in the system. “Disabled” (the default) will only mark sessions/interactions with some kind of content. Two additional options will create a basic entry in the database for calls that occurred but were not recorded: “Missed Recordings” will mark calls that should have been recorded, but were not, while “Full Switch” will mark all sessions/interactions for which we receive CTI without recording (for example, calls that were blocked). You may then search for these types of interactions in the Portal.
Recorded employee segments marked by means of auditing will appear in playback once all Interactions in the related Contact are closed, after a delay of up to five minutes.
- i. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:
 - **Disabled:** No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always:** Sensitive customer information is obscured.
 - **In Fallback:** Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
- j. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:
 - **Disabled:** The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.
 - **In Fallback:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.
- k. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
 - **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.

8. Expand the **TimeZone Settings** area, and select one of the **Local Time Tagging Mode** options from the drop-down list:
 - **Organization**—to base tagging on the organization. This is useful in scenarios where employees are working in different regions, allowing you to unify tagging across multiple time zones.

i If you select **Organization**, it is still necessary to specify the correct time zone for the data source as described in step 6, where you selected a time zone from the **Time Zone** drop-down list.

This is used in fallback selection for monitored extensions without an associated Employee or Profile (that is, extensions that don't belong to an employee).

- **Data Source**—to base tagging on the time-zone specified earlier, where you selected a time zone from the **Time Zone** drop-down list.
9. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. This should be done only in consultation with our field engineers.
 10. If applicable, expand the **Associated Integration Service Installations** area and select the server that is providing Integration Services for the recorder for which you are configuring this data source.

i In a multi-tenant enabled environment, the tenant name associated to each Site Group, Site, and Server appears beside the Site Group, Site, and Server name on the right side of the Installations tree.

11. Click **Save**.

Creating Trader data sources

1. In **Recording Management > Data Sources > Settings**, click **Create Data Source**.
2. In the pop-up **Data Source Type** page, do the following:
 - a. From the **Type** drop-down list box, select **Trader**.
 - b. From the **Switch/Sub Type list box**, select a switch/sub-type.

i Your license determines which switches are displayed in the **Switch/Sub Type** list box.

- c. Click **Select**.
3. **Name** - Type a data source name. This is a required field. Only alphanumeric characters (no quotation marks and no back or forward slashes) are supported in the data source name.
4. Type a short description.
5. Select a **Time Zone** from the drop-down list.

i When defining the Trader Data source, you must select the correct time zone.

For UK installations, select Greenwich Mean Time (GMT): Dublin, Edinburgh, Lisbon, London time zone so that the Daylight Savings Time (DST) changes are accounted for. The same time zone should also be used in Enterprise Manager and Recorder Manager Preferences.

6. Do the following:

- a. Enable the **Rollback Period (in minutes)** to ensure that a recording is kept for a certain amount of time before deletion, so that in the event of a disconnection it is possible to retrieve it. A rollback period is applicable only to Performance Mode (set in the IP Extension Pool member group) and N+N redundancy. The default value is 15; the maximum value is 60.
- b. Type a number for **Alarm - Device Not Recorded Call Count**. This field contains number of calls for a configured device that must fail to record before triggering the DeviceNotRecording alarm. The default is 1 failure.
- c. Type a number in milliseconds for **Alarm - Device Not Recorded Duration (milliseconds)**. Failed call durations under this threshold will not count against the Device Not Recording Call Count. The default is 15 seconds.
- d. **Long Call Duration (minutes)**—This setting allows you to specify the length of a call, in minutes, after which the system will trigger an alarm. The system will also stop tracking the call from a CTI perspective, so in CTI-controlled application or performance mode environments this may cause loss of recording. Enter any number between 1 and 1440 (24 hours)—an alarm is raised in the cases where calls exceed this number of minutes. The default is 120.

i The Integration Service runs maintenance checks every five minutes to close calls that last for more than the length of time specified as the **Long Call Duration**. An alarm indicates when a call is closed because it was too long.

Since these maintenance checks are not run more frequently in order to avoid imposing an additional load on the system, it may take up to five minutes to close a long call after it has passed the defined **Long Call Duration** threshold.

- e. **Long Hold Duration (minutes)**—Indicates the maximum duration of a single hold. Any holds over this duration will raise an alarm. Enter any number between 1 and 3000, representing the number of minutes. The default is 30.
- f. **Recording Resource Allocation Behavior**—This setting is for duplicate streaming solutions, which allow you to distribute recordings across multiple recorders.

i To use the CTI-based recorder selection feature available for Shared Interception or Avaya DMCC environments, you must select either **LineFirst** or **LineExclusive**. For details, see the *Recorder Configuration and Administration Guide*:

- For Shared inception, see the section “IP Extension Pool Member Group Settings”.
- For Avaya, see the section “Extension Recording Resource Member Group Settings”.

- **IgnoreLine**—Records the next recording on the least-utilized recorder connected to the Integration Service, regardless of data source, member group, and extension list settings.
- **LineFirst**—First attempts to record on the least-utilized recorder that contains the extension being recorded in a member group associated with the recorder. If the Integration Service can't find an associated recorder it will attempt to find any connected recorder with the capacity (whether or not the extension is associated with the recorder). LineFirst provides a way to keep recorders local to the extensions/site. The Integration Service will fail over to another set of recorders if a call can't be recorded locally. If you don't want fail over to another set of recorders, use 'LineExclusive', described below. This is the default.
- **LineExclusive**—First attempts to allocate the recording to the least-utilized recorder that contains the extension being recorded in a member group associated to the recorder. If the Integration Service fails to find a recorder associated with the line to be recorded, it will not record the call. By recording calls on a recorder co-located with the PBX for agents taking calls on a remote site, the use of this setting has the advantage of reduced WAN traffic.

The "least-utilized" recorder is the one with the most unused capacity. For example, if one recorder has 300 licenses and 50 calls are currently being recorded, and another recorder has with 100 licenses and 10 calls currently being recorded, the capacity left on the recorders are 250 and 90 respectively. The system will attempt to record the next duplicate streamed call on the first recorder.

- g. **Always Report Extension as Primary Extension**—If enabled, the extension field of the session will always be the primary extension on a telephone. If disabled, the extension field will contain the DN/extension that first answered the call. This only affects multiline phones. Enabled by default.
- h. Select the **Enable Selective Recording** check box to activate selective recording.
When the check box is selected, only the recordings of calls on turrets where a specific set of traders is logged in are saved. Other calls will be deleted.
When the check box is not selected, all recorded content on all turrets is kept.
- i. **Video Recording Mode**— Select one of the following options:
 - **Start On Trigger** - Do not record video calls for the extensions associated with this data source until a recording rule is triggered or an external API command starts recording. Video recording starts whenever the call starts, but video prior to the recording trigger is deleted.
 - **Application Controlled** - Record every video call for every extension associated with this data source, and then delete it. At any time during a call, a recording rule or an external API command can cause the recorder to keep the video call. If the call is kept, the recording includes all video from the start to the end of the call.
 - **Do Not Record** - Do not record video calls for extensions associated with this data source. Recording rules are ignored and cannot trigger the recording of video calls.
 - **Record** - Record all video calls for extensions associated with this data source. Only a block recording rule, AIM command, or external API command can prevent calls from being recorded.
- j. **Keep Duplicate Recording**—
For an N+N recording environment, select one of the following options:

- Select the **Keep Duplicate Recording** option when a customer's compliance recording policies require them to archive duplicate recordings of every call. To support this configuration, you must double the size of the Contact Database, the Archive Database, and the archive storage media.
- Clear the **Keep Duplicate Recording** option (default) so that the system deletes the secondary interaction after determining which copy to keep.



When N+N recording is configured, the system evaluates the interactions captured by both Recorders. It marks one as primary and the other as secondary based on several criteria, including call quality. For details, refer to *Selective Recording Configuration*.

Archive campaigns provide alternative methods for managing recordings in N+N environments. Set the N + N Dual Marking options to turn off the double-archiving of recordings, which keeps a single copy. For details, refer to *Campaign conditions*.

- k. **Require Replay Audio Redaction** - When redaction is enabled for the system, select whether redaction occurs for interactions that the data source captures. Redaction obscures sensitive customer information in captured audio and transcriptions. Select from the following for interactions that the data source captures:
 - **Disabled:** No information in the interaction is obscured. *Disabled* is the default setting.
 - **Always:** Sensitive customer information is obscured.
 - **In Fallback:** Sensitive customer information is obscured, but only in the event of CTI or recorder disconnection from the Integration Service.
 - l. **Require Replay Audio Morphing** - When morphing is enabled for the system, select whether replay of interactions captured by the data source requires morphing. Morphing changes the voice heard during replay such that the speaker remains anonymous and the audio remains intelligible. Select from the following options for interactions that the data source captures:
 - **Disabled:** The original voice of the agent and the customer are heard during interaction replay. *Disabled* is the default setting.
 - **Always:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting.
 - **In Fallback:** The voice of the selected channel or channels is morphed during interaction replay, as configured by the **Audio Morphing Channel** setting, but only in the event of CTI or recorder disconnection from the Integration Service.
 - m. **Audio Morphing Channel** - Enabled when **Require Replay Audio Morphing** is set to **Always** or **In Fallback**, choose the audio channel or channels that use morphing. Select from:
 - **Agent:** Only the voice of the agent channel is morphed during interaction replay. The voice on the customer channel is the original captured voice. *Agent* is the default setting.
 - **Agent and Customer:** The voice of the agent channel and the customer channel are morphed during interaction replay.
7. Under **Time Zone Settings**, specify a **Local Time Tagging Mode**. Select one of the following options:

- **Organization** - Select this option to base the time zone tagging on that of the organization. This setting is useful in scenarios where agents are working in different regions. The setting allows you to unify tagging across multiple time zones.
 - **Data Source** - Select this option to base time zone tagging on the time zone specified in step 5.
8. Expand the **Associated Integration Service Installations** area and select the server for the recorder for which you are configuring this data source.



In a Multi-Tenant SaaS environment, the tenant name associated to each Site Group, Site, and Server appears beside the Site Group, Site, and Server name on the right side of the Installations tree.

9. Under **Advanced Settings**, use the **Key** and **Value** fields to enter any proprietary pairs that are in use in your system. This should be done only in consultation with our field engineers.
10. Click **Save**. The new Trader data source is listed.

Related topics

[Editing a data source \(page 153\)](#)

[Deleting a data source \(page 157\)](#)

Editing a data source

1. Navigate to **Data Sources > Settings** in either the Integration Management or Recording Management module, and select the data source you want to edit.
2. Make changes to the editable fields/check boxes as required.



You *cannot* make changes to the following fields:

- The data source **Type** that you selected when you created the data source (for example, **Phone, Dialer, Operations, Quality**).
- The **Switch/Hub Type** you selected when creating a **Phone, Dialer** or **Trader** data source type.

3. Click **Save**. The changes to the data source are saved.

Creating a parent-child relationship between data sources

Parent and Child Phone Data Sources and Recorder Integration Service associations refer to the organizational structure and interaction between data sources and recording services.

Guidelines about parent and child phone data sources and Recorder Integration Service associations

- If the parent and child data sources are of the type Phone, the child data source is automatically associated to the same Recorder Integration Service as the parent data source.
- When you specify a parent data source for a child Phone data source, the Recorder Integration Service node specified for the child Phone data source is grayed out and cannot be changed. (As noted above, the Recorder Integration Service specified for the child data source is the same as that specified for the parent data source.)
- If you select the No Parent option for the child phone data source, the data source is no longer a child data source. However, the former child data source remains associated to the same Recorder Integration Service that it was associated to when it was in the parent-child relationship.

Procedure

1. Create the Phone or Collection data source you want to act as the parent.
2. Create one or more child Phone data sources.
3. As the **Data Source Parent**, select the data source created in step 1 from the dropdown list.
4. Click **Save**.
A data source nested under **Data Source Name** on the left indicates a parent-child relationship between data sources.

Related topics

[Creating Phone data sources \(page 132\)](#)

Viewing the data sources summary

You can view the list of data sources set up in your system on a summary page. This page lists the **ID**, **Name** and **Type** for each data source. You can also select a data source and edit or delete it.

Procedure

1. Navigate to **Data Sources > Settings** in either the Integration Management or Recording Management module,
2. Between the left and right panels on the page (between the **Data Source Name** panel and the **DataSource Settings** panels) click the right arrow.
3. The page refreshes, and the **Data Source Summary** page displays, with the list of data sources, showing their IDs, names and types.



If you have the **Org Scoped Data Sources** license, the summary page also displays the **Owner Organization** column for Operations, OutSourcer or Phone type data sources. The root organization displays for data sources that have no organization configured. This column is left blank for the other data source types.

4. To edit or delete a data source, select the data source, and do one of the following:

- To edit the data source, click **Edit Data Source**. The **Data Settings** page displays.
 - To delete the data source, click **Delete Data Source**.
5. To return to the original view, click the single left arrow at the right edge of the summary page.

Related topics[Editing a data source \(page 153\)](#)[Deleting a data source \(page 157\)](#)

Importing data source configuration

You can import configurations for Phone, Application, LAN (Screen), Radio, or Trader data sources from an external file. This feature allows you to reuse settings from previous versions or from other sources.

Procedure

1. Select the data source for which the configuration is to be imported.
The work pane refreshes to display the selected data source.
2. Click **Import**. The **Data Source Import** page displays.

3. Complete the fields in the **Data Source Import** page according to the following table:

Item	Description
Import Name	Specify a name to identify the import scheduling operation.
Import File Location	Click Browse and navigate to the folder where the file to be used for import scheduling is located.
Schedule Type	Select one of the three schedule types: • Import Immediately causes the import to take place immediately. No other entries are required. • Import Using Date and Time Within the File causes the import to take place on a scheduled basis at a time specified within the file, according to the choice of Local Time Zone or Universal Time Zone fields. Import Using Specified Date and Time causes the import to take place on a scheduled basis on a date and time specified in the Specify In and Date/Time fields.
Specify In	Select one of two time zone options if you selected a scheduled import (that is, a schedule type other than Import Immediately): • Local Time Zone causes the scheduled import to occur at the local time, so that, for example, imports would be made at different times across the globe. • Universal Time Zone causes the import to take place at a time relative to a universal time so that, for example, imports would be made at the exact same time all across the globe.
Date/Time	Shows the date and time of the import if Import Using Specified Date and Time is selected as the schedule type.

4. Click **Import**.

Exporting data source configurations

You can export a Phone, Application, LAN (Screen), Radio, or Trader data source.

Procedure

1. Select the data source to be exported.
The work pane refreshes to display the selected data source.
2. Click **Export**.
The **Windows File Download** page displays.
3. Click **Save** to save the selected data source configuration to a file you specify.
4. Accept the suggested file name, such as **datasource-export.csv** or type a different, more unique name.
5. Click **Save**.

Settings for the selected data source are saved to the Export File Location.

The following table lists the settings that are exported:

Data Source Type	Settings
Application	Settings, Member groups, Employee mappings, Recording profiles
LAN	Workstations, Workstation Groups, Association of Workstations to Workstation Groups, Workstation to Extension Associations
Phone	Extensions, Member Groups, Associations of extensions for Station-side Extension Pools, IP Extension Pools, Trunk Extensions Spans, Data Source Groups

Deleting a data source

When you delete a data source, you also remove all member group associations, employee mappings, and any other associates you made related to that data source. Some other settings, for example subnets on a LAN data source, that are inherent to that data source are also deleted. In addition, deleting a data source will stop recording of interactions from the data source.

Generally, you would delete a data source if you are changing the set of workstations or switches for which you originally set up the data source.



After deleting a data source, you will *not* be able to search for it in the Portal.

Procedure

1. Navigate to **Data Sources > Settings** in either the Integration Management or Recording Management module, and select the data source you want to delete.
2. Click **Delete Data Source**.
3. In the **Delete Data Source Confirmation** prompt, review the message regarding deleting the data source. If you still want to delete the data source, in the **Delete Data Source Confirmation** prompt, select the check box and click **Delete**.

Working with data source groups

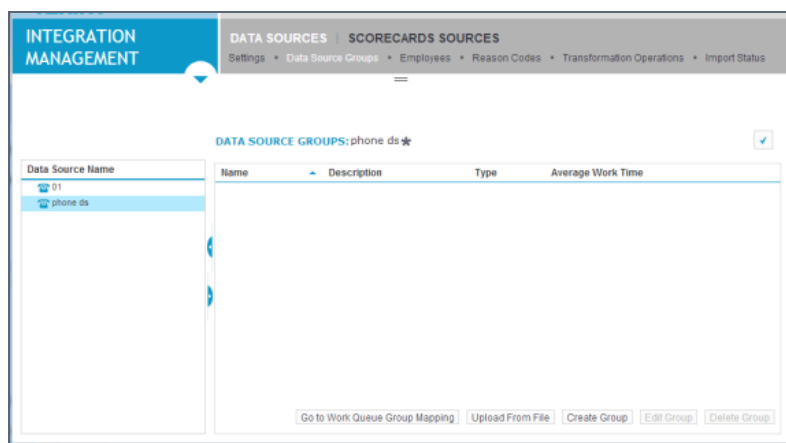
Data Source groups are groups of telephone extensions that allow automation. For example, in a certain type of group, incoming calls are passed from extension to extension within the group until the call is accepted, optimizing employee and extension usage. This section describes how to create and edit groups, import group information from a .csv file, and access the queues for multiple groups.

Data source groups also identify the particular entity for which you are scheduling or forecasting, such as group, skill set, queue, and more.

The **Data Source Groups** page is only available with certain data source types.

Procedure

1. Navigate to **Data Sources > Settings** in either the Integration Management or Recording Management module.
2. On the left pane, select the data source for which you want to create or edit a data source group.
3. Click the **Data Source Groups** page.



Related topics

[Creating or editing a data source group \(page 158\)](#)

[Uploading data source groups \(page 161\)](#)

Creating or editing a data source group

Procedure

1. Navigate to **Data Sources > Data Source Groups** in either the Integration Management or Recording Management module.
2. Select a Data Source in the left pane.
3. Do one of the following:

- Click **Create Group** to create a new Data Source group for the selected Data Source.
 - Select a Data Source group in the right pane and click **Edit Group** to edit an existing group.
4. Complete the following fields:
- **Data Source Group Name**—Type a unique name for the group. For Recorder configurations, it is determined by your switch type.
This is the identifier for the data source group record. This field should auto-populate new group names as they occur in CSI adapter imports. The data source group name is then mapped to queues in the Queue Group Mapping section.
For example, if your switch is Avaya, you would select either Hunt Group or VDN as the group “Type” (as described in the table below), then enter the actual hunt group or VDN number configured in the customer’s switch. Refer to the table below for complete details.
 - **Description**—Type a description of the group (optional).
 - **Type**—The available options in the drop-down list box depend on the switch type assigned to the data source when it was created. The options include the following:

Type	Description
Aastra	Select Hunt Group (to distribute phone calls from a single telephone number to a group of several phone lines).
Alcatel	Select Pilot Number. Pilot Number is a term used to refer to an Agent Group.
Aspect	For a phone data source, select Trunk Group or Agent Groups. For a dialer data source, select Call Queue or Agent Groups.
Avaya	For a phone data source, select one of the following: ■ Hunt Group - to distribute phone calls from a single telephone number to a group of several phone lines). ■ VDN - Vector Directory Number, which is a soft extension number. For a dialer data source, select Call Queue or Agent Groups.
Nortel	Select one of the following: ■ CDN - Controlled Directory Number, wherein calls are queued and can be routed or receive other commands. ■ ACD Queue DN (QDN) - an Automatic Call Distribution Queue, in which calls are held until an agent becomes available.
Cisco or Genesys	Select Route Points or Agent Groups.
Siemens	Select Call Queue.
Trunk Group	Collection of trunks used for the same purpose. An example is a trunk group of outbound trunks used for making outbound calls from a PBX.

Type	Description
Route Points	A queueing mechanism in a PBX to allow calls to wait for an available employee or be routed to different employees or locations based on information in the specific call.
Agent Groups	A collection of similar employees in a call center configured to handle the same type of calls
Hunt Group	Incoming calls are passed from extension to extension within the group until the call is accepted, such that phone calls are distributed from a single telephone number to a group of several phone lines.
Pilot Number	This is a term used to refer to an Agent Group.
VDN	Vector Directory Number, which is a soft extension number
CDN	Controlled Directory Number, wherein calls are queued and can be routed or receive other commands.
ACD Queue DN (QDN)	Automatic Call Distribution Queue, in which calls are held until an employee becomes available.
Call Queue	Calls are held until an employee is available.

See your switch documentation for more information about the distinctions between the above options, and select one of the following:

- **Average Work Time**—Shows the average work time in hours for the group, applicable only in the Workforce Management application, if licensed.

5. Click **Save**.

To edit a group:

1. Highlight the group you want to edit.
2. Click **Edit Group**.
3. If needed, edit the **Name** of the group.
4. If needed, edit the **Description**.
5. If needed, edit the **Average Work Time**.
6. Click **Save**. The page will refresh to display the data source group list with the saved group selected.

To delete a group:

1. Highlight the group you want to delete.
2. Click **Delete Group**. Confirm the deletion by clicking **OK**.

To go to the Queue Group Mapping page:

Click **Go to Queue Group Mapping** to go directly to the queue group mapping page.

Uploading data source groups

You can export Data Source Group information in .csv format. You must ensure that the data being uploaded is in the proper format to be accepted by the Data Source.

Procedure

1. Click **Data Sources > Data Source Groups** in either the Integration Management or Recording Management module, and select a data source from the left pane.
2. Click **Upload from File**.

Field Name	Column Number	Default
☒ Name	1	
☒ Queue	2	
☐ Average Work Time	3	0

3. Complete following fields:
 - **File**—Click **Browse** to locate the .csv file containing the information to be uploaded to the Data Source.
 - **Delimiter**—Specify how the fields in the .csv file are separated: Comma, page, or Semi-colon.
 - **Prefix for comment lines**—Type the character used to indicate lines to be ignored (if applicable).
 - **Data Source**—Identifies the data source.
4. Under Field Name, select each field that appears in the .csv file, and then type the column number in which it appears.
 - Beside the **Average Work Time** field you can type a default value to indicate the average work time per employee, in hours (for WFM tracking only).
 - Beside the **Media** field you can select a default media type: **Voice over IP, Callback, Chat, Email, Fax, Phone, or Phone Outbound**.
5. Click **Upload**.



To cancel without uploading, click **Cancel**.

Skills mapping

The skills mapping feature allows you to map skills to queues for use with outsourcing. The **Skills Mapping** page is only visible if you created an Outsourcer data source.

Procedure

1. Navigate to **Integration Management > Data Sources > Settings**.
2. In the left pane, select the Outsourcer data source for which you want to create or edit skills mapping.
3. Click the **Skills Mapping** page.

The right panel consists of a table with three columns:

- The **Name** column displays all data source skill mappings that have been created.
- The **Description** column gives a brief description of the data source.
- The **Mapped Skill** column lists the skill that has been mapped.

Related topics

[Creating or editing skills mapping \(page 162\)](#)

Creating or editing skills mapping

You can create, edit or delete skills mappings.

Procedure

1. Click **Create Mapping**.
2. Specify a name for the mapping in the **Name** field.
3. Give a brief description of the data source in the **Description** field.
4. Select the mapped skill using the drop-down menu.



You can do this step later; you do not need to map the skill when you first create a skill mapping.

5. Click **Save** to save your mapping and return to the **Skills Mapping** page.

Click **Cancel** to return to the **Skills Mapping** page without saving.

Click **Revert** to cancel any changes you have made to this page. You remain on the mapping creation page.

Editing or deleting a skills mapping

To edit the name, description, or change the skill for any mapped skill, click **Edit Mapping** and replace the content in the fields.

To delete an existing mapping, click **Delete Mapping**. Only the mapping is deleted; skill information is not deleted.

Activity mapping

The activity mapping feature allows you to map activities to queues for use with outsourcing. The **Activities Mapping** page is only visible if you created an **Outsourcer** data source.

Procedure

1. Navigate to **Integration Management > Data Sources > Settings**.
2. On the left panel, select an Outsourcer data source for which you want to create or edit skills mapping.
3. Click the **Activities Mapping** page.

The right pane consists of a table with these columns:

- The **Name** column displays all data source activity mappings that have been created. You specify the name at the time of creation.
- The **Description** column gives a brief description of the data source. You also specify the description at the time of creation.
- The **Mapped Activity** column lists the activity that has been mapped.
- The **Owner Organization** column indicates the organization for which the activity was created.

Related topics

[Creating and editing activity mapping \(page 163\)](#)

Creating and editing activity mapping

Procedure

1. Click **Create Mapping**.
2. Specify a name for the mapping in the **Name** field.
3. Give a brief description of the data source in the **Description** field.
4. Select the relevant organization using the drop-down menu.
5. Select the mapped activity using the drop-down menu.



You can do this step later; you do not need to map the activity when you first create an activity mapping.

6. Click **Save** to save your mapping and return to the **Activity Mapping** page.
Click **Cancel** to return to the **Activity Mapping** page without saving.
Click **Revert** to cancel any changes you have made to this page. You remain on the mapping creation page.

To edit or delete an activity mapping:

To edit the name, description, organization, or change the activity for any mapped activity, click **Edit Mapping** and replace the content in the fields.

To delete an existing mapping, click **Delete Mapping**. Only the mapping is deleted; activity mapping information is not deleted.

Map employees to data sources

You can map employees to data sources to provide employees in your organization with a switch ID, and associate this ID with data sources such as a phone switch or LAN.

Data sources appear in the left pane, and only those employees associated with a data source appear in the right pane.

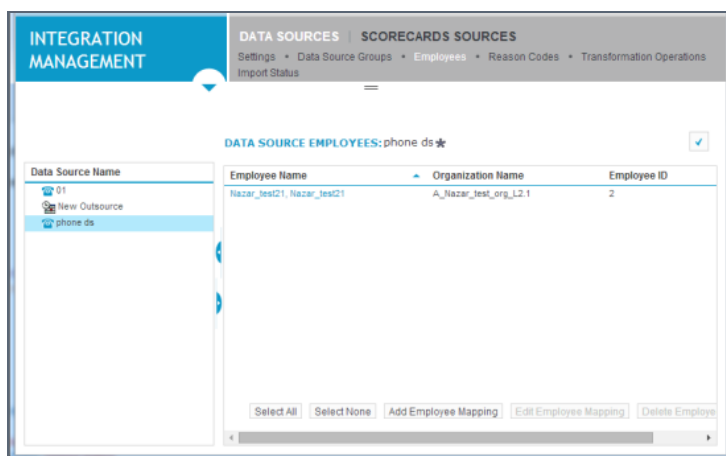
You can add, edit and delete employee mappings, as described in the following topics:



Only phone, LAN, and dialer data sources allow you to record on a per-employee basis. For a LAN data source, you can only give employees a Login ID. You must have the “View and Configure Data Sources” privilege to edit these employee settings.

Procedure

1. Navigate to **Data Sources > Employees** from either the Integration Management or Recording Management module, and select the data source to which you want to map employees.
2. Click the **Employees** page.



If employees have already been mapped to the data source, they are listed in the right panel of the page, with columns that indicate their name and organization, and as applicable, the Employee IDs, extensions, and network extensions to which they are associated.

Related topics

[Selecting employees for employee mapping \(page 165\)](#)

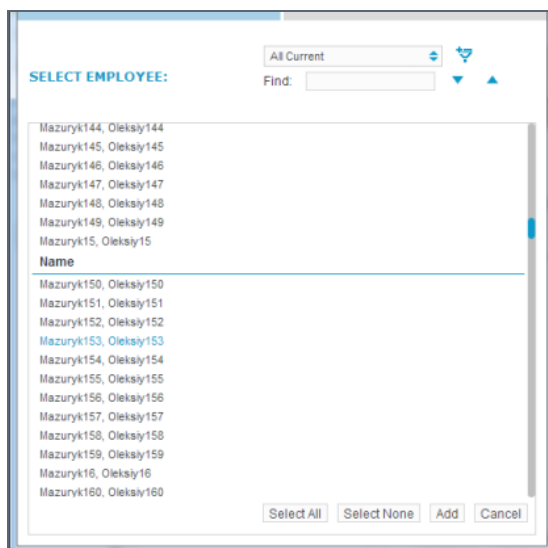
[Creating and editing employee mappings \(page 166\)](#)

Selecting employees for employee mapping

1. Select a data source at the left side of the page.
2. Click **Add Employee Mapping**. The **Select Employee** page displays.



If you have a license for **Org Scoped Data Sources**, only those employees whose current organization assignment is to the data source organization (or a child of that organization) is available for mapping.



3. Select the employees you want to map. You can select employees using the following methods:
 - Selecting one or more displayed employees, and then clicking **Select**. (You can select multiple employees. Click an employee's name and then use the **Shift** key to select a contiguous range, or the **Ctrl** key to select non-contiguous employees.)
 - Clicking **Select All** or **Select None** to select all or deselect all employees respectively.
 - Typing the employee's name or a few letters of the name in the **Find** area, selecting a filter from the **View** area, and then clicking **Go** to find an employee.
 - You can also search for and filter employees if you have a large number of employees
4. Click **Add**.

The pop-up page closes, and the main page refreshes to display a page where you can create or edit mappings for the employees you selected.

Related topics

[Creating and editing employee mappings \(page 166\)](#)

Creating and editing employee mappings

1. Select a data source at the left side of the page and do *one* of the following:
 - If creating a new employee mapping, complete the procedure, [Selecting employees for employee mapping \(page 165\)](#).
 - If editing an existing employee mapping, select the an employee from those listed on the right panel on the page and click **Edit Employee Mapping**.

Based on the setting of **Seating Arrangement** for the data source on the **Settings** page of the **Data Sources** section of the **System** module, a page is displayed, labeled one of the following:

- **Create/Edit association between employee and employee ID**
- **Create/Edit association between employee and extension**
- **Create/Edit association between employee, employee ID and extension**
- **Create/Edit association between employee and network login ID**

This page allows you to create or edit the mappings and associations for the employees you selected.

Column	Description
Employee Name	The name of the employee(s) you previously selected.
Organization Name	The organization to which the employee belongs.
Employee ID	The data sources with which the employee can be associated. Note: This column is not displayed if the Seating Arrangement setting is Free Seating or Hybrid , nor for LAN data sources.
Extension	This a field or drop-down list of extensions. Extensions are the interval at which the adapter tests that the devices are still valid and monitored. This column is only displayed for PBX/ACD data sources, when the Seating Arrangement setting is Fixed or Hybrid .
Network ID	The user's computer login ID. This column is only displayed for LAN data sources.

2. Place the cursor in the field to be edited.
3. Type or select the required information, whether Employee ID and/or Extension, or Network ID.
4. Click **Save**.

Related information

Create and edit mappings on the **Profiles** page of the **People** module (*User Management Guide*)

Creating and editing reason codes

Reason codes are two part codes that consist of an Event mode and an Event reason. Time Collection reason codes are the codes that a data source, typically an ACD, sends to the Workforce Optimization Solution when an employee logs in, logs out, or changes state.

My Time reason codes are the codes that the Workforce Optimization Solution can send to a data source, typically an ACD, to change the state of employees' phones.

Terminology varies among ACD vendors but the Event modes are often referred to as states, events, or modes on the ACD.

The Reason Codes feature is only available for Phone data sources.

When you create Reason Codes, the names must be unique.

Procedure

1. Navigate to **Data Sources > Settings** from either the Integration Management or Recording Management module.
2. On the left pane, select the data source for which you want to view, create or edit reason codes.
3. Click the **Reason Codes** page.

The **Data Source Reason Codes** list displays in the right panel of the page, with columns for **Reason Code**, **Event Mode**, **Event Reason**, **Shift Operation**, and **Origin Data Source**.

Event Reason values are dictated by the data source. Consult the data source documentation to determine the correct values. The Event Reason **UNAVAILABLE** means that no Event Reason will be sent to or received from the data source for that particular Event Mode.

The **Shift Operation** column determines the impact the reason code has on the shift. For example, some sites have several reason codes for **Logoff**. When an event that is marked as **End Shift** is received, the system closes the shift.



Each set of reason codes should have at least one reason code with a **Shift Operation** of **End**.

Related topics

[Create and edit reason codes \(page 168\)](#)

Create and edit reason codes

1. In the right panel, select the data source for which you are creating the reason code.
2. Click **Create Reason Code**. The **Data Source Reason Codes** page opens.

3. Type the name of the reason code.
4. Type the Event Mode.
5. Type the Event Reason.
6. Select the reason code's Shift Operation from the drop-down list.
7. Click **Save**. The reason code is listed in the left pane.

To edit an existing reason code:

1. In the left pane, select the data source for which you are editing the reason code.
2. In the right pane, highlight the reason code you want to edit.
3. Click **Edit Reason Code**. The Data Source Reason Codes page opens with the reason code's current data.
4. Make any needed changes and click **Save**.

To delete a reason code:

1. In the left pane, select the data source the reason code belongs to.
2. In the right pane, highlight the reason code you want to delete.
3. Click **Delete Reason Code**, then confirm the deletion.

Related topics

[Uploading reason codes from a file \(page 169\)](#)

Uploading reason codes from a file

To ease the process of creating reason code definitions, you can upload the definitions to the server from a text file by clicking **Upload From File**.

To create a reason code file:

The file is delimited, using either commas, semi-colons, or tabs as field separators, and can have any file extension, such as **.txt**, **.csv**, or other extensions.

The file should contain the following:

1. A header line.

The header line is identified by the “comment” character at the beginning of the line. For example:

#ReasonCode_Name Event_Mode Event_Reason Purpose ShiftOperation

By default, the comment character is #, but you can specify a different character.

2. The definition of the reason codes.

The following parameters can be provided for each reason code:

- a. Mandatory fields:

- **Name**—a unique name for the reason code
- **Event Mode**—the main employee state mode code
- **Event Reason**—the secondary employee state mode code

- b. Optional field:

- **Shiftoperation**—Use the drop-down menu to select either **End** or **None**.

For example:

Login, 1101,0, ,None

Not-Ready, 1103,0,,End

To upload a reason codes file:

1. At the bottom of the **Reason Codes** page, click **Upload From File** to open the **Upload Reason Codes** page.
2. To locate the reason code file, click **Browse**, navigate to the file and select it. Then click **Open**.
3. In the **Delimiter** drop-down list box, select the delimiter for the file (typically **Comma**).
4. If applicable, in the **Prefix for comment lines**, enter the appropriate parameter (for example, #).
5. Complete additional details under the **Field Name**, **Column Number** and **Default** columns, as required.
6. Click **Upload**.

Once the file is successfully uploaded, the page closes and the uploaded reason codes populate the page.

Working with operations in Workforce Management

Operations features are only available if you are licensed for Operations.

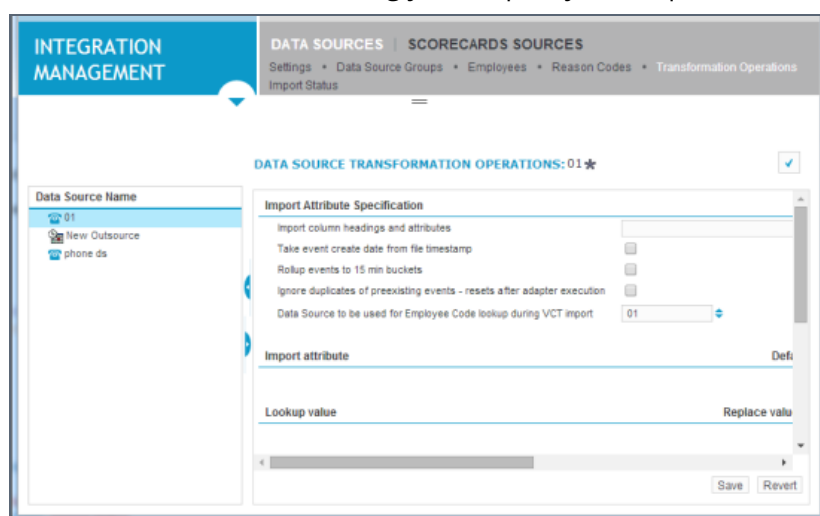
Related topics

[Transformation Operations \(page 171\)](#)

[WIT Configuration \(page 175\)](#)

Transformation Operations

The **Transformation Operations** selection is only visible if you are licensed for the Operations features, and have created an Operations data source that consists of a data source selector pane and a number of areas allowing you to specify the required data transformations.



The transformation you specify here is a step in the processing of the Operations – Event File Import and Transform adapter and the Operations – Arrival Processing adapter. The information you supply governs the mapping, processing, and conversion from the import file format(s) to the data schema used in Workforce Management.

The transformation is configurable for each individual Operations data source. The adapters provide for the scheduling and periodic execution of the transformations.

The configuration of the Operations – Event File Import and Transform adapter governs the mapping between data import frequency, data transformation, and import file location. A new adapter needs to be created for each variation in those items.

The **Transformation Operations** page consists of a Data Source Name selector and six data areas on the right-hand portion of the page:

- **Import Attribute Specification**
- **Import attribute | Default value**
- **Lookup value | Replace value**
- **Import attribute | Filename mask**
- **Operations attribute**
- **Import Attribute Specification** (check box)

The following information is an overview of the process for creating a transformation.

To specify a transformation for an operations data source:

1. Select an operations data source in the Data Source Name selector pane.
2. Specify the column headings of the import file. The **Import column headings and attributes** field is a text box. Enter the headings as a comma-separated text string. The headings should be in the order that they appear in the import file. Column headings must be single words; no spaces are allowed.
3. Check the **Take event create date from file timestamp** box to use the import file's timestamp as the imported events' creation date. This box is used in case the file to be imported doesn't have a Date column. You can then select the file timestamp as the date to be shown next to each event that is in the file. Selecting this option disables the **Create Date** row in the **Operations attribute** table. (The box next to **Create Date** is empty; no Date name needs to be entered in the **Import column headings and attributes** field.)
4. Check the **Rollup events to 15 min buckets** box to roll up event data within 15 minute "buckets." This is to reduce the number of events where very fine grained data is imported.

For example, consider an import file with the following data:

```
Count,DS, ID, Event, Value, Date
0, Oahu, 1A, 1, 10, 10-11-2007 09:00:00
1, Oahu, 1A, 1, 20, 10-11-2007 09:01:00
2, Oahu, 1A, 1, 15, 10-11-2007 09:06:00
3, Oahu, 1A, 1, 10, 10-11-2007 09:10:00
4, Oahu, 1A, 1, 5, 10-11-2007 09:15:00
5, Oahu, 1A, 1, 12, 10-11-2007 09:29:00
```

If you were to roll these up into 15 minute buckets, you would see two events in the web application: those from 09:00:00 through 09:14:00, and those from 09:15:00 through 09:29:00. The aggregate of the first event would be 55 (10+20+15+10), and the second 17 (5+12).

5. Check the **Ignore duplicates of preexisting events - resets after adapter execution** box to remove duplicates of preexisting events from the imported data. This check box resets after each adapter execution.
6. Optionally specify attributes and default values by clicking **Add** and specifying an Import attribute and its associated default value.

Some files have default, unspecified data on a per file basis. You can specify attributes and default values on a per data source basis. These attributes can then be treated just like a column attribute from within the file. For example, they can be used with a mask, arithmetic processing, aggregated with other columns, and so forth.

For example, if a file did not contain a Date column, you could specify a default value for Date.

7. Specify look-up values and replacement values by clicking **Add** and specifying a value to look for in the import file, and the value to convert it to upon import.

This feature is especially useful if, for example, you have too many data source groups. Consider an import file with the following data:

```
Count,DS, ID, Event, Value, Date
0, oahu1, jane, 1,100, 10-12-2007 09:00:00
1, oahu1, jane, 2, 20, 10-12-2007 09:00:00
2, oahu1, jane, 3, 15, 10-12-2007 09:00:00
3, oahu2, jane, 1,100, 10-12-2007 09:00:01
4, oahu2, jane, 2, 20, 10-12-2007 09:00:01
5, oahu2, jane, 3, 15, 10-12-2007 09:00:01
6, oahu3, jane, 1,100, 10-12-2007 09:01:01
7, oahu3, jane, 2, 20, 10-12-2007 09:01:01
8, oahu3, jane, 3, 15, 10-12-2007 09:01:01
9, oahu4, jane, 1,100, 10-12-2007 09:02:00
10, oahu4, jane, 2, 20, 10-12-2007 09:02:00
11, oahu4, jane, 3, 15, 10-12-2007 09:02:00
```

You can consolidate the four different data source groups typing the same value for all four in the **Replace value** field beside each **Lookup value** field.



If two or more Data Source Groups have events that take place in the same time, the same type events should be aggregated.

8. Specify any file name masking needing to be done by clicking **Add** and specifying the column containing the data and the file name mask to apply.

The file name may be used to transfer information that applies to all of the events within the file. Attributes can be declared and masked out of the file name. These attributes can then be treated just like a column attribute from within the file. For example, they can be used with a mask, arithmetic processing, aggregated with other columns, and so forth.

Use the character **X** to extract a character from the file name, and the underscore character **_** to ignore a character.

For example, if your input file name contained both the employee ID and the data source group name, such as **Oahu,jane.csv**, type a **Filename mask** value beside the related **Import Attribute** field.

9. Specify the transformation for each Operations attribute you want to make on the data. There are five basic operations available to apply to transforming the data:

- Column to data field mapping, including aggregation of multiple columns.
- Date formatting.
- Arithmetic operation
- Lookup and replace operation
- Masking

These operations can be combined (with some restrictions) for each required Operations attribute. The list of Operations attributes is:

- **Event type:** Arrival, Check-out, Check-in, Work-in-Progress (WIP). This field is mandatory.
- **Value:** Amount of work for the event.
- **Employee ID:** Identifies the employee. This is the **Employee ID** specified for the data source on the **Profiles** page in the **People** module for that employee. The is alpha-numeric, and unique.
- **Data source group:** Data source group name for the event.
- **Create date:** Date of the event.

For example, consider an import file with the following data:

Count,DS, ID, Event, Value, Date

0, Oahu, 1A, 1, 3, 10-11-2007 09:00:00

1, Oahu, 1A, 1, 4, 10-11-2007 09:01:00

The Operations attributes would then be entered as:

Event type: Event

Value: Value

Employee number: ID

Data source group: DS

Create date: Date



Import files generally have one additional column that is usually named **Count**. This column shows the number of rows that have data in the file to be imported. This column needs to be among the column headings listed in the **Import column headings and attributes** field near the top of the page.

For the arithmetic and logical operations, enter the calculation, in terms of the import file column headings.

Spaces must be entered before and after mathematical operators. Formulas that include parentheses are not supported. For example, **a*(b+c)** should be entered as **a * b + a * c**

For the mask, enter the pattern to apply.

For example, if the file to be imported has the information for Employee ID and Data Source Group shown in one column (DS_ID), such as oahu_jane, you could use the following mask:

Operations attribute	Import attribute	Mask
Event Type	WorkType	
Value		
Employee ID	DS_ID	____X000
Data Source Group	DS_ID	XXXX____
Create Date	StartTime	

For the Date Format, select one of the date formats from the drop-down selector.

10. To auto-create data source groups, check the **Create Data Source Group - no event population, resets after adapter execution** check box. This check box can be used the first time you import data, to facilitate the creation of data source groups. No other data is imported this time.



Once created, these data source groups then have to be manually mapped to respective queues in the **Work Queue Group Mapping** page under **Work Queues** in the **App Admin** module. Once mapped, the first file has to be re-imported to populate the rest of the VCT data.

11. Click **Save** to save your transformation.
12. To use the Operations data source for which you configured the transformation, configure an Operations - Event File Import and Transform adapter. Refer to the online help for the Operations - Event File Import and Transform adapter for more information.

WIT Configuration

Work Item Tracking (WIT) data that is imported from Operations data sources typically contains a number of standard attributes, including:

- Employee
- Data Source Group (mandatory)
- External ID (mandatory)
- Status
- Age
- Is Workable
- Creation Date
- Closed Date
- Closed By
- Created By
- Description
- Type

For items that cannot be mapped to one of the standard attributes, this page allows you to define settings for custom attributes.

Click **Add** in the top page area to create a custom attribute and specify:

- a name for the attribute
- its data type (**DATE**, **TEXT**, or **NUMBER**)
- whether the imported data is a collection (the imported field contains multiple delimited values)

- the separator character used in a collection (# or @)
- miscellaneous settings
 - the units (**Hours** or **Days**) for its aging buckets
 - the fields from the data source that can be used in filters for WIT dashboards and reports
 - **External URL for WIT Tickets** - this is the URL of the external CRM system to which you can link your WIT drill down report.

Depending on the external system's URL, ensure that you type **={0}** in the appropriate location in the URL address.

The **{0}** is replaced with the correct external id contained inside the report, so that it links to the correct external system and also exactly to the appropriate ticket.

Wherever you insert this **{0}** in the URL address, it is replaced with external id.



You *must* enter a URL in this field if you are using the WIT drill down report to identify tickets in an external CRM system.

When the user clicks the leaf node in the WIT drill down report, it shows the details of the tickets in a pop-up report page. When you click the External ID in the pop-up page, the user is linked to the external system.

Click **Add** in the middle page area to create age buckets for the data source. Up to seven age buckets can be defined per data source. This container allows you to specify:

- the age bucket name
- its lower limit
- its upper limit
- an optional description

Click **Add** in the bottom page area to define custom status types that reflect a specific Customer Relationship Management (CRM) system's definitions for ticket status, and map these custom status types to WIT standard status types. (You can then search for these custom status types using the WIT filter in WIT dashboards.) The container allows you to specify:

- the custom status name
- the WIT status to which it is mapped (**ASSIGNED, ON HOLD, REOPEN, REASSIGNED, CLOSED, OPEN**)

For existing items, select the item and click **Delete** in its container to remove that item from the data source definition.

When you are finished making changes, click **Save** to save your changes, or click **Revert** to cancel any changes you have made since last saving.



When the WIT configuration is saved, the WIT Aging Charts and WIT Drilldown Chart are automatically created on the My Dashboards page.

Related information

Workforce Optimization Dashboard Guide

Cache features

This section describes how to use the system's cache features.

Topics

Configuring and viewing the system cache	179
Cleaning the cache	182

Configuring and viewing the system cache

The system includes a page from which you can view details about the system's various caches.

You can access the Cache page from the System Monitoring module in the suite web application, or you can use an external URL to display the page.

The Cache page is separated into three areas:

- The upper two areas of the page are used by our programmers to diagnose programming problems. The information in these two areas relates to Java objects used in our application code.
- The lower area of the page is used to diagnose and verify server cluster configuration. From this area, you can verify the number of hoses, cache nodes, host identities and so on.



To be able to view the Cache page, you need to have the View Cache privilege assigned to your role. To edit privileges associated with a role, navigate to **User Management > Role Setup**.

Related topics

[Using the cache for programming diagnostics \(page 179\)](#)

[Viewing server cluster configuration \(page 180\)](#)

[Using the cache from an external URL \(page 181\)](#)

[Cleaning the cache \(page 182\)](#)

Related information

Edit privileges associated with a role (*Workforce Optimization User Management Guide*)

Using the cache for programming diagnostics

1. Navigate to **System Management > Log > Cache**.
The **Cache** page opens.
2. From the **Select Cache** drop-down list, select the cache that you want to view for diagnosing programming problems.
3. To narrow the number of cache items displayed for programming diagnostics, enter the IDs for the items that you want to see for a particular cache in the **Enter ID(s) for which to retrieve cache** text box. You retrieve these item IDs from tables used in programming databases. Separate each ID number by a comma.
4. Click **Refresh**.

The page refreshes as follows:

- Beside **Object ID**, the number of objects (IDs) displays.
- The **Cache Content** text box contains a description of the cache contents. View these for verification and program diagnostics.

Viewing server cluster configuration

1. Navigate to **System Monitoring > Log > Cache**.
The **Cache** page opens.
2. From the **Select Cache** drop-down list, select the cache for which you want to view or verify server cluster configurations.
3. Click **Refresh**.

When the page refreshes, in the bottom third of the page you see a row for each host related to the cache, with the following columns of information:

- **Host:** identifies the IP address of the identified hosts or cache nodes.
- **ServerName From DB** and **Server Port:** indicate whether the identified host(s) are connecting to the appropriate database.
- **Cache is Clustered:** for clustered servers, the value is **Yes**. Some servers are shown with their cache but not their server names. Server names and server port information are retrieved from the same shared database.
- **Cache Port:** indicates the port number through which the cache services communicate between the clustered servers. The default is 8088. Consistency across a cluster is good practice.
- **Cache Start Time:** indicates the time at which the cache service starts.
- **Synchronized:** indicates the results of the synchronization test across a server cluster.

Related topics

[Troubleshooting server cluster configuration \(page 180\)](#)

Troubleshooting server cluster configuration

- What am I looking for when I verify the lists of Host and Server Names from DB on the page?

When you view the two lists of host IP addresses and server names, make sure all servers in your cluster are listed there.

- If any of the servers are missing, you need to check that the Weblogic server is running and pointing to the database expected.
- If you see an unexpected machine in the lists, some unknown Weblogic server is pulling ['stealing'] the database connection from your database. This can cause data inconsistency. Therefore, you need to detach the Weblogic server from your database, and then run the SQL command **delete from appserver** against your the BPMMainDB database, and restart all the servers.
- Why are some of the servers shown only with their Cache information but not with their server names?

Some of the servers may be seen according to their Cache information, but not their server names. Server Name and Server Port information derives from the database. This view means that the servers are sharing same database.

- What if the Cache Port column indicates a port number other than the default 8088?

By default, the Cache port number is 8088. This is the port number through which the cache services communicate with each other. A different port number does not necessarily mean there is a problem, but consistency across Weblogic servers is good practice.

- What does it mean when the Cache Start Time column is blank, or there is a big interval between 2 cache start times?

- Cache Start Time column is blank:

If there is a **No** shown under the **Cache Is Clustered** column, and if the **Cache Port** and **Cache Start Time** columns show no values, the cache service is probably down.

- Large interval between two cache start times:

If you see a large interval between any two cache start times, the most recent time probably means there is a service restart, possibly a sign of a problem

- How do I interpret 'yes' or 'no' under the Synchronized column?

This column indicates the results of the synchronization test across a cluster.

If the value is **Yes**, the cluster is synchronized. If the value is **No** for one or more cluster, you need to investigate the problem.

Using the cache from an external URL

You can sign into the Cache Viewer from an external URL.

In your internet browser's address bar, type the following URL:

http://yourhost:yourport/wfo/control/system_cache_public

The Cache Viewer page opens and displays the most recently selected cache information.

Related topics

[Using the cache for programming diagnostics \(page 179\)](#)

[Viewing server cluster configuration \(page 180\)](#)

Cleaning the cache

You can clear a cache by selecting a cache and then clicking the **Clean Cache** button.

1. Navigate to **System Monitoring > Log > Cache**.

The **Cache** page opens.

2. From the **Select Cache** drop-down list, select the cache you want to clean.
3. Click **Clean Cache**.

When you clean the cache, the caches of bluepumpkin/workresource manager and witness/role manager are reinitialized immediately.

Related information

[Configuring and viewing the system cache \(page 179\)](#)

System administration for suite servers

This section provides an overview of the system administration tasks that may be required to support the suite's servers and server accounts, including SSO configuration.

Topics

Overview of suite server system administration tasks 184

Overview of suite server system administration tasks

These tasks are described in the following sections:

Chapter	Content
Changing ports (page 278)	Describes how to change WebLogic ports.
Changing server computer names, domains, and workgroups (page 233)	Describes how to change the computer names or the Windows domain memberships (or both) of the servers in your environment.

Changing System Accounts

The system has multiple user accounts to manage, including the Management and Database Management Service Accounts, the internal recorder and EMA accounts, the System Accounts, and the application authentication accounts.

Topics

Change passwords for existing MSA or DMSA accounts	186
Change the SQL Services account	200
Change the Enterprise Manager Agent application user accounts	201
Change the Import Manager application user accounts	204
Change the System Account (DB Realm)	205
Change the System Account (Windows Authentication)	206
Change the WebLogic Administrator Account Password (DB Realm)	207
Workflow: Change the WebLogic 12.x Administrator Account (Windows Authentication) ..	208
Workflow: Change the WebLogic 14.x Administrator Account (Windows Authentication) ..	221
Change the SSObind account	231
Create TAS user group and TAS user accounts	232

Change passwords for existing MSA or DMSA accounts

Use these instructions to make changes to the Management Service Account (MSA) or the Database Management Account (DMSA) after the initial installation and configuration of the system.

The MSA account is a required account. Servers in the enterprise use the credentials of the MSA account to access services in the system.

The DMSA account is *optional*:

- If you use a DMSA account in your enterprise, database-related tasks on the managed servers use the credentials of this account to access and configure all databases in the system.
- If you do *not* use a DMSA account in your enterprise, the MSA account credentials are used for this purpose.

Related topics

[Change the Password of the Existing MSA or DMSA Account \(page 186\)](#)

[Change the MSA or DMSA Account to a Different Windows Account \(page 189\)](#)

Change the Password of the Existing MSA or DMSA Account

Before you begin

Ensure configuration distribution is successful to all servers in Enterprise.

Password change process takes some time to distribute to all servers. While this configuration is being distributed MSA/DMSA accounts need to be kept unlocked (Disable the user lockout policy in AD).

Follow this procedure to continue using the same Windows account as the MSA or DMSA account, but change the password of the account.



If DB permissions have been manually assigned and a database password has changed, refer to the *Assign DB permissions manually* section of the SQL Server Installation and Administration Guide for additional instructions.

Procedure

1. Change the password of the Windows accounts that serve as MSA/DMSA

Step 1 of 5 associated with changing only the password of the MSA or DMSA accounts.

In this step, you change the password of the Windows account that serves as the MSA or DMSA account:

- If MSA/DMSA accounts are configured in any other places manually (such as Scheduled Task or COM+ Applications), these places need to be updated manually with correct password.

- If you are changing the password of the DMSA account, change the password of the Windows account that serves as the DMSA.

2. Change the SSRS Service User

Step 2 of 5 associated with changing only the password of the MSA or DMSA accounts.



Perform this procedure *only* if you are changing the MSA. If you are *only* changing the DMSA, skip this procedure and continue to [Change the DMSA/MSA Accounts \(step-by-step\) \(page 192\)](#).

In this step, you change the password of the MSA account that runs the report server service. Perform this procedure from the server that hosts the Reporting Services server role.

Procedure

1. From Windows, launch the **Reporting Services Configuration Manager** application.
2. In the **Reporting Services Configuration Connection** window:
 1. Ensure that the **Server Name** and **Report Server Instance** fields specify the values appropriate for the computer running SQL Server that hosts the Reporting Services database.
 2. Click **Connect**.
3. In the left-pane, select **Service Account**.
4. Select **Use another account**.
 - In the **Account (Domain\user)** field, enter the domain\username of the existing MSA account.
 - In the **Password** field, enter the new password of the MSA account.
5. Click **Apply**.
6. In the **Backup Encryption Key** window, complete these fields:
 - **File Location** - Specify the file name and location of the file that will contain the backup encryption key.
 - **Password/Confirm Password** - Type a password to protect the file from unauthorized access. The password must be at least 8 characters, include a combination of uppercase and lowercase alphanumeric characters, and at least one symbol character.
7. In the **SQL Server Connection Dialog**, you must specify the credentials of an account that has permission to access the Reporting Services database. The MSA account has this permission. Complete the fields as noted below:
 - **Server Name** - Specify the name of the computer running SQL Server that hosts the Reporting Services database.
 - **Credentials Type** - Select one of the following from the drop-down box.
 - **Current User - Integrated Security** - Select this option if you are currently logged into Windows using an administrator account that has the permission to access the Reporting Services database. If you select this option, you do not need to enter a user name and password.
 - **SQL Server Account** - Select this option to specify the credentials of an account that has

permission to access the Reporting Services database. If you select this option, enter the username and current password for this account in the fields provided.

8. Click **OK**.

3. Configure MSA/DMSA in the Enterprise Settings

Step 3 of 5 associated with changing only the password of the MSA or DMSA accounts.

In this step, you change the Database Management Account or Management Service Account passwords on the Enterprise Settings screen.

Procedure

1. Select **System Management > Management > Enterprise Settings**.
2. In the Installations tree (left-hand pane), select the **Enterprise** node.
3. Perform the appropriate procedure(s) below:
 - If you are changing the password of the MSA account, in the **Management Service Account** section, enter the new password in the **Password** field.
 - If you are changing the password of the DMSA account, in the **Database Management Account** section, enter the new password in the **Password** field.
4. Click **Save and Apply to Children**.
5. Assign DB permissions automatically using the *Database Permissions Configuration Tool*, or manually.

For details, see the *SQL Server Installation and Upgrade Guide*.

4. Stop and start the Watchdog and WFO_ProductionDomain_ProductionServer services on the clustered application servers

Step 4 of 5 associated with changing only the password of the MSA or DMSA accounts.

In this step, you stop and start the Watchdog and WFO_ProductionDomain_ProductionsServer services on the clustered application servers.

Procedure

1. From the Windows desktop of any application server in the cluster:
 - a. Open the **Windows Administrative Tools** and then select **Services**.
 - b. Right-click on the **Watchdog** service and select **Stop**.
 - c. Right-click on the **WFO_ProductionDomain_ProductionServer** service and select **Stop**.
2. Repeat step 1 of this procedure on the remaining servers in the cluster.
3. From the Windows desktop of any application server in the cluster:

- a. Open the **Windows Administrative Tools** and then select **Services**.
- b. Right-click on the **WFO_ProductionDomain_ProductionServer** service and select **Start**.



Do not continue to the next step until the service starts and you can successfully log in to the Enterprise portal.

- c. Right-click on the **Watchdog** service and select **Start**.
4. Repeat step 3 of this procedure on the remaining servers in the server cluster.

5. Review the alarms again and resolve active alarms

Step 5 of 5 associated with changing only the password of the MSA or DMSA accounts. In this step, you use the Alarm Dashboard to resolve all active alarms in the system.

Procedure

1. Click **System Monitoring > System Monitor > Alarm Dashboard**.
2. Resolve every active alarm that appears in the **Enterprise Alarms** pane.
 1. Click on an alarm in the **Enterprise Alarm** pane.
 2. In the **Details** pane, review the **Corrective Action**: for the alarm.
 3. Perform the corrective action steps for the alarm.
 4. Click on an alarm again in the **Enterprise Alarm** pane.
 5. Click on **Servers** to display the Servers pane.
 6. In the Servers pane, click the **Acknowledge** icon  to acknowledge the alarm.
 7. Repeat steps a-f for every alarm in the **Enterprise Alarms** pane.
3. Allow the system to stabilize by ensuring that none of the alarms recur. Do not continue to the next step until you feel certain that none of the alarms will recur.



When you make changes to the Management Services Account, services that run under that account must be restarted. An alarm is raised for each service that requires a restart. It is important to carefully review the alarms and ensure all of these services are restarted.

The particular services that must be restarted in your environment depend on the server roles that are active in your environment.

Change the MSA or DMSA Account to a Different Windows Account

Follow the procedure in this section if you want to change the Windows account that is used as the MSA or DMSA account.

Related topics

[Important Account Details \(page 190\)](#)

[Use Multiple MSAs \(page 190\)](#)

[DMSA/MSA Account Change Workflow \(page 191\)](#)

[Change the DMSA/MSA Accounts \(step-by-step\) \(page 192\)](#)

Important Account Details

Before changing the MSA or the DMSA to a different account, note the following:

- Any Windows user account specified as the MSA or the DMSA must be dedicated to this purpose.
- All servers in the same data center must run using a single dedicated MSA.

Related information

Additional information about the Management accounts, including the rights required (*Technologies, Security, and Network Integration Deployment Guide*)

Use Multiple MSAs

In many deployments, the MSA is specified at the Enterprise node and is the same for every server in the Enterprise.

If necessary, you can specify a different MSA for a particular Site group, Site, or Server node in the Enterprise Manager Installations tree. Some example scenarios where you might specify a different account for a Site Group, Site, or Server include:

- You have a Site that uses a different Windows naming convention. For example, you have a data center site in the U.K. and a remote site in India, and the India site uses a different Windows naming convention. In this case, you can specify a different Management Service Account for the remote India site than is specified for the U.K. data center site.
- Two different sites exist and the MSA is sometimes locked at one of the sites. In this case, using different accounts at each site allows each site to operate independently if it is necessary for one site to lock the account.
- No domain exists and the Servers at a site are deployed in a Windows workgroup.

In this scenario, the MSA is a local Windows account on each computer. The MSA is specified in the Computername\Username format (for example, ComputerName1\JDoe, ComputerName2\JDoe and so on). Since the computer name is different for each server, the MSA username must be specified separately for each server in the workgroup.

As noted above, all servers in the same data center must run using a single dedicated MSA. Therefore, in a workgroup environment, the data center server must either be a single server of the Data Center platform, or a Consolidated server.

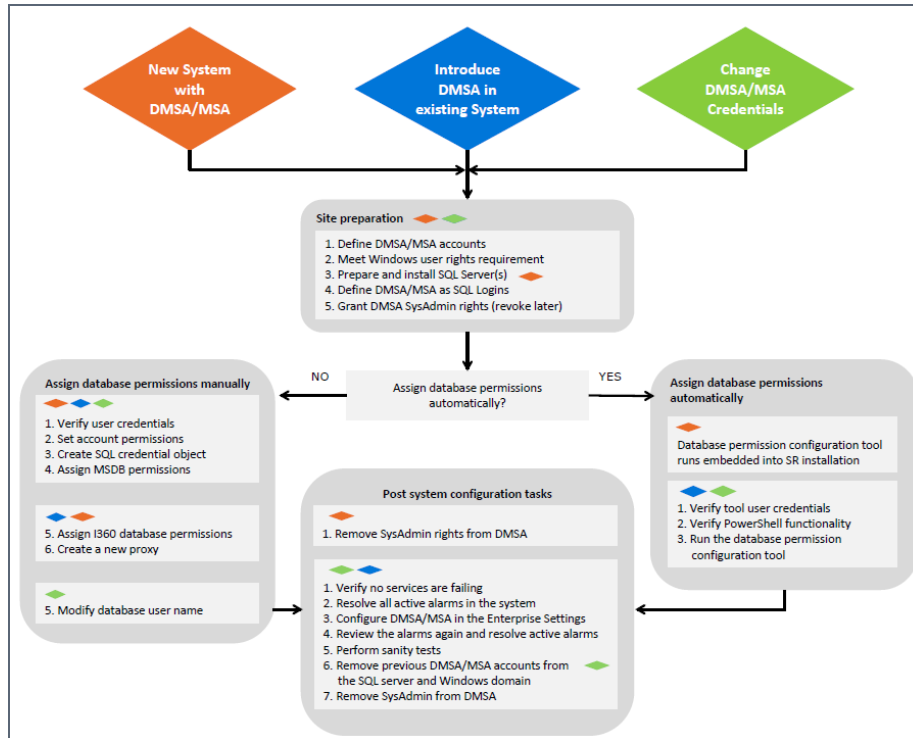
Site Permissions When Multiple Accounts Are Used

If you have two remote Sites (or Site Groups) that have different MSAs, no special configurations are needed at either Site regarding the permissions of the accounts. For example if you have remote Site 1 using account 1 and remote Site 2 using account 2, you do not need to perform any special configurations for account 2 at Site 1, or vice versa. The servers at different Sites do not use Windows authentication when communicating with each other (they use token-based authentication).

DMSA/MSA Account Change Workflow

You can change the DMSA and MSA accounts in the following scenarios:

- Define new DMSA/MSA accounts during initial system installation or upgrade.
- Introduce DMSA into an existing system. If the system is already functioning using only the MSA account, and you want to add the DMSA account.
- Change DMSA/MSA in an existing system. If the system is already functioning and you want to change the DMSA/MSA accounts.



Related information

DMSA and MSA Permissions *SQL Server Installation and Upgrade Guide*

Related topics

[Change the DMSA/MSA Accounts \(step-by-step\) \(page 192\)](#)

Change the DMSA/MSA Accounts (step-by-step)

Eventually, you might need to change the DMSA or MSA accounts or account passwords. Generally, you change these accounts for either of these reasons:

- The security policies of an enterprise require the passwords, or the usernames and passwords, of important accounts to be changed periodically.
- Changes to the Windows network require servers to be moved to a new Windows domain.

Because important services run under the DMSA and MSA accounts, you must follow specific procedures to change these accounts or their passwords.

Follow these steps to change the usernames and passwords of the DMSA and MSA accounts:

Procedure

1. Provide the existing DMSA/MSA accounts with SQL SysAdmin Rights

Step 1 of 13 associated with changing the DMSA or MSA, or both.

In this step, you ensure the existing DMSA and MSA accounts have SysAdmin rights on the computer running SQL Server.

 The *existing DMSA/MSA accounts* are the accounts you are about to change to new accounts.

If these accounts do not currently have SysAdmin rights on the computer running SQL Server, provide them with these rights now.

See the *Technologies, Security, and Network Integration Deployment Guide* for details about the SQL server rights required for the MSA and DMSA accounts.

2. Define the new DMSA/MSA account(s) in the domain

Step 2 of 13 associated with changing the DMSA or MSA, or both.

In this step, you must create new Windows accounts and provide these accounts with the necessary Windows access rights:

- If you are changing the MSA account, create a new Windows account in the domain to serve as the MSA.
- If you are changing the DMSA account, create a new Windows account in the domain to serve as the DMSA.
- Assign the appropriate Windows access rights to the new account(s) you have created.

See the *Technologies, Security, and Network Integration Deployment Guide* for details about the Windows access rights required by the MSA and DMSA accounts.

 For detailed information about altering or creating Windows user accounts, see the Microsoft MSDN site or consult with your Microsoft network administrator.

3. Define the new accounts as SQL Logins with SysAdmin Rights

Step 3 of 13 associated with changing the DMSA or MSA, or both.

In this step, you ensure the new accounts can log in to the computer running SQL Server as SysAdmins.

- If you created a new Windows account to serve as the MSA in the previous step, define that account as an SQL Login with SysAdmin Rights.
- If you created a new Windows account to serve as the DMSA in the previous step, define that account as an SQL Login with SysAdmin Rights.

See the *Technologies, Security, and Network Integration Deployment Guide* for details about the SQL Server rights required by the MSA and DMSA accounts.

4. Assign Database Permissions

Step 4 of 13 associated with changing the DMSA or MSA, or both.

In this step, you assign database permissions to the account(s) you have created.

Assign the database permissions automatically or manually.

4. a) Assign DB permissions automatically

You can use the *Database Permissions Configuration Tool* to automatically assign the required database permissions to the DMSA or MSA accounts, or both.

This procedure is summarized below. For detailed information about each step of the procedure, see the *SQL Server Installation and Upgrade Guide*.

Procedure

1. Access the Database Permission Configuration Tool.
2. Verify tool user credentials.
3. Verify Windows Powershell functionality.
4. Run the Database Permissions Configuration Tool.

4. b) Assign DB permissions manually

If you do not want to automatically assign the database permissions to the DMSA or MSA accounts (or both), you can manually assign them.

Manually assigning database permissions requires that SQL permissions are set for DMSA or MSA for each instance of a computer running SQL Server.

This procedure is summarized below. For detailed information about each step of the procedure, see the *SQL Server Installation and Upgrade Guide*.

Procedure

1. Verify user credentials.
2. Set account permissions.
3. Modify SQL credential object.

4. Assign MSDB permissions.
5. Modify database user name.

5. Change the SSRS Service User

Step 5 of 13 associated with changing the DMSA or MSA, or both.



Perform this procedure only if you are changing the *MSA*. If you are changing only the *DMSA*, skip this procedure and continue to [6. Verify that no services are failing \(page 195\)](#).

In this step, you do the following:

- Specify the new MSA account as the account that runs the report server service and the account used to connect to the Reporting Services database.
- Backup the SSRS encryption keys (you will restore these keys in a subsequent step in this procedure).

Perform this procedure from the server that hosts the Reporting Services server role.

Procedure

1. Launch the **Reporting Services Configuration Manager**.
(Usually located at **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools**.)
2. In the **Reporting Services Configuration Connection** window:
 - a. Ensure that the **Server Name** and **Report Server Instance** fields specify the values appropriate for the computer running SQL Server that hosts the Reporting Services database.
 - b. Click **Connect**.
3. In the left-pane, select **Service Account**.
4. Select **Use another account**.
 - In the **Account (Domain\user)** field, enter the domain\username of the MSA account.
 - In the **Password** field, enter the password of the MSA account.
5. Click **Apply**.
6. In the **Backup Encryption Key** window, complete these fields:
 - **File Location** - Specify the file name and location of the file that will contain the backup encryption key.
 - **Password/Confirm Password** - Type a password to protect the file from unauthorized access. The password must be at least 8 characters, include a combination of uppercase and lowercase alphanumeric characters, and at least one symbol character.



You will use this backup key file to restore the encryption key in a subsequent step of this procedure. You *must* know both the file *location* and the *password* entered here to restore the encryption key.

7. In the **SQL Server Connection Dialog**, you must specify the credentials of an account that has permission to access the Reporting Services database. The MSA account has this permission. Complete the fields as noted below:
 - **Server Name:** - Specify the name of the computer running SQL Server that hosts the Reporting Services database.
 - **Credentials Type** - Select one of the following from the drop-down box.
 - **Current User - Integrated Security** - Select this option if you are currently logged into Windows using an administrator account that has the permission to access the Reporting Services database. If you select this option, you do not need to enter a user name and password.
 - **SQL Server Account** - Select this option to specify the credentials of an account that has permission to access the Reporting Services database. If you select this option, enter the username and password for this account in the fields provided.
8. Click **OK**.

6. Verify that no services are failing

Step 6 of 13 associated with changing the DMSA or MSA, or both.

In this step, you verify that the Watchdog application is not repeatedly starting failing services on any of the servers in the enterprise.

Procedure

You must perform this procedure on every server in the enterprise.

1. From the Windows desktop on a managed server, use the System Tools to turn off the Watchdog application.
2. Verify that none of the services monitored by the Watchdog application are failing. If any services are failing, you must correct the problem causing the services to fail.
3. When you are sure that none of the services monitored by the Watchdog application are failing, use the System Tools to restart the Watchdog application.
4. Repeat steps 1 through 3 on every server in the enterprise.

7. Resolve all active alarms in the system

Step 7 of 13 associated with changing the DMSA or MSA, or both.

In this step, you use the Alarm Dashboard to resolve all active alarms in the system.



Changing the MSA account can cause a server to falsely trigger two alarms if the server hosts both the Import Manager application and any one or more of these server roles:

- IP Recorder
- IP Recorder Video
- TDM Recorder

- Screen Recorder
- Recorder Ingestion Web Service
- Analytics Framework

The two alarms that are falsely triggered on such a server are:

- Disk Manager Deleted Unarchived Files (alarm number 39003)
- Disk Manager Detected Unarchived Files (alarm number 39004)

The server may continue to trigger these alarms for some time (possibly months) after you change the MSA account. If you see either of these alarms raised by such a server in the Alarm Dashboard, you can acknowledge the alarm without performing the alarm corrective action. These alarms false; the conditions that normally cause these alarms do not exist.

Procedure

1. Click **System Monitoring > System Monitor > Alarm Dashboard**.
2. Resolve every active alarm that appears in the **Enterprise Alarms** pane.
 - a. Click on an alarm in the **Enterprise Alarm** pane.
 - b. In the **Details** pane, review the **Corrective Action:** for the alarm.
 - c. Perform the corrective action steps for the alarm.
 - d. Click on an alarm again in the **Enterprise Alarm** pane.
 - e. Click on **Servers** to display the Servers pane.
 - f. In the Servers pane, click the **Acknowledge** icon  to acknowledge the alarm.
 - g. Repeat steps a. through f. for every alarm in the **Enterprise Alarms** pane.
3. Allow the system to stabilize by ensuring that none of the alarms recur. Do not continue to the next step until you feel certain that none of the alarms will recur.

8. Configure DMSA/MSA in the Enterprise Settings

Step 8 of 13 associated with changing the DMSA or MSA, or both.

In this step, you change the Database Management Account or Management Service Account credentials on the Enterprise Settings screen.

Procedure

1. Select **System Management > Management > Enterprise Settings**.
2. In the Installations tree (left-hand pane), select the **Enterprise** node.

3. Perform the appropriate procedure(s) below:

- If you are changing to a new MSA account, change these two settings in the **Management Service Account** section:
 - **Username** - Enter the username associated with the Windows account you created to serve as the MSA.
 - **Password** - Enter the password associated with the Windows account you created to server as the MSA.
- If you are changing to a new DMSA account, change these two settings in the **Database Management Account** section:
 - **Username** - Enter the username associated with the Windows account you created to serve as the MSA.
 - **Password** - Enter the password associated with the Windows account you created to server as the MSA.

3. Click **Save and Apply to Children**.

9. Review the alarms again and resolve active alarms

Step 9 of 13 associated with changing the DMSA or MSA, or both.

In this step, you must review the active alarms again and restart any services that are indicated in any new active alarms. To do this, repeat [7. Resolve all active alarms in the system \(page 195\)](#) to resolve any active alarms.



When you change the Management Services Account, services that run under that account must be restarted. An alarm is raised for each service that requires a restart. It is important to carefully review the alarms and ensure all of these services are restarted.

The particular services that must be restarted in your environment depend on the server roles that are active in your environment.

10. Perform Sanity Tests

Step 10 of 13 associated with changing the DMSA or MSA, or both.

In this step, you perform steps to assure the system is operating properly following the credential change to the Management Service Account or database management account, or both.

Procedure

1. Verify that you can record and playback a new interaction in Quality Monitoring.
2. Verify that you can perform an evaluation on the new interaction.
3. Ensure that the alarm statuses are green and that all jobs have succeeded in the agent job monitor on the computer running SQL Server.
4. Verify that you can generate a QM report that includes the new interaction.

11. Remove previous management accounts (optional)

Step 11 of 13 associated with changing the DMSA or MSA, or both.

In this step, you have the option to remove the old accounts you are no longer using.

The new DMSA and MSA accounts are now fully set up and the system is operating. Optionally, you can remove the previous accounts from the computer running SQL Server and from the Windows Domain.

12. Remove SysAdmin rights (optional)

Step 12 of 13 associated with changing the DMSA or MSA, or both.

In this step, you have the option to remove SQL SysAdmin from the new DMSA or MSA accounts you are now using.

Earlier in this procedure, you provided the DMSA or MSA account with SQL SysAdmin privileges.

The SQL SysAdmin privileges are only required by these accounts during the first time server installation, and when you are changing the DMSA/MSA accounts to new accounts.

Following the first successful Enterprise Manager distribution, you can remove the SQL SysAdmin permission from the DMSA or MSA user account.

During future service pack and hotfix installations, SysAdmin privileges will need to be re-instated. This is also the case whenever changing the MSA or DMSA accounts.

13. Restore the SSRS Encryption Keys

Step 13 of 13 associated with changing the DMSA or MSA, or both.

In this step, you restore the SSRS encryption keys that you backed up when you performed Step 5. *Change the SSRS Service User.*

For details the procedure to restore the encryption keys, see the *Workforce Optimization Maintenance Guide*.



Changing the MSA account can cause a server to falsely trigger two alarms if the server hosts both the Import Manager application and any one or more of these server roles:

- IP Recorder
- TDM Recorder
- Screen Recorder
- Recorder Ingestion Web Service
- Analytics Framework

The two alarms that are falsely triggered on such a server are:

- Disk Manager Deleted Unarchived Files (alarm number 39003)
- Disk Manager Detected Unarchived Files (alarm number 39004)

The server may continue to trigger these alarms for some time (possibly months) after you change the MSA account. If you see either of these alarms raised by such a server in the Alarm Dashboard, you can acknowledge the alarm without performing the alarm corrective action. These alarms are false; the conditions that normally cause these alarms do not exist.

Details:

The server triggers these alarms if there are recordings in the call buffer that are already archived at the time the MSA account is changed.

The server begins to trigger the “Disk Manager Deleted Unarchived Files” (39003) alarm when the call buffer becomes full and old recordings must be deleted to make space for new recordings. The server triggers this alarm each time a recording that is already archived is deleted from the buffer. The server continues to trigger this alarm until all recordings that were in the call buffer and already archived at the time the MSA account was changed are deleted from the call buffer.

The server triggers the “Disk Manager Detected Unarchived Files” (alarm number 39004) once every 3 to 5 days until all recordings that were in the call buffer and already archived at the time the MSA account is changed are deleted from the call buffer.

Change the SQL Services account

The SQL Server database engine and the SQL Server agent services are run by a domain account defined by the customer during site preparation. This user is referred to as the SQL Services account. If you are using the MSA or DMSA account to run the SQL Server services, refer to those procedures for changing the account.

Procedure

1. Prepare a new account in the domain, according to DRG requirements.
2. Configure the **SQL Server service** and **SQL agent service** to run under this account.

Related information

SQL Server Installation and Upgrade Guide

Change the SQL Services account password

It is possible to change the password of the existing account used to run the SQL database engine and SQL agent services.

Procedure

1. Change the account password in the domain.
2. Right-click **My Computer** and select **Manage**.
3. In the Computer Management console, expand Services and Applications > SQL Server Configuration Manager and select **SQL Server services**.
4. In the list of SQL Server services, right-click the **SQL Server** and **SQL Server Agent (MSSQLSERVER)** services in turn, and select **Properties**.
5. In the **Log On** tab, type the new **Password** defined for the account in the domain.

Change the Enterprise Manager Agent application user accounts

You can manage user accounts individually for the Enterprise Manager Agent (EMA) application.



Every server managed by the Enterprise Manager application hosts either the RM or the EMA application. Recorder servers host the RM application. All other servers host the EMA application.

The EMA application has a default admin user account. You can change the password of the default admin user account. You can also create new user accounts, and edit existing accounts for the EMA application.

Default admin user account

The default admin user account the EMA application has these privileges:

- View and edit privileges to every screen in the application
- **User Administrator** privileges (specifically, the ability to create new user accounts and edit or delete existing ones)

The default admin user account is hard-coded in the EMA application. You cannot:

- Delete this account
- Change the username of this account
- Revoke **User Administrator** privileges from this account

You can change the password of the default admin user account if you are logged in to an EMA application under any account that has User Administrator privileges (including the default admin user account itself).

Create and edit accounts

If you are logged into an EMA application under an account that has User Administrator privileges, you can do the following:

- Create new user accounts
- Delete any account except the default admin user account
- Grant or revoke **User Administrator** privileges to or from any account except the default admin user account
- Change the user name of any account except the default admin user account
- Change the password of any account, including the admin user account

Every user account in the RM or EMA application has view and edit privileges to every screen in the application. Only the User Administrator privilege is optional for each user account.

Related topics[Create, edit, or delete an EMA user account \(page 202\)](#)[RM and EMA User Management create/edit account screen reference \(page 203\)](#)

Create, edit, or delete an EMA user account

In the EMA application, you can create, edit, or delete user accounts. To manage user accounts, you must access these applications directly with a web browser.

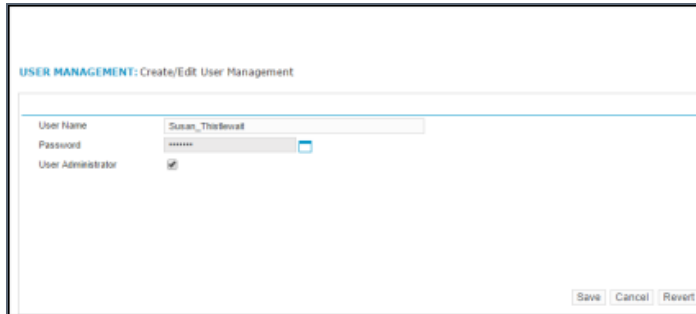
Procedure

1. Open a web browser.
2. In the web browser, use the appropriate URL to access the EMA application:
 - - `http://servername/RM`
 - **EMA** - `http://servername/EMA`
servername is the IP address or host name of the server hosting the application).
3. At the **SIGN IN** screen, enter the user name and password of a user account that has User Administrator privileges in the application (such as the default admin user account). Select **GO**.
4. Go to **System Management** and select **Manage User**.
5. Do one of the following:
 - Create a new account:
 - Select **Create**.
 - Enter a **User Name** and **Password** for the account.
 - To provide the user account with the ability to create, edit, or delete user accounts, select **User Administrator**.
 - Select **Save**.
 - Edit an existing account:
 - Select the account to edit.
 - Select **Edit**.
 - Make changes to the **User Name** or **Password**, or grant or revoke **User Administrator** privileges to or from the account. (You can edit only the **Password** field of the default admin user account.)
 - Select **Save**.
 - Delete an existing account:
 - Select the account to delete.
 - Select **Delete**.

Related topics[RM and EMA User Management create/edit account screen reference \(page 203\)](#)[Change the Enterprise Manager Agent application user accounts \(page 201\)](#)

RM and EMA User Management create/edit account screen reference

If you are signed in with a user account that has the User Management privilege (such as the default admin user account), you can complete or edit the fields of the User Management screen.



The table below describes the User Management screen settings:

Item	Description
User Name	The user name for the user account. You cannot change the user name of the default admin user account.
Password	Creates or changes a password. Select the Password icon  to create or change a password,
User Administrator	Provides the account with the ability to create, edit, and delete user accounts. You cannot revoke this privilege from the default admin user account.

Related topics

[Create, edit, or delete an EMA user account \(page 202\)](#)

[Change the Enterprise Manager Agent application user accounts \(page 201\)](#)

Change the Import Manager application user accounts

You can manage user accounts individually for the Import Manager (IM) application.

The IM application is available on any server on which the Import Manager server role is activated.

The IM application has a default admin user account. You can change the user name and password of this account. You can also create new user accounts.

All IM user accounts have full access to all features of the IM application.

Procedure

1. In a web browser, access the IM application:
`http://servername/ExtractionUI`
servername is the IP address or host name of the server hosting the application.
2. At the **SIGN IN** screen, enter the user name and password of an existing user account, such as the default admin user account. Select **GO**.
3. Go to **System**. Under **Security**, select **User Management**.
4. Do one of the following:
 - Create a new account:
 - Select **Create**.
 - Enter a **User Name** and **Password** for the account.
 - Select **Save**.
 - Edit an existing account:
 - Select the account to edit.
 - Select **Edit**.
 - Make changes to the **User Name** or **Password**.
 - Select **Save**.
 - Delete an existing account:
 - Select the account to delete.
 - Select **Delete**.

Related topics

[Change the Enterprise Manager Agent application user accounts \(page 201\)](#)

Change the System Account (DB Realm)

The system automatically installs a default user to manage all administrative tasks. This user is referred to as the System Account.

Change the user name or password of the System Account as needed.

Procedure

1. On the Application server, open a web browser.
2. Enter:
`http://localhost:7001/bbmWebApp/SecurityUtil`
3. When prompted, enter the current WebLogic administrator credentials, and select **OK**.
4. Modify the user name and password for the system account as needed.
If SAML is configured for the System Account user, an Enable-db-authentication check box is also available. To turn on database authentication as an alternative authentication mechanism for the System Account user, select the check box.
5. Select **Change**.

Change the System Account (Windows Authentication)

In a Windows domain authentication environment, the customer prepares a dedicated domain user to manage all administrative tasks. This user is referred to as the System Account.

You can change the user name or password of the System Account in the domain.

- When you change the user name, follow this procedure to ensure that the enterprise suite logon and administration features function correctly.

Running the Active Directory Validation tool saves an XML file that contains the new account settings. The WebLogic configuration tool uses the data in the XML file to configure the WebLogic server settings.

- When you change the password only, nothing else is required.

Procedure

1. Prepare a new domain account, according to DRG requirements.
2. Run the Active Directory Validation tool.
3. Run the WebLogic Configuration Tool.

Related information

Technology, Security and Network Integration Deployment Reference Guide

Configure WebLogic settings (*Authentication Configuration Guide*)

Change the WebLogic Administrator Account Password (DB Realm)

In a DB Realm environment, the customer prepares a dedicated user to manage the system-based user application authentication. This user is referred to as the DBRealm WebLogic Admin Account. To change the password of the WebLogic Admin Account in a DBRealm environment, you complete three tasks.



Changing only the user name of the DBRealm WebLogic Admin Account is not supported.

Change the Password in the WebLogic Administration Console

1. On the Application Server, access the WebLogic administration console using the following URL:
`http://localhost:7001/console`
2. Sign in to the console using the existing WebLogic admin account credentials.
3. In the left pane, under **Domain Structure**, select **Security Realms**.
4. In the **Realms** table, select **BPDBRealm**.
5. Select the **Users and Groups** tab.
6. In the **Users** table, select the existing WebLogic admin user account.
7. Click the **Passwords** tab.
8. Enter the new password in the **New Password** and **Confirm New Password** fields and click **Save**.
9. Close the WebLogic Server Administration Console.

Change the Password in the Framework Applications Server Role Settings

1. Sign in to the WFO Portal.
2. Browse to **System Management > Enterprise > Settings**.
3. Expand the Application server select the **Framework Application** server role.
4. Modify the **Administrator Password**.

Edit the `boot.properties` File and restart the `WFO_ProductionDomain_ProductionServer` service

1. Use a text editor to open the **boot.properties** file on the application server at the location below:
`%VERINT_WEBLOGIC_DOMAIN_HOME%servers\ProductionServer\security`
2. For the **password=** parameter, type the new password (to replace the existing password value).
3. Save the **boot.properties** file and close the text editor.
4. Restart the **WFO_ProductionDomain_ProductionServer** Windows service on the server on which you have edited the `boot.properties` file. (Go to **Start > Administrative Tools > Services** and restart the service.)

Related topics

[Change the System Account \(DB Realm\) \(page 205\)](#)

Workflow: Change the WebLogic 12.x Administrator Account (Windows Authentication)

In a windows domain authentication environment, the customer prepares a dedicated domain user to manage the WebLogic service for domain user application authentication. This user is referred to as the domain WebLogic Admin Account.



Follow this workflow only when using WebLogic 12.x. When using WebLogic 14.x, then follow the workflow for that version.

To change the user name or password for this account, use the following series of tasks:

1. [Back up the WebLogic 12.x Files Needed to Restore the Existing Account or Password \(page 208\)](#)
Before you change the Weblogic Admin Account user name or password, you must back up some files on the application server. If you cannot complete the account or password change procedure successfully, you need these files to restore the system to the existing account user name or password.
2. [Change the WebLogic 12.x Administrator Account to a Different User Account \(Windows Authentication\) \(page 209\)](#)
Perform this procedure to change the Weblogic Admin Account user name.
3. [Change the WebLogic 12.x Admin Account Password \(Windows Authentication\) \(page 216\)](#)
Perform this manual procedure to change only the WebLogic Admin Account password.
4. [Restore the Existing WebLogic 12.x Admin Account User Name or Password \(page 220\)](#)
If you cannot complete the WebLogic Admin Account user name or password change procedure successfully, you can restore (or rollback) the system to the existing WebLogic Admin Account user name or password.

Related topics

[Workflow: Change the WebLogic 14.x Administrator Account \(Windows Authentication\) \(page 221\)](#)

Back up the WebLogic 12.x Files Needed to Restore the Existing Account or Password

Before you change the Weblogic Admin Account user name or password, you must back up some files on the application server. If you cannot complete the account or password change procedure successfully, you need these files to restore the system to the existing account user name or password.

Back up these files and store them in a convenient location.

- %VERINT_WEBLOGIC_DOMAIN_HOME%\config\config.xml
- %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\security\boot.properties
- %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\data\ldap

What to do next

[Change the WebLogic 12.x Administrator Account to a Different User Account \(Windows Authentication\) \(page 209\)](#)

Change the WebLogic 12.x Administrator Account to a Different User Account (Windows Authentication)

Perform this procedure to change the Weblogic Admin Account user name.

Before you begin

[Back up the WebLogic 12.x Files Needed to Restore the Existing Account or Password \(page 208\)](#)

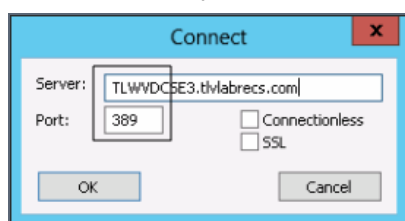
Procedure

1. Do one of the following:
 - Prepare a new account in the domain, according to requirements specified in the *Technologies, Security and Network Integration Deployment Reference Guide*.
 - Identify an existing account in the domain that meets the DRG requirements.



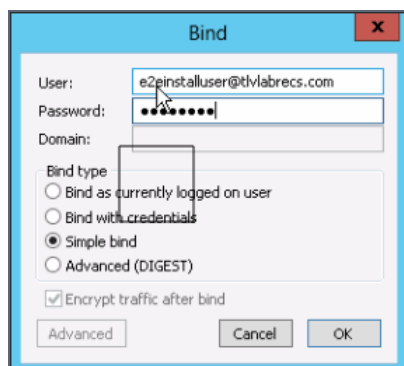
If you have an application server cluster, you must repeat steps 2 through 26 on each application server in the cluster.

2. Verify the new account created or identified in the previous step is working correctly. To verify, open the **ldp.exe** tool, connect to the domain controller, and do a simple bind using the account, as described in the steps that follow.
 - a. From the command prompt, start the **ldp.exe** tool.
 - b. Select **Connections > Connect**, complete these fields, and click **OK**:
 - **Server:** Enter the server name (FQDN) of the domain controller.
 - **Port:** Enter the port (default 389) to connect to the domain controller.



- c. Select **Connection > Bind**, complete these fields, and click **OK**:

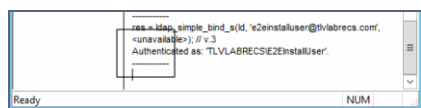
- **User:** Enter the user name of the new account in the User Principal Name (UPN) format.
- **Password:** Enter the password for the new account.
- **Bind Type:** Select the **Simple bind** option.



- d. Verify that the bind was successful.

A successful bind shows a result such as:

```
res=ldap_simple_bind_s(id, 'e2installuser@tlvlabrecs.com',
<unavailable>); // v.3
Authenticated as 'TLVLABRECS\E2EInstallUser'.
```

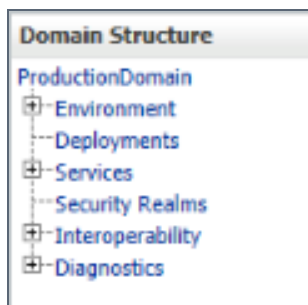


- e. Use the **ldp.exe** tool to search for any application user in the Active Directory.
3. On the Application Server, access the WebLogic administration console using the following URL:
<http://localhost:7001/console>
 4. Sign in to the console using the existing WebLogic Admin Account credentials.

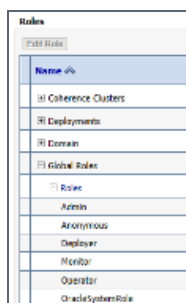
i The user name and password you use to sign in to the WebLogic Server Administration Console are the same account name and password that are specified on the **Framework Applications** server role **Settings** page.

To view this user name and password, select **System Administration > Enterprise > Settings** and select the **Framework Applications** server role in the Installations pane. The account name and password appear under the **Server Access** settings.

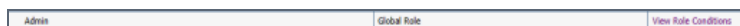
5. Under **Domain Structure** (left pane), select **Security Realms**.



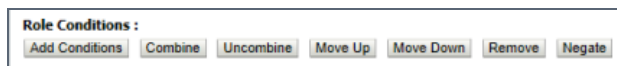
6. In the **Realms** table, click **BPDBRealm**.
7. Click the **Roles and Policies** tab.
8. In the **Roles** table, expand **Global Roles**, then expand **Roles**.



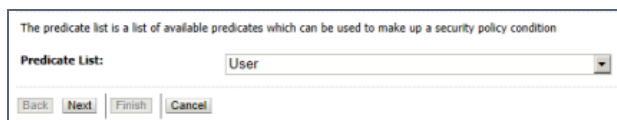
9. For the **Admin** role, under the **Role Policy** column, select **View Role Conditions**.



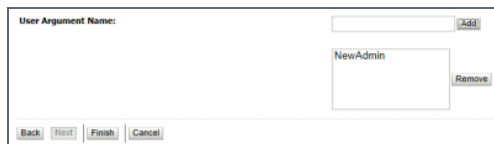
10. From **Role Conditions**, click **Add Conditions**.



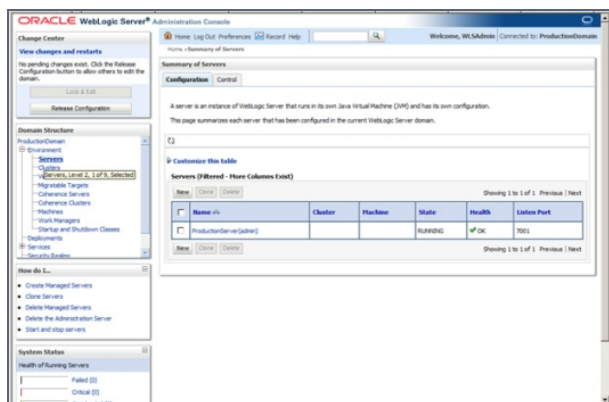
11. In the **Predicate List** drop-down, select **User**.



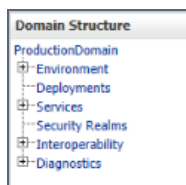
12. From the **Predicate List** buttons, click **Next**.
13. In the **User Argument Name** text box, type the case-sensitive user name associated with the domain account you created or identified in step 1. Then click **Add**.



14. Click **Finish**.
15. In the **Edit Global Rule** screen, confirm the **User:** field specifies the new user name and that the **Or** operator is selected beneath the new user name. Then click **Save**.

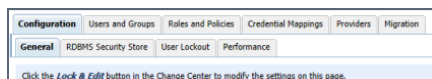


16. Under **Domain Structure** (left pane), select **Security Realms**.



17. In the **Realms** table, click **BPDBRealm**.

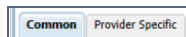
18. Click the **Providers** tab.



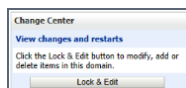
19. In the **Authentication Providers** table, click the name of the Active Directory provider. (The **Description** column for this provider states, **Provider that performs LDAP authentication**.)



20. Click the **Provider Specific** tab.



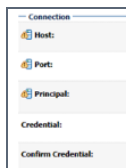
21. Under **Change Center** (left pane), click **Lock & Edit**.



22. In the **Connection** area, complete these fields:

- **Principal** text box - Type the new user account in the UPN format (for example, **user@domain.com**).

- **Credential** text box - Type the password for the account.
- **Confirm** Credential text box - Retype the password for the account.



The screenshot shows a 'Connection' dialog box with the following fields: Host, Port, Principal, Credential, and Confirm Credential. Each field has a small icon to its left.

23. Click **Save**.



If the changes are not saved, change the Provider-Specific items one at a time. For example, change **Principal** and click **Save**, change **Credential** and click **Save**, then change **Confirm Credential** and click **Save**.

24. Under **Change Center** (left pane), click **Activate Changes**.

When the changes are activated, the following message displays in the right pane: **All changes have been activated. However 1 items must be restarted for the changes to take effect.**

25. Use a text editor to update the **boot.properties** file on the application server.

- Use Notepad or a similar text editor to open the **boot.properties** file on the application server from the following location:
`%VERINT_WEBLOGIC_DOMAIN_HOME%servers\ProductionServer\security\boot.properties`
- For the **username=** parameter, type the new username (to replace the existing username value).
- For the **password=** parameter, type the new password (to replace the existing password value).
- Save the **boot.properties** file and close the text editor.



The clear text username and password are encrypted after you restart the **WFO_ProductionDomain_ProductionServer** service in the next step

- Restart the **WFO_ProductionDomain_ProductionServer** Windows service from the Services window on the server on which you have edited the **boot.properties** file.
 - If the **WFO_ProductionDomain_ProductionServer** service fails to start, or stops unexpectedly, verify the username and password are both entered correctly in the **boot.properties** file and restart the service again.
 - If the service still fails to start, check for errors in the **ProductionServer.log** at this location:
`%AVAYAAURADATADIR%\Logs\ProductionServer\weblogic\ProductionServer.log`
26. Open a web browser and browse directly to the application server where you have made changes. To verify that you can successfully sign in using LDAP, sign in with the username and password of an active user.



If you have an application server cluster, repeat all of the steps from the beginning of this procedure to this step on each application server in the cluster before continuing to the next step.

27. From the enterprise portal, select **System Management > Enterprise > Settings**.
28. Under **Installations** (left pane), open the **Framework Applications** server role.
29. In the Framework Applications server role settings, update these two fields:
 - **Administrator Account Name** - Enter the username for the new WebLogic Admin Account here.
 - **Administrator Account Password** - Enter the password for the new WebLogic Admin Account here. (Click the icon to the right of the text box to set and confirm the password.)
30. Wait for the Pending Messages icon to disappear from the top of the screen before continuing to the next step.
31. Verify that the CMA distribution is completed successfully for the application servers.
 - a. Open the Enterprise Manager Agent (EMA) application on the application server. To access the EMA, enter this URL in the web browser: **http://hostname/EMA**, where **hostname** is the host name of the application server.
 - b. Select **Status > System Monitor**.
 - c. In the **Status Messages** area, look for a message stating: **CMA Distribution: complete successfully on date_and_time**

Status Messages		
Component Name	Status	Message Details
CMA Distribution		CMA Distribution: Completed successfully on 8/12/2015 11:10:23 PM

32. Check the Alarm Dashboard for an alarm indicating that it is necessary to restart the WFO service.
 - a. From the enterprise portal, select **System Monitoring > System Monitor > Alarm Dashboard**.
 - b. In the Alarm Dashboard, look for an alarm named **Service restart required** that is active on an application server for which you have changed the WebLogic Admin Account.
If you have multiple application servers, you see one alarm for each application server.
The alarm indicates that a restart of the **WFO_ProductionDomain_ProductionServer** service is required. (The alarm **Details** pane for an alarm indicates the specific service that must be restarted.)
 - c. When you see this alarm for an application server, restart the **WFO_ProductionDomain_ProductionServer** service on that application server and then acknowledge the alarm.
If the Framework Applications plug-in fails, check the pluginerror.log file. This log file is found in **<install_directory>\Software\UCMServices\Plugins\Databases\FrameworkApplications**.
To complete the account change process, correct the error.

What to do next

[Change the WebLogic 12.x Admin Account Password \(Windows Authentication\) \(page 216\)](#)

Related information

Troubleshoot SSO (*Authentication Configuration Guide*)

Technologies, Security and Network Integration Deployment Reference Guide

Change the WebLogic 12.x Admin Account Password (Windows Authentication)

Perform this manual procedure to change only the WebLogic Admin Account password.



Perform this procedure before changing the WebLogic Admin Account password in the Windows domain.

Before you begin

[Back up the WebLogic 12.x Files Needed to Restore the Existing Account or Password \(page 208\)](#)

Procedure

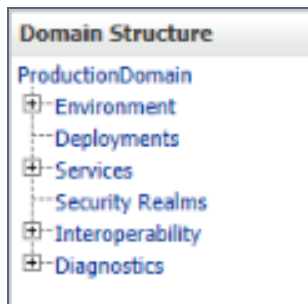
1. On the Application Server, access the WebLogic administration console using the following URL:
`http://localhost:7001/console`
2. Sign in to the console using the existing WebLogic Admin Account credentials.



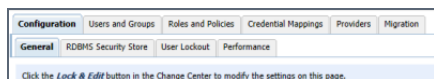
The user name and password you use to log into the WebLogic Server Administration Console are the same account name and password that are specified on the **Framework Applications** server role **Settings** page.

To view this user name and password, select **System Administration > Enterprise > Settings** and select the **Framework Applications** server role in the Installations pane. The account name and password appear under the **Server Access** settings.

3. Under **Domain Structure** (left pane), select **Security Realms**.



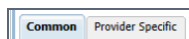
4. In the **Realms** table, click **BPDBRealm**.
5. Click the **Providers** tab.



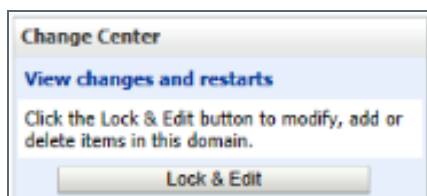
6. In the **Authentication Providers** table, click the name of the Active Directory provider. The **Description** column for this provider states, **Provider that performs LDAP authentication.**



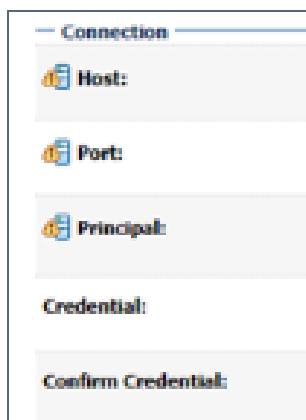
7. Click the **Provider Specific** tab.



8. Under **Change Center** (left pane), click **Lock & Edit**.



9. In the **Connection** area, complete the following fields:
- **Credential** text box - Type the new password for the account.
 - **Confirm Credential** text box - Type the new password for the account again.



10. Click **Save**.

When the update is successful, the message "Settings updated successfully" appears under the **Messages** setting in the right pane.



If you have an application server cluster, repeat all steps of this procedure from the beginning of this procedure to this step on each application server in the cluster before continuing to the next step.

11. Under **Change Center** (left pane), click **Activate Changes**.

When the activation is successful, the message "All changes have been activated. No restarts are necessary." appears under the **Messages** heading in the right pane.



At this point, it is possible for the WebLogic admin user to be locked out of the WFO application. If this occurs, just continue with this procedure. This problem is resolved in the next step.

12. An Active Directory administrator must perform this procedure in Active Directory. Reset the WebLogic admin user password to the new value in **Active Directory > Users & Computers**.
 - a. Right click the user object and click **Reset Password**.
 - b. In the **New password** field, enter the new password.
 - c. In the **Confirm password** field, enter the new password again.
 - d. Make sure the **Unlock the user's account** check box is selected.
 - e. Click **OK**.
 13. Access the enterprise portal with a web browser, and verify that you can sign in using any Windows domain account that was previously used to access the portal.

If you cannot sign in, a mistake has occurred somewhere in this procedure. To reset the password, repeat this procedure from step 1.
 14. Use a text editor to update the **boot.properties** file on the application server.
 - a. Use Notepad or a similar text editor to open the **boot.properties** file on the application server from the following location:
%VERINT_WEBLOGIC_DOMAIN_HOME%servers\ProductionServer\security
 - b. For the **password=** parameter, type the new password (to replace the existing password value).
 - c. Save the **boot.properties** file and close the text editor.
-
- The clear text password is encrypted after you restart the **WFO_ProductionDomain_ProductionServer** service in the next step.
- d. Restart the **WFO_ProductionDomain_ProductionServer** Windows service from the Services window on the server on which you have edited the **boot.properties** file.
-
- If the **WFO_ProductionDomain_ProductionServer** service fails to start, or stops unexpectedly verify, the password is entered correctly in the **boot.properties** file.
- e. If you have an application server cluster, repeat this step on every server in the cluster before continuing to the next step.
15. From the enterprise portal, select **System Management > Enterprise > Settings**.
16. Under **Installations** (left pane), open the **Framework Applications** server role.
17. In the Framework Applications server role settings, update this field:
 - **Administrator Account Password** - Enter the new password for the WebLogic Admin Account here. (Click the icon to the right of the text box to set and confirm the password.)

18. Wait for the Pending Messages icon to disappear from the top of the screen before continuing to the next step.
19. Verify that the CMA distribution is completed successfully for the application servers.
 - a. Open the Enterprise Manager Agent (EMA) application on the application server.
 - b. To open the EMA, enter this URL in the web browser: **http://hostname/EMA**, where **hostname** is the host name of the application server.
 - c. Select **Status > System Monitor**.
 - d. In the **Status Messages** area, look for a message stating: **CMA Distribution: complete successfully on date_and_time**

Status Messages		
Component Name	Status	Message Details
CMA Distribution		CMA Distribution: Completed successfully on 8/12/2015 11:10:23 PM

20. Check the Alarm Dashboard for an alarm indicating that it is necessary to restart the WFO service.
 - a. From the enterprise portal, select **System Monitoring > System Monitor > Alarm Dashboard**.
 - b. In the Alarm Dashboard, look for an alarm named **Service restart required** that is active on an application server for which you have changed the WebLogic Admin Account password. If you have multiple application servers, you see one alarm for each application server. The alarm indicates that it is necessary to restart the **WFO_ProductionDomain_ProductionServer** service. (The alarm **Details** pane for an alarm indicates the specific service that must be restarted.)
 - c. When you see this alarm for an application server, restart the **WFO_ProductionDomain_ProductionServer** service on that application server and then acknowledge the alarm. If the Framework Applications plug-in fails, check the pluginerror.log file. Find the log file in: **<install_directory>\Software\UCMServices\Plugins\Databases\FrameworkApplications**.

What to do next

[Restore the Existing WebLogic 12.x Admin Account User Name or Password \(page 220\)](#)

Related information

Technologies, Security and Network Integration Deployment Reference Guide

Restore the Existing WebLogic 12.x Admin Account User Name or Password

If you cannot complete the WebLogic Admin Account user name or password change procedure successfully, you can restore (or rollback) the system to the existing WebLogic Admin Account user name or password.

Procedure

1. On the application server, stop the **WFO_ProductionDomain_ProductionServer** Windows service.
2. On the application server, restore the files that you backed up before beginning the account user name or password change procedure.

Copy the following backed up files over the existing ones on the application server:

- %VERINT_WEBLOGIC_DOMAIN_HOME%\config\config.xml
- %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\security\boot.properties
- %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\data\ldap

3. Complete this step if you attempted to change only the WebLogic Admin Account password. Otherwise, skip this step.

In Active Directory, reset the WebLogic Admin Account password to its previous value.

4. On the application server, start the **WFO_ProductionDomain_ProductionServer** Windows service.

Related topics

[Workflow: Change the WebLogic 12.x Administrator Account \(Windows Authentication\) \(page 208\)](#)

Workflow: Change the WebLogic 14.x Administrator Account (Windows Authentication)

In a windows domain authentication environment, the customer prepares a dedicated domain user to manage the WebLogic service for domain user application authentication. This user is referred to as the domain WebLogic Admin Account.



Follow this workflow only when using WebLogic 14.x. When using WebLogic 12.x, then follow the workflow for that version.

To change the user name or password for this account, use the following series of tasks:

1. [Back up the WebLogic 14.x Files Needed to Restore the Existing Account or Password \(page 221\)](#)
Before you change the Weblogic Admin Account user name or password, you must back up some files on the application server. If you cannot complete the account or password change procedure successfully, you need these files to restore the system to the existing account user name or password.
2. [Change the WebLogic 14.x Administrator Account to a Different User Account \(Windows Authentication\) \(page 222\)](#)
Perform this procedure to change the Weblogic Admin Account user name.
3. [Change the WebLogic 14.x Admin Account Password \(Windows Authentication\) \(page 227\)](#)
Perform this manual procedure to change only the WebLogic Admin Account password.
4. [Restore the Existing WebLogic 14.x Admin Account User Name or Password \(page 229\)](#)
If you cannot complete the WebLogic Admin Account user name or password change procedure successfully, you can restore (or rollback) the system to the existing WebLogic Admin Account user name or password.

Related topics

[Workflow: Change the WebLogic 12.x Administrator Account \(Windows Authentication\) \(page 208\)](#)

Back up the WebLogic 14.x Files Needed to Restore the Existing Account or Password

Before you change the Weblogic Admin Account user name or password, you must back up some files on the application server. If you cannot complete the account or password change procedure successfully, you need these files to restore the system to the existing account user name or password.

Back up these files and store them in a convenient location.

- %VERINT_WEBLOGIC_DOMAIN_HOME%\config\config.xml
- %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\security\boot.properties
- %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\data\ldap

What to do next

[Change the WebLogic 14.x Administrator Account to a Different User Account \(Windows Authentication\) \(page 222\)](#)

Change the WebLogic 14.x Administrator Account to a Different User Account (Windows Authentication)

Perform this procedure to change the Weblogic Admin Account user name.

Before you begin

[Back up the WebLogic 14.x Files Needed to Restore the Existing Account or Password \(page 221\)](#)

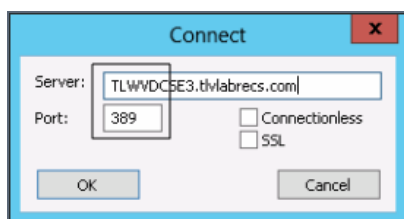
Procedure

1. Do one of the following:
 - Prepare a new account in the domain, according to requirements specified in the *Technologies, Security and Network Integration Deployment Reference Guide*.
 - Identify an existing account in the domain that meets the DRG requirements.



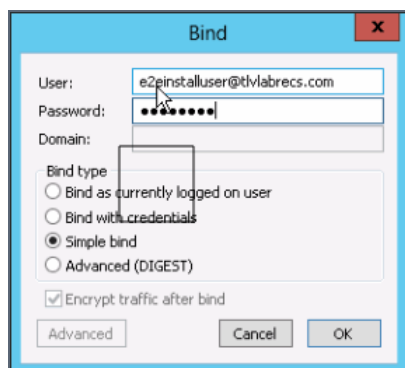
If you have an application server cluster, you must repeat steps 2 through 26 on each application server in the cluster.

2. Verify the new account created or identified in the previous step is working correctly. To verify, open the **ldp.exe** tool, connect to the domain controller, and do a simple bind using the account, as described in the steps that follow.
 - a. From the command prompt, start the **ldp.exe** tool.
 - b. Select **Connections > Connect**, complete these fields, and click **OK**:
 - **Server:** Enter the server name (FQDN) of the domain controller.
 - **Port:** Enter the port (default 389) to connect to the domain controller.



- c. Select **Connection > Bind**, complete these fields, and click **OK**:

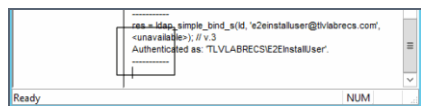
- **User:** Enter the user name of the new account in the User Principal Name (UPN) format.
- **Password:** Enter the password for the new account.
- **Bind Type:** Select the **Simple bind** option.



- d. Verify that the bind was successful.

A successful bind shows a result such as:

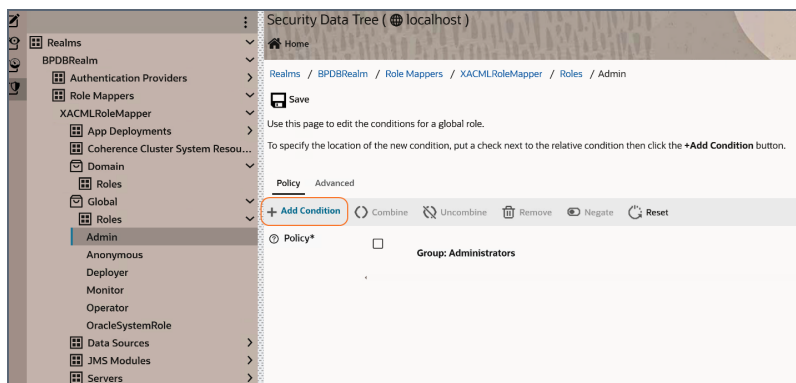
```
res=ldap_simple_bind_s(id, 'e2installuser@tlvlabrecs.com',
<unavailable>); // v.3
Authenticated as 'TLVLABRECS\E2EInstallUser'.
```



- e. Use the **ldp.exe** tool to search for any application user in the Active Directory.
3. On the Application Server, access the WebLogic administration rconsole using the following URL:
<http://localhost:7001/rconsole>
 4. Sign in to the rconsole using the existing WebLogic Admin Account credentials.
 5. From the tiles shown, select **Security Data Tree**.



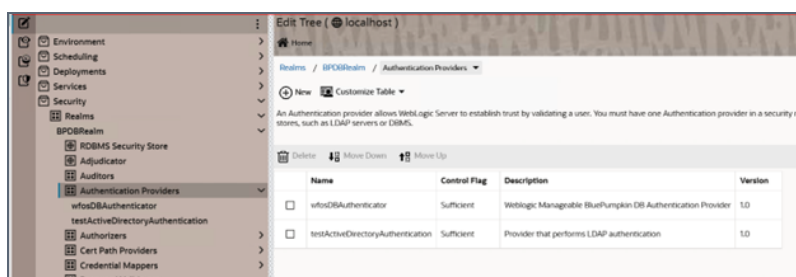
6. From the tree shown in the left pane, expand **Realms** and then expand **BPDBRealm**. Under **Global**, expand **Roles** and then select **Admin**.
7. From the **Policy** tab in the right pane, click **Add Condition**.



8. From the **Add New First Condition...** dialog box shown, complete the following settings:

- **Predicate List:** User
- **User Argument Name:** Enter the case-sensitive user name associated with the domain account that you created or identified in step 1 of this procedure.

9. From the Add New First Condition dialog box, click **OK**.
10. From the conditions page for the Admin role, click **Save**.
11. From the left pane toolbar, select **Edit Tree**.
12. From the tree shown in the left pane, expand **Security** and then expand **Realms**. Under **BPDBRealm**, select **Authentication Providers**.



13. From the right pane, select the name of the Active Directory provider. The **Description** for the Active Directory provider states, **Provider that performs LDAP authentication**.
14. Complete the following Active Directory Authenticator settings:

- **Principal: WLSAdmin**
 - **Credential:** Provide the WLSAdmin credential.
15. Click **Save**.
 16. From the upper right of the page, select the cart icon .
 17. Click **Commit Changes**. After the changes activate, the right pane shows the message, **All changes have been activated. However, 1 items must be restarted for the changes to take effect.**
 18. Use a text editor to update the **boot.properties** file on the application server.
 - a. Use Notepad or a similar text editor to open the **boot.properties** file on the application server from the following location:
%VERINT_WEBLOGIC_DOMAIN_HOME%servers\ProductionServer\security\boot.properties
 - b. For the **username=** parameter, type the new username (to replace the existing username value).
 - c. For the **password=** parameter, type the new password (to replace the existing password value).
 - d. Save the **boot.properties** file and close the text editor.

 The clear text username and password are encrypted after you restart the **WFO_ProductionDomain_ProductionServer** service in the next step

 - e. Restart the **WFO_ProductionDomain_ProductionServer** Windows service from the Services window on the server on which you have edited the boot.properties file.
 - If the **WFO_ProductionDomain_ProductionServer** service fails to start, or stops unexpectedly, verify the username and password are both entered correctly in the **boot.properties** file and restart the service again.
 - If the service still fails to start, check for errors in the **ProductionServer.log** at this location:
%AVAYAAURADATADIR%\Logs\ProductionServer\weblogic\ProductionServer.log
 19. Open a web browser and browse directly to the application server where you have made changes. To verify that you can successfully sign in using LDAP, sign in with the username and password of an active user.

 If you have an application server cluster, repeat all of the steps from the beginning of this procedure to this step on each application server in the cluster before continuing to the next step.
 20. From the enterprise portal, select **System Management > Enterprise > Settings**.
 21. Under **Installations** (left pane), open the **Framework Applications** server role.
 22. In the Framework Applications server role settings, update these two fields:
 - **Administrator Account Name** - Enter the username for the new WebLogic Admin Account here.
 - **Administrator Account Password** - Enter the password for the new WebLogic Admin Account here. (Click the icon to the right of the text box to set and confirm the password.)

23. Wait for the Pending Messages icon to disappear from the top of the screen before continuing to the next step.
24. Verify that the CMA distribution is completed successfully for the application servers.
 - a. Open the Enterprise Manager Agent (EMA) application on the application server. To access the EMA, enter this URL in the web browser: **http://hostname/EMA**, where **hostname** is the host name of the application server.

- b. Select **Status > System Monitor**.

- c. In the **Status Messages** area, look for a message stating: **CMA Distribution: complete successfully on date_and_time**

Status Messages		
Component Name	Status	Message Details
CMA Distribution		CMA Distribution: Completed successfully on 8/12/2015 11:10:23 PM

25. Check the Alarm Dashboard for an alarm indicating that it is necessary to restart the WFO service.
 - a. From the enterprise portal, select **System Monitoring > System Monitor > Alarm Dashboard**.
 - b. In the Alarm Dashboard, look for an alarm named **Service restart required** that is active on an application server for which you have changed the WebLogic Admin Account.
If you have multiple application servers, you see one alarm for each application server.
The alarm indicates that a restart of the **WFO_ProductionDomain_ProductionServer** service is required. (The alarm **Details** pane for an alarm indicates the specific service that must be restarted.)
 - c. When you see this alarm for an application server, restart the **WFO_ProductionDomain_ProductionServer** service on that application server and then acknowledge the alarm.
If the Framework Applications plug-in fails, check the pluginerror.log file. This log file is found in **<install_directory>\Software\UCMServices\Plugins\Databases\FrameworkApplications**.
To complete the account change process, correct the error.

What to do next

[Change the WebLogic 14.x Admin Account Password \(Windows Authentication\) \(page 227\)](#)

Related information

Troubleshoot SSO (*Authentication Configuration Guide*)

Technologies, Security and Network Integration Deployment Reference Guide

Change the WebLogic 14.x Admin Account Password (Windows Authentication)

Perform this manual procedure to change only the WebLogic Admin Account password.



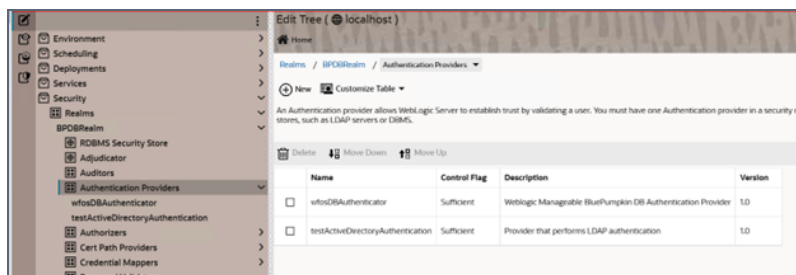
Perform this procedure before changing the WebLogic Admin Account password in the Windows domain.

Before you begin

[Back up the WebLogic 14.x Files Needed to Restore the Existing Account or Password \(page 221\)](#)

Procedure

1. On the Application Server, access the WebLogic administration rconsole using the following URL:
http://localhost:7001/rconsole
2. Sign in to the rconsole using the existing WebLogic Admin Account credentials.
3. From the left pane toolbar, select **Edit Tree**.
4. From the tree shown in the left pane, expand **Security** and then expand **Realms**. Under **BPDBRealm**, select **Authentication Providers**.



5. From the right pane, select the name of the Active Directory provider. The **Description** for the Active Directory provider states, **Provider that performs LDAP authentication**.
6. In the Active Directory Authentication parameters, provide the **Credential** used for authentication.
7. Click **Save**.
8. From the upper right of the page, select the cart icon .
9. Click **Commit Changes**. After the changes activate, the right pane shows the message, **All changes have been activated. However, 1 items must be restarted for the changes to take effect**.
10. An Active Directory administrator must perform this procedure in Active Directory.
 - a. Right click the user object and click **Reset Password**.
 - b. In the **New password** field, enter the new password.

- c. In the **Confirm password** field, enter the new password again.
- d. Make sure the **Unlock the user's account** check box is selected.
- e. Click **OK**.
11. Access the enterprise portal with a web browser, and verify that you can sign in using any Windows domain account that was previously used to access the portal.
If you cannot sign in, a mistake has occurred somewhere in this procedure. To reset the password, repeat this procedure from step 1.
12. Use a text editor to update the **boot.properties** file on the application server.
 - a. Use Notepad or a similar text editor to open the **boot.properties** file on the application server from the following location:
%VERINT_WEBLOGIC_DOMAIN_HOME%servers\ProductionServer\security
 - b. For the **password=** parameter, type the new password (to replace the existing password value).
 - c. Save the **boot.properties** file and close the text editor.

 The clear text password is encrypted after you restart the **WFO_ProductionDomain_ProductionServer** service in the next step.

- d. Restart the **WFO_ProductionDomain_ProductionServer** Windows service from the Services window on the server on which you have edited the **boot.properties** file.

 If the **WFO_ProductionDomain_ProductionServer** service fails to start, or stops unexpectedly verify, the password is entered correctly in the **boot.properties** file.
- e. If you have an application server cluster, repeat this step on every server in the cluster before continuing to the next step.
- 13. From the enterprise portal, select **System Management > Enterprise > Settings**.
- 14. Under **Installations** (left pane), open the **Framework Applications** server role.
- 15. In the Framework Applications server role settings, update this field:
 - **Administrator Account Password** - Enter the new password for the WebLogic Admin Account here. (Click the icon to the right of the text box to set and confirm the password.)
- 16. Wait for the Pending Messages icon to disappear from the top of the screen before continuing to the next step.
- 17. Verify that the CMA distribution is completed successfully for the application servers.
 - a. Open the Enterprise Manager Agent (EMA) application on the application server.
 - b. To open the EMA, enter this URL in the web browser: **http://hostname/EMA**, where **hostname** is the host name of the application server.
 - c. Select **Status > System Monitor**.
 - d. In the **Status Messages** area, look for a message stating: **CMA Distribution: complete successfully on date_and_time**

Status Messages		
Component Name	Status	Message Details
CMA Distribution		CMA Distribution: Completed successfully on 8/12/2015 11:10:23 PM

18. Check the Alarm Dashboard for an alarm indicating that it is necessary to restart the WFO service.
 - a. From the enterprise portal, select **System Monitoring > System Monitor > Alarm Dashboard**.
 - b. In the Alarm Dashboard, look for an alarm named **Service restart required** that is active on an application server for which you have changed the WebLogic Admin Account password. If you have multiple application servers, you see one alarm for each application server. The alarm indicates that it is necessary to restart the **WFO_ProductionDomain_ProductionServer** service. (The alarm **Details** pane for an alarm indicates the specific service that must be restarted.)
 - c. When you see this alarm for an application server, restart the **WFO_ProductionDomain_ProductionServer** service on that application server and then acknowledge the alarm. If the Framework Applications plug-in fails, check the pluginerror.log file. Find the log file in: **<install_directory>\Software\UCMServices\Plugins\Databases\FrameworkApplications**.

What to do next

[Restore the Existing WebLogic 14.x Admin Account User Name or Password \(page 229\)](#)

Related information

Technologies, Security and Network Integration Deployment Reference Guide

Restore the Existing WebLogic 14.x Admin Account User Name or Password

If you cannot complete the WebLogic Admin Account user name or password change procedure successfully, you can restore (or rollback) the system to the existing WebLogic Admin Account user name or password.

Procedure

1. On the application server, stop the **WFO_ProductionDomain_ProductionServer** Windows service.
2. On the application server, restore the files that you backed up before beginning the account user name or password change procedure.
Copy the following backed up files over the existing ones on the application server:
 - %VERINT_WEBLOGIC_DOMAIN_HOME%\config\config.xml
 - %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\security\boot.properties
 - %VERINT_WEBLOGIC_DOMAIN_HOME%\servers\ProductionServer\data\ldap
3. Complete this step if you attempted to change only the WebLogic Admin Account password. Otherwise, skip this step.
In Active Directory, reset the WebLogic Admin Account password to its previous value.
4. On the application server, start the **WFO_ProductionDomain_ProductionServer** Windows service.

Related topics

[Back up the WebLogic 14.x Files Needed to Restore the Existing Account or Password \(page 221\)](#)

[Change the WebLogic 14.x Administrator Account to a Different User Account \(Windows Authentication\) \(page 222\)](#)

[Change the WebLogic 14.x Admin Account Password \(Windows Authentication\) \(page 227\)](#)

Change the SSObind account

You can change the user name or password of the SSObind account. If you change the *password* of the SSObind account, you *must* replace the Keytab file.

In a windows domain with Single Sign-On (SSO) authentication environment, the customer prepares a dedicated domain user to authenticate against the Active Directory for SSO. This user is referred to as the domain SSObind account.

Procedure

1. Prepare a new account in the domain, according to DRG requirements.
Ensure to set the new account with a dedicated service principle name (SPN) and ktpass.
2. Validate **Active Directory** settings.
3. Run the **WebLogic Configuration** Tool.

Related topics

[Replace the Keytab file \(page 231\)](#)

Replace the Keytab file

Replace the keytab file if you change the SSOBind account's password, or if you change an encryption type. These are common scenarios for replacing the keytab file.

Procedure

1. Run a new SSO validation using the Active Directory Validation Tool. Make sure you select the correct encryption types in the SSO validation.
2. Do one of the following:
 - If the validation *is* successful, locate the file **SSOKeyTabFile** that was created in the AD Validation Tool's folder under the **products** sub-folder.
 - If the validation *is not* successful, troubleshoot SSO until it passes successfully.
3. Place the new **SSOKeyTabFile** in the following folder, replacing the previous version:
%Impact360Softwaredir%ProductionServer\weblogic\Impact360\ProductionDomain
4. Restart the **WFO_ProductionDomain_ProductionServer** service.

Related information

Workforce Optimization Active Directory Validation Tool Guide

Create TAS user group and TAS user accounts

Create a TAS user group, and add the required types of TAS users, the Installation, Application, Advanced Application, and Maintenance users.



You must create the TAS user group and the TAS users on each of the TAS servers in your deployment.

Procedure

1. Create a **TAS user group** with ID 5000, and default name `tas`.

```
groupadd -g 5000 tas
```

2. Create an **Installation** service user:

- a. Add the installation user with user name `tas_inst` to the TAS user group:

```
useradd -g 5000 -u 5002 tas_inst
```

- b. If required, change the default password for the `tas_inst` user:

```
passwd tas_inst
```

- c. Open the `/etc/sudoers` file and add the following line at the end of the file to add the `tas_inst` user to the sudoers group:

```
tas_inst ALL=(ALL) ALL
```

3. Create an **Application Management** service user:

- a. Add the application user with user name `tas_app` to the TAS user group:

```
useradd -g 5000 -u5001 tas_app
```

- b. If required, change the default password for the `tas_app` user:

```
passwd tas_app
```

- c. Disable login for `tas_app` user:

```
usermod -s /usr/sbin/nologin tas_app
```

4. Create a **Maintenance** service user:

- a. Add the maintenance user with the user name `tas_maint` to the TAS user group:

```
useradd -g 5000 -u 5003 tas_maint
```

- b. If required, change the default password for the `tas_maint` user:

```
passwd tas_maint
```

- c. Add the `tas_maint` user to the Docker group:

```
usermod -G docker tas_maint
```

- d. Open the `/etc/sudoers` file and add the following line at the end of the file to add the `tas_maint` user to the sudoers group:

```
tas_maint ALL=(ALL) ALL
```


Changing server computer names, domains, and workgroups

You may need to change the Windows computer names, the Windows domain memberships, or the Windows workgroup memberships of the managed servers in your enterprise for a variety of reasons.

Topics

Overview	234
Understand the workflow for changing computer names, domains, and workgroups	235
Step 1: Establish trust between the current domain and the target domain	237
Step 2: Change the computer name, domain, or workgroup of an individual server	239
Step 3: Break the trust between the original domain and the new domain	267

Overview

This chapter explains how to change any of the following on one or more servers in your enterprise:

- The computer name
- The domain membership
- Both the computer name and the domain membership
- The workgroup membership
- Both the computer name and the workgroup membership

Before beginning these procedures, it is important to understand the workflow for changing computer names, domains, and workgroups. The procedures you must perform vary depending on the type of change you want to make.

Understand the workflow for changing computer names, domains, and workgroups

Before you perform any procedures described in this chapter you must understand the workflow for changing Windows computer names, domain memberships, and workgroup memberships. The workflow varies depending on the type of change you are making.

There are three different possibilities when changing the computer names, domain memberships, and workgroup memberships of the servers in your environment.

Determine which of these three types of changes you need to make. The workflow varies for each of these three types of changes:

- **Change computer name(s) without changing the domain membership** - In this scenario, you need to change one or more computer names (or computer workgroup memberships), but you do not need to change the domain memberships of any servers in your environment. You might make a change like this when replacing old hardware with new hardware.

This type of change requires you to perform only the procedures in [Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#), as illustrated in the [Computer name and domain change workflow \(page 235\)](#). You must repeat the procedures in Step 2 on every server whose name you want to change.

- **Change the domain memberships of some, but not all, of your servers** - In this scenario, you need to move some of the servers in your environment into a new Windows domain, while others will remain in the original domain. Also, you may (or may not) need to change the computer names of these servers. You might make a change like this due to a reorganization of your enterprise.

This type of change requires you to perform these procedures:

- [Step 1: Establish trust between the current domain and the target domain \(page 237\)](#)
- [Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#). You must repeat the procedures in Step 2 on every server you want to change.

This workflow is also illustrated in the [Computer name and domain change workflow \(page 235\)](#).

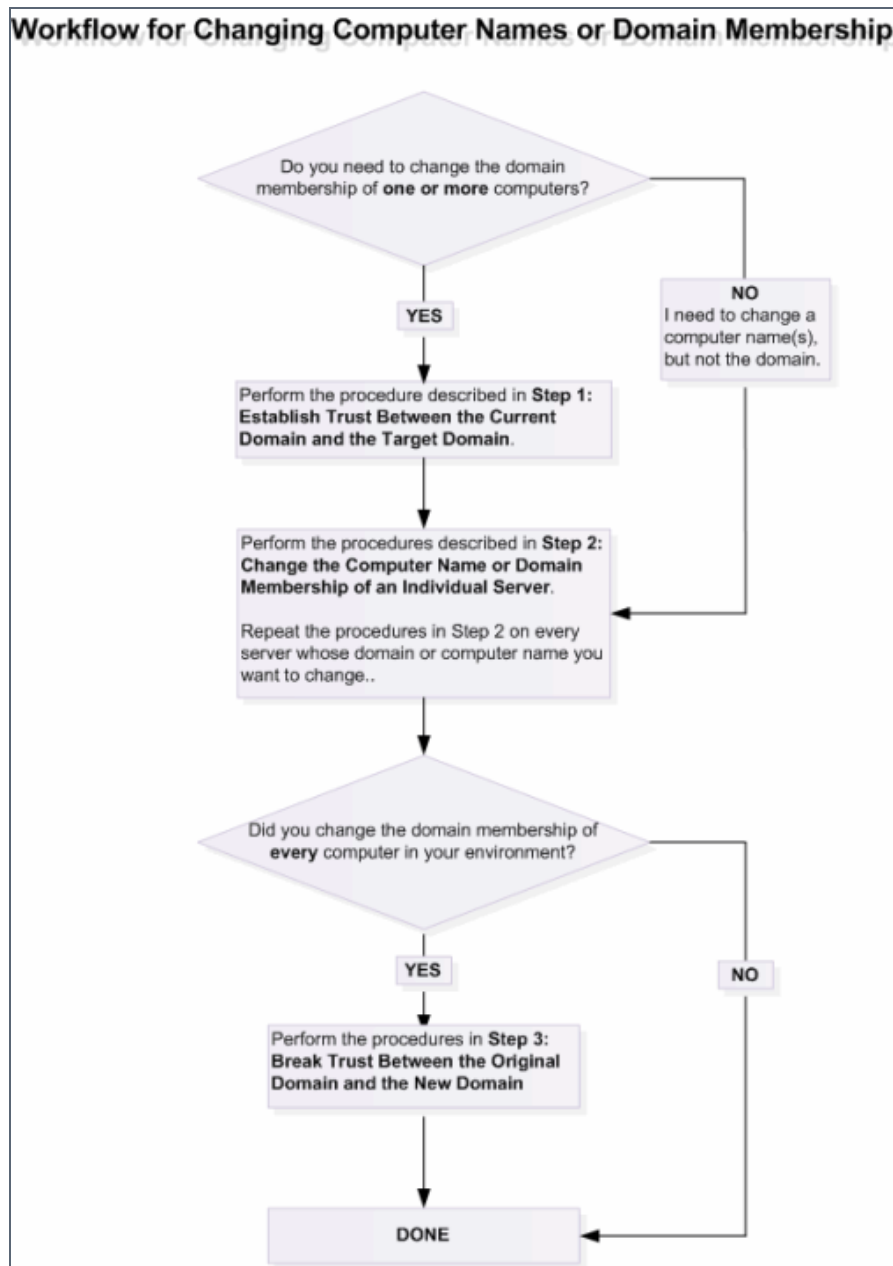
- **Change the domain memberships all of your servers** - In this scenario, you need to move **all** of the servers in your environment to a new Windows domain. Also, you may (or may not) need to change the computer names of the servers. You might make a change like this if one company merges with another and you need to move all of the servers in an enterprise onto a different Windows network.

This type of change requires you to perform all three steps described in this chapter, as illustrated in the [Computer name and domain change workflow \(page 235\)](#).

Computer name and domain change workflow

The following diagram illustrates the workflow for changing the Windows computer names, domains, and workgroups of the servers in your environment. If necessary, review the topic [Understand the](#)

[workflow for changing computer names, domains, and workgroups \(page 235\)](#) for assistance in understanding this workflow.



Step 1: Establish trust between the current domain and the target domain

Step 1 is the first of three steps associated with changing the Windows computer name or domain membership of the managed servers in your enterprise.



Perform this step *only* if you intend to change the domain membership of one or more computers in your environment.

If you only want to change a computer name(s), or workgroup membership, and you do *not* intend to change the domain membership of any computers in your environment, skip this step and continue to [Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#).

Consult the workflow diagram, [Computer name and domain change workflow \(page 235\)](#), for more information.

The two procedures associated with Step 1 include:

1. Establish trust between the domains

Procedure 1 of 2 associated with Step 1 - establish trust between the current domain and the target domain.

To complete this procedure, you must establish trust between the Windows domain that the servers currently reside in, and the target Windows domain to which you intend to move the servers.

If you are moving one or more computers from their current domain to a different domain, it is mandatory that a full two-way trust exist between the two domains. If this trust does not exist, establish this trust before continuing to [Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#).

For details on establishing full two-way trust between forests and domains, see the Microsoft MSDN site or consult with your Microsoft network administrator.

2. Change domain for desktop users

Procedure 2 of 2 associated with Step 1 - establish trust between the current domain and the target domain.



Perform this procedure only if the users of desktop applications (employees) in your enterprise are moving to a new Windows domain. If the employees are not moving to a new domain, skip this procedure and continue to [Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#).

When users move to a new domain, you must update the enterprise settings that specify the fully-qualified domain name of the users. These updates are required to enable the users to use desktop applications after the users are moved to a new domain.

To complete this procedure, perform the updates described in the “Change Domain for Desktop Users” section of the *User Management Guide*.

What to do next

[Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#)

Step 2: Change the computer name, domain, or workgroup of an individual server

Step 2 is the second of three steps associated with changing the Windows computer name, domain membership, or workgroup membership of the managed servers in your enterprise.

This procedures in this step explain how to make any of the following changes on one managed server:

- The computer name
- The domain membership
- Both the computer name and the domain membership
- The workgroup membership
- Both the computer name and the workgroup membership



If you are changing the domain membership of any of your servers, you must perform the procedure described in [Step 1: Establish trust between the current domain and the target domain \(page 237\)](#) before performing this step.

Consult the [Computer name and domain change workflow \(page 235\)](#) for more information.

Changing multiple servers

If you are changing the Windows computer name, domain membership, or workgroup membership of multiple servers, you must change the servers one at a time by repeating the procedures in Step 2 on every server you want to change.

If you are changing multiple servers, change the servers in the order shown below:

1. **Framework Database server** - First, change the server with the active Framework Database server role.
2. **Framework Applications server** - Next, change the server with the active Framework Applications server role. If you have a cluster of servers with the Framework Applications server role active, be sure to perform the procedures in Step 3 that are specific to clustered servers.
3. **Remaining Database servers** - Next, change the remaining database servers.
At this point, you have already changed the server with the Framework Database server role. The remaining database servers include any server on which a database server role is active, and any computer running an SQL Server that is accessed by those database server roles.
4. **Data Center servers** - Next, change the remaining servers in the Data Center.
5. **Site Servers** - Next, change the Site servers (Speech Analytics servers, Customer Feedback Survey servers, and Framework Integration Service servers).

Step 2 procedures

This section includes all of the procedures for making any of the following changes on one managed server:

- The computer name
- The domain membership
- Both the computer name and the domain membership
- The workgroup membership
- Both the computer name and the workgroup membership

This process includes the procedures listed below.



When performing the procedures in Step 2, it is usually not necessary to perform every procedure described for every server. The procedures you must perform are dependent on the configuration of the server, and the server roles that are active on the server whose computer name, domain, or workgroup you are changing.

Review the procedures in the order they are presented and read each procedure carefully. Each procedure will state when it is, and is not, necessary to perform the procedure.

1. [Verify the server meets the requirements \(page 241\)](#)
2. [Stop and disable the Integration Server Service \(page 241\)](#)
3. [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#)
4. [Back up the SSRS Encryption Key \(page 245\)](#)
5. [Change the Management Services Account and Database Management Account for the server \(page 246\)](#)
6. [Change the Windows computer name/domain/workgroup membership on the server \(page 247\)](#)
7. [Run the SQL Server Change Computer Name application to rename an SQL Server \(page 248\)](#)
8. [Ensure that SSRS can access the Reporting Services database \(page 250\)](#)
9. [Restore the SSRS Encryption Key \(page 251\)](#)
10. [Generate and install new TLS Server Certificates \(page 252\)](#)
11. [Run the ChangeComputerName.cmd script \(page 253\)](#)
12. [Change the server name on the server Settings screen \(page 255\)](#)
13. [Change the SQL server name on server role Settings screens \(page 255\)](#)
14. [Update DPA with new Recorder server name \(page 257\)](#)
15. [Review the alarms and restart services \(page 257\)](#)
16. [Remove the old Integration Server name from BPMAINDB \(page 259\)](#)
17. [Restart the IP Analyzer \(page 259\)](#)
18. [Change the configuration of any affected desktop applications \(page 260\)](#)
19. [Perform the steps to complete the changes for clustered Framework Application servers \(page 262\)](#)
20. [Review alarms and restart services \(page 264\)](#)
21. [Determine what to do next \(page 265\)](#)

Step-by-step instructions for each of these procedures are described in the topics that follow.

Verify the server meets the requirements

Procedure 1 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



This procedure is required for *every* server.

The subsequent procedures in Step 2 assume that the server whose name or domain membership is being changed meets all of the requirements that are described in Chapters 2 through 5 of the *Technologies, Security and Network Integration Deployment Reference Guide*.

Before you continue with the subsequent procedures in Step 2, first verify that all requirements described in the *Technologies, Security and Network Integration Deployment Reference Guide* are met for the server you are changing.

What to do next

[Stop and disable the Integration Server Service \(page 241\)](#)

Stop and disable the Integration Server Service

Procedure 2 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure only if the server whose name or domain you are changing is an Integration Server.

To determine if the server is an Integration Server:

- Go to **Integration Management > Integration Server > Integration Servers**
- All Integration Servers appear under the **Server Name** column on the Integration Servers page.

If the server appears under the **Server Name** column, perform this procedure.

If the server does not appear under the **Server Name** column, skip this procedure and continue to the next procedure, [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#).

In this procedure, you must stop and disable the Integration Server service on the managed server.

To stop and disable the Integration Server service do one of the following:

- If the Watchdog application is running on the managed server, use the Watchdog application to stop and disable the Integration Server service.

If the Watchdog application is running on the server, a System Tools icon is available from the Windows task bar.

1. Right-click on the **System Tools** icon, and select **Run > Watchdog**.
2. Click on the **Integration Server** service and click **Stop**.
If prompted with "The Watchdog Service is running. Do you want to stop it now?", select **No**.
Note that it may take a minute or two for the Integration Server service to stop.
3. Click on the Integration Server service, click **Startup**, and select **Disabled**.
- If the Watchdog application is not running on the managed server, use the Windows Administrative Tools to stop the Integration Server service.
 1. From the Windows desktop, select **Start > Administrative Tools > Services**.
 2. Right-click on the Integration Server service and select **Stop**.
 3. Right-click on the Integration Server service and select **Properties**.
 4. In the Startup type: drop-down list, select **Disabled**.
 5. Click **Apply** and then click **OK**.
 6. Close the Services page.

What to do next

[Perform the prerequisite steps for clustered framework applications servers \(page 242\).](#)

Perform the prerequisite steps for clustered framework applications servers

Procedure 3 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure only if your enterprise includes a cluster of application servers (a cluster of servers that have the Framework Application server role active), and you want to change the computer name or domain membership of one or more of those servers.

If you do not have an application server cluster in your enterprise, skip this procedure. Go on to [Back up the SSRS Encryption Key \(page 245\)](#) and continue.

If you have a cluster of application servers, the procedure you must perform at this point depends on the type of change you want to make:

- If you are changing the computer name, but not the domain membership, of one or more servers in the cluster, perform the procedure described in [Changing only the computer names of clustered servers \(page 242\)](#).
- If you are changing the computer names **and** domain membership, or just the domain membership, of all servers in the cluster, perform the procedure described in [Changing the domain of the clustered servers \(page 243\)](#).

Changing only the computer names of clustered servers

Perform these steps if you are changing the computer name of one or more clustered servers, but not the domain membership of the clustered servers.

In this procedure, you use Enterprise Manager to delete the server whose name you are changing from the cluster, and then disconnect the server from the load balancing device.

Follow the steps below:

1. Click on **System Management > Enterprise Management > Settings**.
2. In the installations tree (left pane), expand the Cluster node to which the server belongs and then select the individual server.
3. Click **Delete**.
4. Physically disconnect the server you have just deleted from the load balancing device that distributes connections to the cluster.
5. Continue to [Change the Management Services Account and Database Management Account for the server \(page 246\)](#) and continue following the procedures in Step 2 to change the name of the server you have just deleted from the cluster.

You will add this server back to the cluster in a subsequent procedure at the end of Step 2.

Changing the domain of the clustered servers

Perform these steps if you are changing the computer name and domain membership, or just the domain membership, of all servers in the cluster.

In this procedure, you use Enterprise Manager to perform two tasks:

- Delete all of the servers from the cluster except for one.
- Delete all of the servers from the cluster except for one.

Follow the steps below.



If you have already performed this procedure, and you are now in the process of changing the names of the servers that were deleted from the cluster, skip this procedure and see the Important note at the end of this procedure.

1. Click on **System Management > Enterprise Management > Settings**.
2. In the Installations tree (left pane), expand the Cluster node to which the server belongs and then select an individual server.
3. Click **Delete**.
4. Repeat steps 2 and 3 to delete all of the servers from the cluster **except one** of the servers.
5. Physically disconnect the deleted servers from the load balancing device that distributes connections to the cluster.
6. Move the one remaining server in the cluster out of the Cluster node and into the Site node that contains the cluster. (This procedure removes the server from the cluster).
 - a. In the Installations tree (left pane), expand the Cluster node to which the server belongs and then select the one remaining server in the cluster.
 - b. Select **More Actions > Move Installation**.
 - c. In the right-hand pane, under Target Installations, select the Site node that contains the Cluster node.
 - d. Click **Move**. (The server now exists in the same Site as the cluster but is no longer part of the cluster.)

7. Continue to [Change the Windows computer name/domain/workgroup membership on the server \(page 247\)](#) and continue following the procedures in Step 2 to change the name of the server you have just moved from the Cluster node to the Site node.

A subsequent procedure at the end of Step 2 will explain how to return this server to the cluster and how to handle the other servers that you deleted from the cluster.



If you have already performed the procedure above, and you are now changing the domain of one of the servers that you deleted from the cluster (not moved, but deleted), skip the procedure above and continue to [Change the Windows computer name/domain/workgroup membership on the server](#) to continue performing the procedures in Step 2 for the server that was deleted from the cluster

What to do next

[Back up the SSRS Encryption Key \(page 245\)](#)

Back up the SSRS Encryption Key

Procedure 4 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this procedure only if you are changing the name of the computer running SQL Server that hosts the Reporting Services database. Otherwise, skip this procedure and continue to [Change the Management Services Account and Database Management Account for the server \(page 246\)](#).

In this procedure, you back up the SSRS Encryption Key on the server that hosts the Reporting Services database. (You will be required to restore the Encryption Key backup in a subsequent procedure.)

1. On the computer running SQL Server that hosts the Reporting Services database, open the **Reporting Services Configuration Manager**.
Click **Start > All Programs > Microsoft SQL Server R2 > Configuration Tools > Reporting Services Configuration Manager**.
2. Click **Yes** when prompted to allow the program to make changes to this computer.
3. In the **Reporting Services Configuration Connection** screen, click **Connect** to connect to the Report Server Instance that hosts the Reporting Services database.
4. In the **Reporting Services Configuration Manager**, click **Encryption Keys** in the left pane.
5. In the Backup section, click **Backup**.
6. In the **Backup Encryption Key** screen, complete these fields.
 - **File Location:** - Select the directory where you want to store the Encryption Key backup.
 - **Password:** - Enter the password that protects the Encryption Key backup from unauthorized access. (You will be required to enter this password to successfully restore the Encryption Key in a subsequent procedure.)
 - **Confirm Password:** - Re-enter the password specified above.



Be sure to note the file location and the password of the Encryption Key backup file. You must know this information to restore the Encryption Key in a subsequent procedure.

7. Click **OK**.
8. Enter a file name for the Encryption Key backup file, and click **Save**.
9. Click **Exit**.

What to do next

[Change the Management Services Account and Database Management Account for the server \(page 246\)](#)

Change the Management Services Account and Database Management Account for the server

Procedure 5 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this procedure only if you are changing the name of a computer that is a member of a Windows workgroup.

If the computer you are changing is a member of a Windows domain, skip this step and continue to [Change the Windows computer name/domain/workgroup membership on the server \(page 247\)](#).

This procedure consists of two tasks:

1. [Create a new Management Service Account \(MSA\) and Database Management Service Account \(DMSA\) \(page 246\)](#)
2. [Use Enterprise Manager to change the MSA and DMSA for the server \(page 246\)](#)

Create a new Management Service Account (MSA) and Database Management Service Account (DMSA)

Task 1 of 2 associated with changing the Management Services Account and Database Management Account for the server.

To complete this task, you must create two new Windows Workgroup user accounts, as noted below:

- Create one Windows Workgroup user account to serve as the MSA for the computer whose name you are changing.
- Create one Windows Workgroup user account to serve as the DMSA for the computer whose name you are changing.

For details about creating MSA and DMSA user accounts, see the *Technology, Security, & Network Integration Deployment Reference Guide*.

Use Enterprise Manager to change the MSA and DMSA for the server

Task 2 of 2 associated with changing the Management Services Account and Database Management Account for the server.

To complete this task, you must use Enterprise Manager to specify the new accounts you have just created as the MSA and DMSA for the server whose name you are changing.

1. Select **System Management > Enterprise > Settings**.
2. In the Installations tree (left pane), select the **server whose name you are changing**.
3. Select **Enterprise Settings**.
4. In the **Management Service Account** section, change the **Username:** field value so that it specifies the account user name of the new MSA user account you have just created.

For example:

The **Username:** field specifies the account user name in this format:
computername\accountname

Change the **computername** parameter of the account user name so that it specifies the new name for the computer.

5. In the **Database Management Account** section, change the **Username:** field value so that it specifies the account user name of the new DMSA user account you have just created (exactly as described for the **Management Service Account** above).
6. Click **Save**.

What to do next

[Change the Windows computer name/domain/workgroup membership on the server \(page 247\)](#)

Change the Windows computer name/domain/workgroup membership on the server

Procedure 6 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this procedure for every server you change.

Note that if HTTPS is enabled on the server you are changing, you will be instructed to replace the TLS Server Certificates in a subsequent procedure.

Even if you have changed to a new domain, use the OLD DOMAIN and OLD DOMAIN ACCOUNT in this procedure, until you are prompted to do otherwise.

In this step you must change one or more of these settings in the Windows operating system of the computer you are changing.

- The computer name
- The domain name
- The workgroup name

For example, if you are changing only the computer name, change only the computer name setting. If you are changing both the computer name and domain, change both the computer name and domain.

1. To change the server's computer name, domain membership, or workgroup membership in the Windows operating system, follow this basic procedure:
 - a. Open the Windows Control Panel on the server computer.
 - b. Click the **System** icon.
 - c. In the **Computer name, domain, and workgroup settings** section, click **Change Settings**.

- d. Click **Change**.
- e. Change the computer name, domain membership, and workgroup membership as appropriate.

 The procedure above may vary slightly for different Windows operating system versions. If necessary, see the Microsoft MSDN site or consult with your Microsoft network administrator for more information.

2. Reboot the server after changing the computer name, domain membership, or workgroup membership.

 If you have stopped and disabled the Integration Server service as described in [Stop and disable the Integration Server Service \(page 241\)](#), make sure that the Integration Server service does not restart automatically after the server reboots. If the service does restart automatically, stop and disable it again.

What to do next

[Run the SQL Server Change Computer Name application to rename an SQL Server \(page 248\)](#)

Run the SQL Server Change Computer Name application to rename an SQL Server

Procedure 7 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.

 Perform the steps in this procedure only if you are changing the name of a computer running SQL Server. (This is the server whose name you just changed in [Change the Windows computer name/domain/workgroup membership on the server \(page 247\)](#).)

If the computer whose name is being changed is not running SQL Server, skip this procedure and continue to the next procedure, [Ensure that SSRS can access the Reporting Services database \(page 250\)](#).

Note that this procedure is also relevant for remote computers running SQL server, where the SQL Server is not installed on the same server as the database server platform but on a separate server that hosts only the SQL Server.

In this procedure, you run the SQL Server Change Computer Name application to execute an internal name change required by the SQL server.

The SQL Server Change Computer Name application resides on every server on which a database server platform is installed (for example, the Database platform or Framework Database platform). You can use the SQL Server Change Computer Name application to create a remote connection to the computer running SQL Server and execute the name change on the computer running SQL Server. The SQL Server Change Computer Name application does not have to run on the same computer as the computer running SQL Server.

Procedure

1. Open the following directory on any computer on which a database server platform is installed:
<install_directory>\Software\CommonDB\Utils\Change Computer Name

i On the Customer Feedback Survey server, the SQL Server Change Computer Name application is in the following location:
<install_directory>\Software\CFtomcat64\Utils

2. Do the following:
 - a. Press SHIFT+Right-click on the **SQL Server Change Computer Name** application and select **Run as different user**.
 - b. Enter the name and password of the Windows account that has SysAdmin administrative privileges on the computer running SQL Server.

i The account used in step 2 b. above is at the discretion of the customer.
If you have configured a Database Management Account (DMSA) in your enterprise, you can provide DMSA with SysAdmin privileges and run the SQL Server Change Computer Name application under the DMSA account.

3. In the SQL Server Change Computer Name dialog, do the following:
 - a. Under **SQL Server Connection Properties**, in the **SQL Server:** field, enter the new name of the computer on which the SQL Server resides. (The application will connect to this server to make the internal name change.)
 - b. In the **Port:** field, enter the port on which the computer running SQL Server listens for connections (default 1433).
 - c. Click **Connect**.
The previous name of the computer running SQL Server and the current (new) name of the computer running SQL Server display under the **Computer Name Details** section on the right-side of the dialog.
 - d. Verify that the **Previous Name:** field and the **Current Name:** fields display the correct previous and current names of the computer running SQL Server, respectively.
 - e. Click **Change SQL Name** and respond to the prompts.
 - f. When prompted to restart the SQL Server Service, restart the Windows service named **SQL Server** on the server whose name you have changed. (For example, from Windows select **Start > Administrative Tools > Services** and restart the service.)

i If you provided the DMSA account with SysAdmin privileges to complete step 2 b., remember to revoke those privileges from the account.

What to do next

Ensure that SSRS can access the Reporting Services database (page 250).

Ensure that SSRS can access the Reporting Services database

Procedure 8 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an individual managed server.



Perform this procedure only if you are changing the name of the computer running SQL Server that hosts the Reporting Services database. Otherwise, skip this procedure and continue to [Change the server name on the server Settings screen \(page 255\)](#).

In this procedure, you use the Reporting Services Configuration Manager to ensure that SSRS can access the Reporting Services database on the renamed computer running SQL Server.

Perform this procedure from the server that hosts the Reporting Services server role.

1. Launch the **Reporting Services Configuration Manager**.
(Usually located at **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > Reporting Services Configuration Manager**.)
2. In the left pane, select **Databases**.
3. Select **Change Database**.
The Report Server Database configuration wizard opens.
4. Select **Choose an existing report server database** and click **Next**.
The Database Server settings display in the right pane.
5. In the **Server Name** field, enter the new name of the server that hosts the Reporting Services database.
6. Verify that **Authentication Type** is set to **Current User-Integrated Security**, and then click **Test Connection**.
The database connection is tested.
 - If the connection succeeds, a page will indicate a successful connection. Click **OK** to close the page.
 - If the connection fails, you must diagnose the connection issue and retry the connection test.After successfully testing the connection, click **Next**.
7. At the **Select a report server database** screen, do the following:
 - For **Report Server Database**, select **ReportServer** (the Reporting Services database).
 - Click **Next**.
8. In the right pane, the Credential settings display. Do not change any settings on this page. Click **Next**.
9. In the right pane, the Wizard Summary displays. Click **Next**.
The database configuration launches, and the status is displayed in the right pane. When the configuration completes, **Finish** is enabled.
10. Click **Finish**. The Reporting Services Configuration Manager page is displayed again.

What to do next

[Restore the SSRS Encryption Key \(page 251\)](#)

Restore the SSRS Encryption Key

Procedure 9 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this procedure only if you are changing the name of the computer running SQL Server that hosts the Reporting Services database. Otherwise, skip this procedure and continue to [Generate and install new TLS Server Certificates \(page 252\)](#).

In this procedure, you:

- Restore the SSRS Encryption Key on the server that hosts the Reporting Services database. You restore the Encryption Key that you backed up in the procedure [Back up the SSRS Encryption Key \(page 245\)](#).
 - Test the Web Service URL used to access the Report Server. This step verifies connectivity with the Report Server after restoration of the encryption key.
1. On the computer running SQL Server that hosts the Reporting Services database, open the **Reporting Services Configuration Manager**.
Click **Start > All Programs > Microsoft SQL Server R2 > Configuration Tools > Reporting Services Configuration Manager**.
 2. Click **Yes** when prompted to allow the program to make changes to this computer.
 3. In the **Reporting Services Configuration Connection** screen, click **Connect** to connect to the Report Server Instance that hosts the Reporting Services database.
 4. In the **Reporting Services Configuration Manager**, click **Encryption Keys** in the left pane.
 5. In the Restore section, click **Restore**.
 6. In the **Restore Encryption Key** screen, do the following:
 - a. **File Location:** - Open the directory in which you stored the Encryption Key backup file, and select the backup file. Click **Open**.
 - b. **Password:** - Enter the password that you specified to protect the Encryption Key backup from unauthorized access. Click **OK**.
 7. Test the Web Service URL used to access the Report Server.
 - a. Click **Web Service URL** in the left pane.
 - b. Under **Report Server Web Service URLs** in the right pane, click on the URL.
 - c. On the **SQL Server Reporting Services - Report Server** login page, enter the User Name and Password of the MSA and click **Logon**. Verify that the connection to the Report Server is successful.
 8. Click **Exit**.



You specified the file location and the password for the Encryption Key backup file in the procedure [Back up the SSRS Encryption Key \(page 245\)](#).

What to do next

[Generate and install new TLS Server Certificates \(page 252\)](#)

Generate and install new TLS Server Certificates

Procedure 10 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this step only if **both** of the following are true:

- HTTPS is enabled for the managed server you are changing
- The server name on the server's existing TLS Server Certificate is different than the new name that you specified for the server in the procedure [Change the Windows computer name/domain/workgroup membership on the server \(page 247\)](#).

To complete this procedure, you must generate new TLS Server Certificates that specify the new server name, and then install these certificates on the server.

For details about generating and installing TLS Server Certificates on a managed server, see the Security Guide.

What to do next

[Ensure the Recorder Archive Service log on account can run in the new domain or new workgroup \(page 252\)](#)

Ensure the Recorder Archive Service log on account can run in the new domain or new workgroup

Procedure 11 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure only if **all** of the following are true:

- The Central Archive server role is active on the server you are changing. (In this case, the Recorder Archiver Service also runs on the server.)
- You are changing either the server's domain membership or the server's workgroup membership.
- The archive media type used in the enterprise is SAN and the network path to this media type is a fileshare.

If all of the conditions above are **not** true, skip this procedure and continue to the next procedure, [Run the ChangeComputerName.cmd script \(page 253\)](#).

In this procedure, you must ensure that the Windows account under which the Recorder Archiver Service runs has read/write/delete permission to the network fileshare specified for the SAN media type. (This network fileshare path is specified in the Recording Management > Campaigns > Archive Media page.)

Use the following procedure to determine the Log On account under which the Recorder Archiver Service runs and to verify that this account has the appropriate permissions to the SAN fileshare in the new Windows domain.

1. On the computer whose domain membership you have changed, select **Start > Administrative Tools > Services**.
2. In left-hand pane of the **Component Services** page, select **Services (Local)**.
3. In the right-hand pane, right-click on **Recorder Archive Service** and select **Properties**.
4. Select the **Log On** page.
5. The **Log On** page displays the Log On account under which the Recorder Archive Service runs.
6. Once you have determined the account under which the Recorder Archiver Service runs, verify that this account has read/write/delete permission in the new domain to the network fileshare specified for the SAN media type.

If the existing account does not have read/write/delete permission to the SAN network fileshare in the new domain, assign a Windows account to the Recorder Archiver Service that does have these permissions.

What to do next

[Run the ChangeComputerName.cmd script \(page 253\)](#)

Run the ChangeComputerName.cmd script

Procedure 12 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an individual managed server.



Perform this procedure on every server whose computer name you change. If you are changing the domain membership of the server, but not the computer name, you can skip this procedure and continue to the next procedure, [Change the server name on the server Settings screen \(page 255\)](#).

- If you are changing the computer name of the server **that hosts the Framework Database** you must perform this procedure on **both** of these servers in the order shown below:
- The server hosting the Framework Database.
- The application server.

In this procedure, you run the ChangeComputerName.cmd script. This script performs Secure Gateway proxy configuration changes and changes the Weblogic connection strings for the BPMAINDB database. The script also reinstalls the Weblogic service when it is run on the application server.

You run this script from the server command prompt. Follow the instructions below:

1. Open the Command Prompt on the server using the Run as administrator option:
 - a. From the Windows desktop, click **Start**.
 - b. Right-click on the **Command Prompt** option and select **Run as administrator**.
 - c. Log in to the Command Prompt using the name and password of the Windows administrator account on the server.
2. From the Command Prompt, run the **ChangeComputerName.cmd** script in the **<install_directory>\Software\Conf\Security** directory.

- a. In the Command Prompt window, use the **cd** command to change to the following directory (the script resides in this directory):
`<install_directory>\Software\Conf\Security`
- b. At the Command Prompt, type **ChangeComputerName.cmd** and press **Enter** to run the script.
3. The script prompts you for the following parameters:
 - **New computer name of the host** - Enter the new computer name of the server on which you are running the script (note the exception below).



If you are changing the name of the server that hosts the Framework Database, you must run the script on both that server and the application server.

- Complete these parameters only when running the script on the application server (for example, if you have changed the name of the application server, or if you have changed the name of the server that hosts the Framework Database and you are also running the script on the application server):
 - **Management Service Account Domain** - Enter the Windows domain of the Windows account specified as the Management Service Account.
 - **Management Service Account Username** - Enter the account username.
 - **Management Service Account Password** - Enter the account password.
 - **Was the name of the server hosting the Framework Database changed?** At this prompt, type **Y** only if you are running the script on the application server because the server hosting the Framework Database server name has changed. Otherwise, type **N**, and continue to step 4. If you type **YES**, complete these two prompts:
 - **New computer name of the FW Database Server** - Enter the new computer name of the server that hosts the Framework Database.
 - **SQL Port on the Framework Database Server** - Enter the port number on which the computer running SQL Server that hosts the Framework Database listens for connections (default port is 1433).
4. Verify that the confirmation message is displayed indicating the script completed successfully.



When changing the name of the server that hosts the Framework Database, make sure to run this script both on the Framework Database server and on the application server.

What to do next

[Change the server name on the server Settings screen \(page 255\)](#)

Change the server name on the server Settings screen

Procedure 13 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this procedure for every server that you change.

In some cases, it may not be necessary to change any settings on the Server's **Settings** page (for example, if you change only the domain membership of a server and not its computer name).

However, you should always perform this procedure to verify that the Settings page is configured appropriately for the server, and to change the Server's **Settings** page if necessary.

In this procedure, use Enterprise Manager to change the Server Name field on the server's Settings page (if necessary) so that it matches the new computer name for the server. (You specified the new computer name in the procedure [Change the Windows computer name/domain/workgroup membership on the server \(page 247\)](#).)

To change the server name in the server's Settings page:

1. Click **System Management > Enterprise > Settings**.
2. In the Installations tree (left pane), select the Server node for the computer whose name you have changed.
3. In the right-hand pane, in the **Server Name** field under the **Server Connection Details** section, replace the old computer name with the new computer name.
4. Under **Additional Settings**, if required, change the HTTP Alias.
5. Click **Save**.



You may see a message at the top of the Settings page indicating that it is necessary to restart services on the server. You do not have to restart the services at this time. You will restart the service in a later procedure.

What to do next

[Change the SQL server name on server role Settings screens \(page 255\)](#)

Change the SQL server name on server role Settings screens

Procedure 14 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this procedure only if you are changing the name of a computer running SQL Server. (You have changed the name of a computer running SQL Server if you completed the procedure described in [Run the SQL Server Change Computer Name application to rename an SQL Server \(page 248\)](#).)

If you have not changed the name of a computer running SQL Server, skip this procedure and continue to the next procedure, [Review the alarms and restart services \(page 257\)](#).

In this procedure, you must change the **SQL Server Host Address** field for every server role that accesses the computer running SQL Server whose name has changed.

All of the following server roles contain the **SQL Server Host Address** field and access a computer running SQL Server.

- Archive Database
- Biometrics Database
- Contact Database
- Contact OTLP Database
- DPA Database
- Framework Reports
- Framework Data Warehouse
- Framework Database
- Interaction Data Warehouse
- Interaction Reports
- QM Database
- Speech Analytics Database
- Speech Products Database
- Customer Feedback Survey

You must locate and examine the settings of the active server roles in your enterprise that are of the types listed above. For each server role that accesses computer running SQL Server whose name you have changed, you must change the SQL Server Host Address field. In that field, you must replace the old name of the computer running SQL Server with the new computer name.

Use the following procedure to change the SQL Server Host Address field for the server roles:

1. Click **System Management > Enterprise Management > Settings**.
2. Locate the server roles in your enterprise that are of the types listed above.
For example, in the Installations tree (left pane), expand each Server node to view the server roles that are active on the each of the servers. Identify each server role that is of a type listed above.
3. In the left-hand pane, select one of the active server roles listed above to display the server role's settings.
4. In the right-hand pane, in the **SQL Server Host Address** field, replace the old name of the computer running SQL Server with the new name of that computer.
5. Click **Save**.
6. Repeat these steps for every active server role listed above that exists in the enterprise and that specifies the old server name of the SQL server in the **SQL Server Host Address** field. All of these active server roles must specify the new computer name of the computer running SQL Server in the **SQL Server Host Address** field to connect to that SQL Server.

What to do next

[Update DPA with new Recorder server name \(page 257\)](#)

Update DPA with new Recorder server name

Procedure 15 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform this procedure only if you are changing the name of a recorder server that is integrated with (controlled by) Desktop and Process Analytics (DPA). Otherwise, skip this procedure and continue to [Review the alarms and restart services \(page 257\)](#).

In this procedure, you update DPA by deleting the entry associated with the old server name and import the server with its new name.

1. Click **Tracking > Desktop and Process Analytics**.
2. Select the **System** menu and then select **Recording**.
3. In the **IS Servers** tab, select the row that details the old recorder server, click **Edit** and then click **Delete**.
4. Click **Import IS Servers**.
5. From the list of recorder servers, select the recorder server that you have renamed.
6. If relevant, define a Class of Service and click **Save**.

What to do next

[Review the alarms and restart services \(page 257\)](#)

Review the alarms and restart services

Procedure 16 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



You must perform this procedure for every server you change.

Some of the changes that you have made in previous procedures may require services to be restarted on specific servers. In this case, alarms are raised in the Alarm Dashboard in Enterprise Manager.

In this procedure, you access the Alarm Dashboard in Enterprise Manager to review the active alarms and restart any services that are indicated by the alarms.

Also, if you stopped the Integration Server service in an earlier procedure, you must restart that service at this time, as noted below.

Follow this procedure to review the alarms and restart the services.

1. Perform this step if you stopped and disabled the Integration Server service in the procedure titled [Stop and disable the Integration Server Service \(page 241\)](#). Otherwise, skip this step and continue to step 2.

If you stopped and disabled the Integration Server service, you must restart that service now. There are some alarms that you cannot clear unless this service is restarted (these “Adapter Failure Message” alarms are noted in step 4 below).

If you used Watchdog to stop and disable the Integration Server service, use Watchdog to restart the service. From Watchdog, you can then click Startup in Watchdog to change the service Startup type from Disabled to Automatic.

If Watchdog is not running on the server, use the Services page available from the Windows Administrative Tools to restart the Integration Server service and change the service Startup type from Disabled to Automatic.

2. Click **System Monitoring > System Monitor > Alarm Dashboard**.
3. In the Installations tree (left pane), select the Server node for a server to which you have made any kind of change during this process (a name or domain change, a Settings page change, a server role change, etc). Then click **Filter** at the bottom of the left pane.
4. All of the active alarms for the selected server display in the **Enterprise Alarms** section on the right side of the page.
For each alarm displayed in the **Enterprise Alarms** section, do the following:
 - a. Click on the alarm.
 - b. Examine the **Details** section for the selected alarm. Look for information that indicates it is necessary to restart a service on any server in the enterprise.
 - c. Restart any services indicated by the alarm.



If you changed the name of the application server or a database server, also look for alarms indicating an Archive database connection failure occurred (for example an alarm named “Archive DB Error”). Restart the Recorder Archive service to resolve these alarms.

If you see “Adapter Failure Message” alarms triggered for the Integration Server in the Alarm Dashboard, you must do the following to clear these alarms:

- Click **Integration Management > Integration Servers > Integration Server**.
- Select the server on which the Integration Server service was restarted in step 1 of this procedure.
- Click **Edit Configuration**.
- Under **Integration Packages** (left pane), select the adapter indicated by the “Adapter Failure Message” alarms associated with the server.
- In the right pane, click the **Import Now** button. (This button usually appears in the top-half of the screen that shows the adapter status.)

5. Repeat steps 2 through 4 of this procedure for each server to which you have made any kind of change during this process.

What to do next

[Remove the old Integration Server name from BPMAINDB \(page 259\)](#)

Remove the old Integration Server name from BPMAINDB

Procedure 17 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.

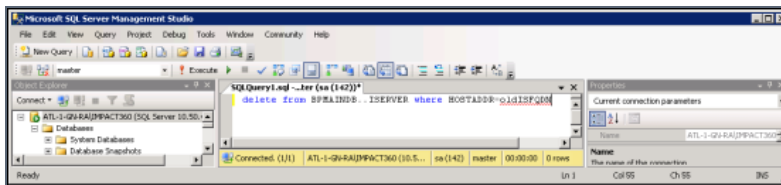
In this procedure, you use the Microsoft SQL Server Management Studio to remove the old name of the Integration Server from the BPMAINDB database.



Perform the steps in this procedure *only* if the server whose name or domain you are changing is an Integration Server.

Perform this procedure from the computer running SQL Server that hosts the BPMAINDB database.

1. Launch the Microsoft SQL Server Management Studio application. (For example, choose **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.**)
2. Click **New Query**.
3. In the query editor (right pane), enter the following command:
delete from BPMAINDB..ISERVER where HOSTADDR=oldISFQDN
where **oldISFQDN** is the old FQDN of the Integration Server.



4. Click **Execute**.
5. After the command executes, close the Microsoft SQL Server Management Studio.

What to do next

[Restart the IP Analyzer \(page 259\)](#)

Restart the IP Analyzer

Procedure 18 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure only if **both** of the following are true:

- You are changing the computer name or the domain membership of a server on which an IP Recorder or an IP Recorder Video server role is active.
- The IP Recorder or IP Recorder Video server role on the server you are changing is managed by an IP Analyzer server role.

If both of the above are **not** true, skip this procedure and continue to the next procedure [Change the configuration of any affected desktop applications \(page 260\)](#).

In this procedure, you use the Recorder Manager application on the IP Analyzer server to update the server name of the IP Recorder or IP Recorder Video server and then restart the Recorder Analyzer Service.

Follow the instructions below:

1. Select **System Management > Enterprise Management > Settings**.
2. In the Installations tree (left pane), select the Server node for the server that contains the active IP Analyzer server role. (This server contains the IP Analyzer server role that manages the IP Recorder or IP Recorder Video server role on the computer whose name or domain membership you are changing.)
3. Click **Launch** to launch the Recorder Manager application on the IP Analyzer server.
4. In Recorder Manager, select **General Setup > Call Control**.
5. In the left pane, select the Recorder Group to which the IP Recorder or IP Recorder Video server that is being change belongs.
6. In the right pane, the IP Addresses and Server Names are listed for all of the IP Recorders in the Recorder Group. Do the following:
 - a. Under the **Server** column, locate the old server name of the IP Recorder whose name or domain you have changed.
 - b. Change the server name to the new computer name of the IP Recorder or IP Recorder Video server.
7. Click **Save**.
8. From Recorder Manager, restart the **Recorder Analyzer Service**.
 - a. Select **Operations > Start and Stop**.
 - b. Select the **Recorder Analyzer Service**.
 - c. Click **Restart**.
9. Close the Recorder Manager.

What to do next

[Change the configuration of any affected desktop applications \(page 260\)](#)

Change the configuration of any affected desktop applications

Procedure 19 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure if you are changing the computer name or the domain membership of a server on which **one or more** of the following server roles are active:

- Recorder Integration Service server role
- Framework Applications server role

- Interactions Applications server role
- DPA Applications server role

If the server you are changing does not contain any of the server roles listed above, skip this procedure and continue to the next procedure, [Perform the steps to complete the changes for clustered Framework Application servers \(page 262\)](#).

Servers that contain any of the server roles listed above are accessed by applications that reside on the agent desktops.

These desktop applications include configuration settings that specify the host names of the server's that contain the server roles listed above. These configuration settings enable the desktop applications to connect to the server roles on which they rely.

If you are changing the server name or domain membership of a server that includes one or more of the server roles listed above, you must ensure that the desktop applications that access the server role are configured to use the new computer name of the server that contains the server role.

The procedures required to alter the configuration of the desktop applications to accommodate server name changes are discussed in the "Application Configuration Updates" section of the "System Administration for Desktop Applications" chapter of the *Desktop Applications Deployment Reference and Installations Guide*.

Perform the appropriate procedures described in the *Desktop Applications Deployment Reference and Installations Guide*.

What to do next

[Perform the steps to complete the changes for clustered Framework Application servers \(page 262\)](#)

Perform the steps to complete the changes for clustered Framework Application servers

Procedure 20 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure *only* if you have performed either of the procedures described in [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#).

If you did *not* perform either of the procedures described in [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#), skip this procedure and continue to [Determine what to do next \(page 265\)](#).

At this point, there are two possible procedures that you can perform to complete the changes for clustered Framework Applications servers. Review the descriptions of these procedures to determine which one(s) you need to perform.

- [Move the server from the Site Node back to the Cluster Node \(page 262\)](#) - In the procedure [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#), you might have been instructed to move one server out of the Cluster node and into the Site node that contains the Cluster node. If you have just completed the procedures to change the domain membership of the server that you moved to the Site node, perform the procedure described in [Move the server from the Site Node back to the Cluster Node \(page 262\)](#).
- [Add a deleted server back to the cluster \(page 263\)](#) - In the procedure [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#), you might have been instructed to delete (not move, but delete) one or more servers from the cluster. If you have just completed the procedures for renaming a server that was deleted from a cluster, perform the procedure described in [Add a deleted server back to the cluster \(page 263\)](#).

Move the server from the Site Node back to the Cluster Node

If you performed the procedure described in [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#), and you have just completed the procedure to change the name of the server that was moved from the Cluster node to the Site node, perform the procedure below.

In this procedure, you must move the changed server from the Site node back to the Cluster node, and reconnect it to the load balancer.

1. Click on **System Management > Enterprise > Settings**.
2. In the Installations tree (left pane), expand the Site node to which you moved the remaining server in the cluster.
3. Select the Server you moved from the Cluster node to the Site node when you performed the procedure [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#).
4. Select **More Actions > Move Installation**.
5. In the right-hand pane, select the Cluster node as the Target Installation.

6. Click **Move**.
7. Reconnect the server to the load balancer.

Add a deleted server back to the cluster

If you were instructed to delete a server from a cluster in the [Perform the prerequisite steps for clustered framework applications servers \(page 242\)](#), and you have just completed the procedure for changing the computer name or domain membership of the deleted server, perform the procedure below to add the deleted server back to the cluster.

Follow the instructions below:

1. Ensure that the server you are adding to the server cluster is **not** connected to the load balancing device that distributes connections to the server cluster.
2. Click on **System Management > Enterprise > Settings**.
3. In the Installations tree (left pane), select the Server Cluster node.
4. Select **Create Installations**.
5. Complete the fields in the Server page.
In the **Server Name** field under the **Server Connection Details** section, be sure to enter the new computer name of the server.
6. Click **Save**.
7. After you add the server to the Server Cluster node, a Pending Messages icon (asterisk) appears at the top of the page while Enterprise Manager processes the configuration change.
8. Wait for the Pending Messages icon to disappear before continuing to the next step. It may take a few minutes for the icon to disappear.
9. On the newly added server, restart these services (in the order shown) from the Windows Services dialog:
 - Impact Configuration and Monitoring Service
 - Impact System Monitoring Agent
 - WFO_ProductionDomain_ProductionServer
10. Verify the cache is set up correctly and the cluster is functioning.
You can perform the following check to verify that the cache is set up correctly and the cluster is functioning:
 - a. Click **System Management > General Settings > Cache**.
 - b. In the **Cache Viewer** page, all of the servers in the cluster should be listed under the **Host** and the **ServerNamefromDB** columns. For each server, the page should indicate that the **Cache is Clustered** and the server is **Synchronized**.
 - c. Connect the newly-added server to the load balancing device.

What to do next

[Restart Recorder services from Recorder Manager \(page 264\)](#)

Restart Recorder services from Recorder Manager

Procedure 21 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure only if you are changing the name of a Recorder server or a Consolidated server.

If you are not changing the name of a Recorder server or a Consolidated server, skip this procedure and continue to the next procedure [Review alarms and restart services](#) (page 264).

In this procedure, you access the Recorder Manager application on the Recorder or Consolidated server whose name you are changing, and restart all recording services.

1. Select **System Management > Enterprise Management > Settings**.
2. In the Installations tree (left pane), select the Server node for the Recorder or Consolidated server whose name you are changing.
3. Click **Launch** to launch the Recorder Manager application on that server.
4. In Recorder Manager, select **Operations > Start and Stop**.
5. Restart all of the recording-related services (shown below). To ensure minimal disruption to any recording that is currently occurring, restart these services one at a time.

Component Name	Status	Startup Type
Recorder Agent Service	Started	Automatic
Recorder Alarm Service	Started	Automatic
Recorder Archiver Service	Started	Automatic
Recorder Compressor Service	Started	Automatic
Recorder Consolidator Service	Started	Automatic
Recorder Content Server	Started	Automatic
Recorder DiskManager Service	Started	Automatic
Recorder Integration Service	Started	Automatic
Recorder IP CaptureEngine	Stopped	Automatic
Recorder Redundancy Controller	Started	Automatic
Recorder Screen CaptureEngine	Started	Automatic
RecorderTomcat(Restart Only)	Started	Automatic
Recorder Workflow Service	Started	Automatic

Select All Select None Edit Start Stop Restart Reboot

6. When you have restarted all of the recording-related services, close the Recorder Manager application.

What to do next

[Review alarms and restart services](#) (page 264)

Review alarms and restart services

Procedure 22 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.



Perform the steps in this procedure only if you are changing the name of a Recorder server or a Consolidated server.

If you are not changing the name of a Recorder server or a Consolidated server, skip this procedure and continue to the next procedure [Determine what to do next](#) (page 265).

1. Click **System Monitoring > System Monitor > Alarm Dashboard**.
2. In the Installations tree (left pane), select the Server node for a server to which you have made any kind of change during this process (for example, a name or domain change, a Settings page change, or a server role change). Then click **Filter** at the bottom of the left pane.
3. All of the active alarms for the selected server display in the **Enterprise Alarms** section on the right side of the page. For each alarm displayed in the **Enterprise Alarms** section, do the following:
 - a. Click on the alarm.
 - b. Examine the **Details** section for the selected alarm. Look for information that indicates it is necessary to restart a service on any server in the enterprise.
 - c. Restart any services indicated by the alarm.

What to do next

[Determine what to do next \(page 265\)](#)

Determine what to do next

Procedure 23 of 23 associated with Step 2 - Change the Computer Name, Domain, or Workgroup of an Individual Managed server.

At this point, you have completed every procedure associated with changing the computer name, domain membership, or workgroup membership of one managed server.

The procedure below describes what to do next:

1. If you are changing the computer name or the domain or workgroup membership of more than one computer, repeat the steps described in [Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#) to change another computer.

When changing multiple servers, change the servers in the order described in [Changing multiple servers \(page 239\)](#).

If the last server you changed was a member of a server cluster, repeat the Step 2 procedures for each of the other servers in the server cluster before continuing on to change any of the non-clustered servers.

Continue repeating Step 2 until you have changed all of the computers you want to change.

2. After you have repeated the Step 2 procedures to change every server you want to change, use the table below to determine what to do next:

If your servers are in a:	Follow these instructions:
Workgroup	You are finished. You do not need to perform the procedures described in Step 3 of this chapter.

If your servers are in a:	Follow these instructions:
Domain	1. If you are not changing the domain membership of any servers, you are finished. You do not need to perform the procedures described in Step 3 of this chapter. 2. If you are changing the domain membership of some, but not all, of the servers, you are finished. You do not need to perform the procedures described in Step 3 of this chapter. 3. If you are changing the domain membership of every server in your environment, continue to Step 3: Break the trust between the original domain and the new domain (page 267).

Step 3: Break the trust between the original domain and the new domain

Step 3 is the last of three steps associated with changing the computer name or domain membership of all of the managed servers in your enterprise.



Perform the procedures in this step only if you have moved **all** of the servers in your environment onto a new Windows domain, as illustrated on the [Computer name and domain change workflow \(page 235\)](#).

Before performing the step 3 procedures

Before performing the Step 3 procedures, you must have completed the following prerequisite steps:

- [Step 1: Establish trust between the current domain and the target domain \(page 237\)](#).
- [Step 2: Change the computer name, domain, or workgroup of an individual server \(page 239\)](#).

You *must* have performed the procedures in Step 2 on **all** of the servers in your enterprise. All of the servers in your enterprise must be moved to the new domain before you perform the procedures in Step 3 to break the trust between the original domain and the new domain.

At this point in the domain change process, the trust relationship still exists between the original domain and the new domain to which you have moved all of your servers.

The Step 3 procedures explain all of the procedures you must perform if you intend to break the trust between the original domain and the new domain. It is not always mandatory to perform the Step 3 procedures, as noted below:

- If for any reason you expect the old domain to remain in operation, it is not mandatory to perform the Step 3 procedures. As long as the trust relationship remains in place, the servers you have moved to the new domain will continue to function properly even if you do not perform the procedures in Step 3.
- If, however, you intend to discontinue the use of the old domain and discard it, it is mandatory that you perform the Step 3 procedures.

Step 3 procedures

If you intend to break the trust between the original domain and the new domain, you must perform the procedures below before you break this trust.

1. [Configure the required accounts in the new Windows domain \(page 268\)](#)
2. [Complete the SSO configuration for servers in the new domain \(page 275\)](#)
3. [Break the trust between the original domain and the new domain \(page 277\)](#)

Step-by-step instructions for each of these procedures are provided in the following sections.

Configure the required accounts in the new Windows domain

Procedure 1 of 3 associated with breaking the trust between the original domain and the new domain.

When you move servers to a new Windows domain, you must create five accounts that are required in the new domain.

In this procedure, you do the following:

- Create the five required Windows accounts
- Perform additional configurations to ensure that the Management Service Account and the Database Management Account function properly in the new domain.

The steps in this procedure include:

1. [Create the five required Windows accounts \(page 268\)](#)
2. [Complete the changes for the new MSA and DMSA accounts \(page 269\)](#)

Create the five required Windows accounts

Step 1 of 2 associated with the procedure to configure the required accounts in the new Windows domain.

To complete this step, you must create five accounts in the new Windows domain.



Each account must be assigned the same access rights in the new domain that it had in the old domain.

See the *Technology, Security, & Network Integration Deployment Reference Guide* for details about creating each of the five accounts, and the access rights associated with them.

The accounts you must create in the new domain include:

- Installation service account
- Maintenance service account
- SQL services account
- Management Service Account (MSA)
- Database Management Service Account (DMSA) - This is an **optional** account that is not used by all enterprises.

If a DMSA was not configured in the old domain (that is, your enterprise does not use a DMSA), note the following:

- The MSA account acts as the DMSA. In this case, ensure that the MSA in the new domain is granted all privileges required by the DMSA.
- You enter the MSA credentials in any field that requests DMSA credentials, as noted in this document.

What to do next

[Complete the changes for the new MSA and DMSA accounts \(page 269\).](#)

Complete the changes for the new MSA and DMSA accounts

Step 2 of 2 associated with the procedure to configure the required accounts in the new Windows domain.

Perform these sub-procedures in the order listed. Step-by-step instructions for each sub-procedure are provided below.

Procedure**1. Verify that no services are failing**

Sub-procedure 1 of 8 associated with completing the changes for the new MSA and DMSA accounts.

In this procedure, you must verify that the Watchdog application is not repeatedly restarting failing services. This procedure requires you to turn off the Watchdog application temporarily on every managed server in the enterprise.

You must perform this procedure on every managed server in the enterprise.

1. From the Windows desktop on a managed server, use the System Tools to turn off the Watchdog application.
2. Verify that none of the services monitored by the Watchdog application are failing. If any services are failing, you must correct the problem causing the services to fail.
3. When you are sure that none of the services monitored by the Watchdog application are failing, use the System Tools to restart the Watchdog application.
4. Repeat steps 1 through 3 on every server in the enterprise.

2. Resolve any active alarms

Sub-procedure 2 of 8 associated with completing the changes for the new MSA and DMSA accounts.

Before using Enterprise Manager to specify the change the Management Services Account and Database Management Account, you must resolve any active alarms in the enterprise.



If your environment includes a single server that hosts the Import Manager application and an active IP Recorder server role or IP Recorder Video role, changing the MSA account can cause this server to falsely trigger an alarm named "Disk Manager Detected Unarchived Files" (alarm number 39004).

If you see this alarm raised by such a server in the Alarm Dashboard, you can acknowledge the alarm without performing the corrective action for the alarm. The alarm is triggered falsely and the conditions that normally cause the alarm do not exist.

Procedure

1. Click **System Monitoring > System Monitor > Alarm Dashboard**.
2. In the **Installations** tree (left pane), select the **Enterprise** node, and then click **Filter** at the bottom of the pane.
3. All of the active alarms on all servers in the enterprise display in the **Enterprise Alarms** section on the right side of the page.
For each alarm displayed in the Enterprise Alarms section, do the following:
 - a. Click on the alarm.
 - b. In the **Details** section, review the corrective action for the selected alarm.
 - c. Perform the corrective action for the alarm.
4. After you have performed the corrective actions for all of the alarms, acknowledge all of the alarms.
 - a. In the **Alarm Dashboard**, click the **Servers** page (next to the **Instances** page).
 - b. Click the icon under the **Acknowledge** column to acknowledge each alarm.
 - c. Click **Yes** when prompted to acknowledge the alarm.
5. Allow the system to stabilize by ensuring that all of the corrective actions you have performed have resolved all of the conditions that were causing the alarms. Do not continue to the next sub-procedure until you feel certain that none of the alarms will recur.

3. Assign database permissions

Sub-procedure 3 of 8 associated with completing the changes for the new MSA and DMSA accounts.

In this procedure, you run the Database Permissions Configuration Tool to automatically assign the new Management Service Account (MSA) and the new Database Management Account (DMSA) with the required database permissions.

To complete this procedure, you must complete these three tasks:

Ensure you have the administrative privileges Required to run the database configuration tool

You can run the Database Permissions Configuration Tool from any server on which a database platform is installed.

In this procedure, do the following:

- Identify the database platform server from which you will run the Database Permissions Configuration Tool.

To verify the tool is present on the server, look for this directory: **[Software Directory]/CommonDB/Utils/Database Permissions Configuration Tool**.

- Verify that you are defined as the following on the server from which you will run the Database Permissions Configuration Tool:

- A local Windows administrator on the server on which the tool resides
- A member of the SQL SysAdmin server role on each computer running an SQL Server

Verify Windows PowerShell functionality

Perform this procedure on the server from which you will run the Database Permissions Configuration Tool.

Verify that the PowerShell execution policy on the server is Unrestricted.

1. On the computer running SQL Server, run **Start > Windows PowerShell**.
2. In the Administrator: Windows PowerShell console, run the **Get-ExecutionPolicy** command.

If the result is:

- **Unrestricted:** Servers with the Unrestricted, RemoteSigned, or AllSigned PowerShell functionality can run the PowerShell setup file (Setup_signed.ps1).
- **Restricted:** Enable the machine for restricted functionality and then use the PowerShell setup file, as follows:
 - a. In the console, run the **Set-ExecutionPolicy AllSigned** command.
 - b. Enter **Y** to confirm the change.

Use the **Setup_signed.ps1** when running the tool.

Run the Database Permissions Configuration Tool

Run the Database Permissions Configuration Tool once for each computer in the enterprise that runs an SQL Server. Update the server name and port for each instance.

1. From the **Database Permissions Configuration Tool** folder run the relevant setup file.
2. If prompted, confirm that you trust the publisher, enter [A] Always run or [R] run once.
3. Enter the Details of the the computer running SQL Server:
 - **SQL Server Name:** The host name or IP address of the computer running SQL Server.
 - **Port:** The SQL Server listening port. The default port is 1433.
4. Enter the Login Details of the computer running SQL Server:

Parameter	Description
Database Management Account Name	Enter the user name of the Windows domain account used as the Database Management Account (DMSA). Note: If your enterprise does not use the DMSA, enter the user name of the MSA.
Database Management Password Name	Enter the password of the Windows domain account used as the Database Management Account. Note: If your enterprise does not use the DMSA, enter the password of the MSA.

Parameter	Description
Management Service Account Name	Enter the user name of the Windows domain account used as the Management Service Account.
Management Service Account Password	Enter the password of the Windows domain account used as the Management Service Account.

5. Click **Apply**. When the confirmation message appears, click **Yes**.
6. A permissions validation message appears if the SQL public server role does not have the execute permission. Click **Details** to troubleshoot relevant scripts and refer to the SQL public server role permissions table.
7. **Result:** When the database permissions are all successfully assigned to the service accounts, the success message **All database permission scripts ran successfully** appears.
If the success message does not appear at the end of the text box, scroll through the SQL Server scripts the tool ran and search for Status: Failed. Troubleshoot the stored procedure script above this status. If not, scroll through the logs displayed to review which database permission was denied or failed.
8. For multiple instances of computers running SQL Server, run the tool again for each instance from the same machine by changing the **SQL Server Name** and **Port** to the server name hosting the next instance.

4. Change the Management Services account and Database Management account in Enterprise Manager

Sub-procedure 4 of 8 associated with completing the changes for the new MSA and DMSA accounts.

In this procedure, you use Enterprise Manager to specify the new Management Services Account and Database Management Account in the Enterprise Settings page.

Follow the steps below:

1. Select **System Management > Enterprise Management > Settings**.
2. In the Installations tree (left-hand pane), select the Enterprise node.
3. Select the **Enterprise Settings** page.
4. Under the **Access** section, change the following settings:
 - **Management Service Account Username** - Enter the username associated with the new Management Service Account you created earlier in Step 1.
 - **Management Service Account Password** - Enter the password associated with the new Management Service Account you created earlier in Step 1.
 - **Database Management Account Username** - Enter the username associated with the new Database Management Account you created earlier in Step 2. If the enterprise does not use this account, enter the username associated with the MSA.
 - **Database Management Account Password** - Enter the password associated with the new Database Management Account you created earlier in Step 2. If the enterprise does not use this account, enter the password associated with the MSA.
5. Click **Save**.

5. Change the SSRS Service User

Sub-procedure 5 of 8 associated with completing the changes for the new MSA and DMSA accounts.

In this step, you do specify the new MSA account as the account that runs the report server service and the account used to connect to the Reporting Services database.

Perform this procedure from the server that hosts the Reporting Services server role.

Procedure

1. Launch the **Reporting Services Configuration Manager**.
(Usually located at **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools**.)
2. In the **Reporting Services Configuration Connection** window:
 - a. Ensure that the **Server Name** and **Report Server Instance** fields specify the values appropriate for the computer running SQL Server that hosts the Reporting Services database.
 - b. Click **Connect**.
3. In the left-pane, select **Service Account**.
4. Select **Use another account**.
 - In the **Account (Domain\user)** field, enter the domain\username of the MSA account.
 - In the **Password** field, enter the password of the MSA account.
5. Click **Apply**.
6. In the **SQL Server Connection Dialog**, you must specify the credentials of an account that has permission to access the Reporting Services database. The MSA account has this permission. Complete the fields as noted below:
 - **Server Name**: - Specify the name of the computer running SQL Server that hosts the Reporting Services server role.
 - **Credentials Type** - Select one of the following from the drop-down box.
 - **Current User - Integrated Security** - Select this option if you are currently logged into Windows using an administrator account that has the permission to access the Reporting Services database. If you select this option, you do not need to enter a user name and password.
 - **SQL Server Account** - Select this option to specify the credentials of an account that has permission to access the Reporting Services database. If you select this option, enter the username and password for this account in the fields provided.
7. Click **OK**.

6. Save the Reporting Services server role settings

Sub-procedure 6 of 8 associated with completing the changes for the new MSA and DMSA accounts.

In this step, you save the Reporting Services server role settings. This step ensures that SSRS will be redeployed after you break the trust with the old domain.

Perform this procedure from the server that hosts the Reporting Services server role.

Procedure

1. Select **System Management > Enterprise Management > Settings**.
2. In the Installations tree (left-hand pane):
 1. Expand the Server node that hosts the **Reporting Services** server role.
 2. Click in the **Reporting Services** server role node.
3. Click **Save**.

7. Review the alarms again and restart any services indicated

Sub-procedure 7 of 8 associated with completing the changes for the new MSA and DMSA accounts.

The changes you have made in previous sub-procedures will trigger alarms that indicate it is necessary to restart particular services.

In this procedure, repeat the procedure discussed in [2. Resolve any active alarms \(page 269\)](#). Resolve the new alarms that were raised by restarting the services indicated by the alarms.

8. Verify the SQL Services are running under the new accounts

Sub-procedure 8 of 8 associated with completing the changes for the new MSA and DMSA accounts.

In this procedure, verify that the SQL services are running under the new MSA and DMSA (if applicable) accounts that you have created in the new domain.

You can verify the accounts under which the SQL services are running from the Windows Services window (select Start > Administrative Tools > Services from the Windows desktop).

What to do next

[Complete the SSO configuration for servers in the new domain \(page 275\)](#)

Complete the SSO configuration for servers in the new domain

Procedure 2 of 3 associated with breaking the trust between the original domain and the new domain.



Perform this procedure only if SSO was implemented on the servers you have moved into the new domain.

If SSO was not implemented on the servers you have moved into the new domain, skip this procedure and continue to [Break the trust between the original domain and the new domain \(page 277\)](#).

The steps required to configure SSO for servers in the new domain include:

1. [Create the Windows accounts required by WebLogic and SSO \(page 275\)](#)
2. [Run the Weblogic Configuration Tool for SSO configuration \(page 275\)](#)
3. [Change user names to reflect the new domain \(page 276\)](#)

Create the Windows accounts required by WebLogic and SSO

Step 1 of 3 associated with completing the SSO configuration for servers in the new domain.

In this procedure you must create Windows accounts in the new domain that are required by the WebLogic server and to support Single Sign-On (SSO).

You must create the following Windows accounts in the new domain:

- **WebLogic Admin Account**
- **SSOBind account:** this account is required only for SSO configuration, and it requires a new Kerberos SPN.
- **Firstuser Account (also called System Account)** - a user account used to administer the application.

What to do next

[Run the Weblogic Configuration Tool for SSO configuration \(page 275\)](#)

Related information

Windows Active Directory (LDAP/SSO) (*Authentication Configuration Guide*)

Run the Weblogic Configuration Tool for SSO configuration

Step 2 of 3 associated with completing the SSO configuration for servers in the new domain.

To complete this procedure, you must run the SSO wizard to reconfigure SSO for the servers in the new domain.

What to do next

[Change user names to reflect the new domain \(page 276\)](#)

Related information

Configure WebLogic settings (*Authentication Configuration Guide*)

Change user names to reflect the new domain

Step 3 of 3 associated with completing the SSO configuration for servers in the new domain.



Perform this procedure only if the User Principal Name (UPN) of the users is entered as the User Name for any users at **User Management > Security > User Logins**.

If the UPN is not entered as the User Name for any user at **User Management > Security > User Logins**, skip this step and continue to [Break the trust between the original domain and the new domain \(page 277\)](#).

If a UPN is entered as the User Name for any users at User Management > Security > User Logins, you must do the following to ensure the User Names specify the UPN that is appropriate for the new domain:

- Export the all user profiles to a single text file.
- Use a text editor to manually alter the user names in the text file so that each user name reflects the new UPN of the user.
- Import the text file containing the altered user profiles.

Follow the instructions below:

1. To determine whether the UPN is entered as the username for a user, do the following:
 - a. Select **User Management > Security > User Logins**.
 - b. At the bottom of the **Name** (left-hand) pane, click **Select All** and then click **View**.
 - c. Examine the name that appears in the **User Name** field.
 - If the **User Name** fields specify the UPNs of the users, perform the remaining steps in this procedure.
 - If the **User Name** fields do not specify the UPNs of the users, you do not need to perform the remaining steps in this procedure. Skip to [Break the trust between the original domain and the new domain \(page 277\)](#)
2. Select **User Management > Employees > Profiles**.
3. At the bottom of the **Name** (left-hand) pane, click **Select All** and then click **View**.
4. Click **Export**.
5. When prompted with **Do you want to open or save this file?**, click **Save**. Provide the file with a unique name and save it to a convenient directory on your hard drive.
6. When prompted with **Download Complete**, click **Open** to open the file you have just saved. The file opens in Notepad.
7. In the file, do the following:

- a. Select the existing User Name (the user's UPN) of the first user listed in the file.
- b. Manually replace the existing User Name. To do this, delete the existing User Name and type in the UPN that is appropriate for the user in the new domain. Do not alter any other values in the user's profile listing.
- c. Click **File > Save** to save the file.
- d. Repeat steps a through c to change the User Name of every user in the file.
- e. Click **File > Exit** to exit Notepad.
8. From the **User Management > Employees > Profiles** page, click **Import**.
9. For the **Mode:** option, select **Update**.
10. In the **File to import:** option, browse to and select the text file you altered in step 7.
11. In the **Check the fields to import and enter the column number from your file:** section, select **User Name**.
12. Click **Save** to import the user profiles containing all of the changed User Names.



If you receive an error message that says "Record number 1: Employee Internal ID could not be updated as the employee with the given ID could not be found, do the following:

Enter the value of **1** in the **Number of lines to ignore at start of file:** option and repeat steps 9 through 12.

What to do next

[Break the trust between the original domain and the new domain \(page 277\)](#)

Break the trust between the original domain and the new domain

Procedure 3 of 3 associated with breaking the trust between the original domain and the new domain.

At this point, you have completed all of the procedures necessary for the servers to function correctly in the new domain without relying on the trust relationship with the original domain.

In this procedure, you sever the trust relationship between the original domain and the new domain.

For the specific procedures required to sever the trust relationship between the original domain and the new domain, see the Microsoft MSDN web site, or consult with your Windows network administrator.

After you break the trust between the two domains, all of your servers will continue to operate successfully in the new domain.

Changing ports

You may need to change the ports through which the WebLogic or Tomcat communicates.

Topics

Change the Tomcat Server Ports	279
Change WebLogic port to a port other than 7001	283

Change the Tomcat Server Ports

Tomcat HTTP servers reside on each server in the enterprise. The Tomcat servers that reside on a given server depend on the platform of the server. Use the instructions in this section to change the ports on which the Tomcat servers listen for connections.

The table below lists Tomcat servers and shows the default SHUTDOWN and HTTP ports on which each Tomcat server listens for connections.

Tomcat Server	Default SHUTDOWN Port:	Default HTTP Port:
CF Tomcat	29282	29280
Recorder Tomcat	8005/29306 (from 15.2 Security Kit 2 onward, the port is 29306)	8080
Speech Tomcat	29173	29171
TRS Tomcat	29302	29303
Miner Tomcat	8006	29174

The procedure below lists the steps you must perform to change the ports on which a Tomcat server listens for connections.

Procedure

1. Open the appropriate server.xml file

Procedure 1 of 5 required to change the ports on which a Tomcat server listens for connections.

1. On the server that hosts the Tomcat server, open Notepad (or a similar text editor).
2. From Notepad, open the **server.xml** file for the Tomcat server whose ports you want to change. The table below shows the directory where the **server.xml** file for each Tomcat server resides:

Tomcat Server	Location of server.xml file
CF Tomcat	<installdir>\Software\CFTomcat64\conf
Recorder Tomcat	<installdir>\Software\Tomcat\conf
Speech Tomcat	<installdir>\Software\SpeechCattomcat64\conf
TRS Tomcat	<installdir>\Software\TrsTomcat64\conf
Miner Tomcat	<installdir>\Software\Tomcat Miner\conf\server.xml

2. Edit the port settings in the server.xml file

Procedure 2 of 5 required to change the ports on which a Tomcat server listens for connections.

Attributes in the server.xml file specify the port numbers on which the Tomcat server listens for connections.

In this procedure, search the server.xml file for the existing port number(s) you want to change, and replace each instance of the existing port number with the new port number.

1. Use the Find/Replace feature of Notepad (or similar text editor) to find and replace each instance of the port number you want to change in the server.xml file.

Examples include:

- If you are changing the default HTTP port of the CF Tomcat server from 29280 to 12345, find each instance of 29280 in the server.xml file and replace it with 12345.
 - If you are changing the default HTTP port of the Recorder Tomcat server from 8080 to 8085, find each instance of 8080 in the server.xml file and replace it with 8085.
 - If you are changing the default SHUTDOWN port of the CF Tomcat server from 29282 to 12347, find each instance of 29282 in the server.xml file and replace it with 12347.
2. When you have changed each port number you want to change, save and close the server.xml file.

3. Change the port settings in the Windows Registry

Procedure 3 of 5 required to change the ports on which a Tomcat server listens for connections.

In this procedure, you must change the port settings in the Windows Registry key that is associated with the Tomcat server whose ports you are changing.

1. On the server that hosts the Tomcat server, open the Windows Registry Editor.
 - a. From the Windows desktop, select **Start > Run**.
 - b. In the **Run** window text box, type **regedit** and click **OK**.
2. In the Registry Editor, navigate to the registry key that is associated with the Tomcat server whose ports you are changing. The table below shows the location of each of these registry keys:

Tomcat Server	Registry key location:
CF Tomcat	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AvayaAura\CFTomcat64
Recorder Tomcat	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AvayaAura\RecorderTomcat
Speech Tomcat	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AvayaAura\SpeechCatTomcat64
TRS Tomcat	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AvayaAura\TrsTomcat64
Miner Tomcat	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Impact360\MinerTomcat

3. In the registry key, change these values as appropriate:
 - **HttpPort** - If you changed the HTTP port in the server.xml file, enter the new HTTP port number for this value.
 - **ShutDownPort** - If you changed the SHUTDOWN port in the server.xml file, enter the new HTTP port number for this value.
4. Close the Registry Editor.

4. Restart the appropriate Windows service

Procedure 4 of 5 required to change the ports on which a Tomcat server listens for connections. In this procedure, restart the Windows server associated with the Tomcat server whose ports you have changed.

1. From the Windows desktop of the server that hosts the Tomcat server, select **Start > Administrative Tools > Services**.
2. In the **Services** window, right-click on the service associated with the Tomcat server whose ports you have changed, and select **Restart**. Use the table below to determine the service associated with each Tomcat server.

For this Tomcat Server:	Restart this Windows service:
CF Tomcat	I360 CF Tomcat
Recorder Tomcat	Recorder Tomcat
Speech Tomcat	I360 Speech Categorization Tomcat
TRS Tomcat	I360 Transcription Repository Service Tomcat
Miner Tomcat	Miner Tomcat

5. Run the ConfigureGateway.exe file as the Windows administrator

Procedure 5 of 5 required to change the ports on which a Tomcat server listens for connections.

In this procedure, you run the ConfigureGateway.exe file as the Windows administrator.

This procedure enables the Secure Gateway proxy on the server to detect the port number changes.

1. On the server hosting the Tomcat server, open the Command Prompt using the Run as administrator option:
 1. From the Windows desktop, click **Start**.
 2. Right-click on the **Command Prompt** option and select **Run as administrator**.
 3. Log in to the Command Prompt using the name and password of the Windows administrator account on the server
2. From the Command Prompt, run the **ConfigureGateway.exe** file in the **<installdir>\Software\SecureGateway** directory.
 1. In the Command Prompt window, use the cd command to change to this directory:
<installdir>\Software\SecureGateway

At the Command Prompt, type **ConfigureGateway.exe** and press **Enter**.

Change WebLogic port to a port other than 7001



This procedure should only be performed by an authorized services and support representative. Contact an authorized services and support representative if you want to change the WebLogic port to a port other than 7001. This procedure requires use of an Advanced mode that is available only to authorized services and support representatives.

To successfully change WebLogic, complete the following procedures in the following order:

1. [Adjust the Framework Applications Server Settings \(page 283\)](#)
2. [Adjust system properties \(page 286\)](#)
3. [Change the WebLogic server listening port \(page 284\)](#)
4. [Verify successful change to WebLogic ports \(page 286\)](#)

Adjust the Framework Applications Server Settings

1. Log on to the Suite's web application using the system administrator user name and password. These were established during installation.
2. Navigate to **System Management > Enterprise > Settings**.
3. From the left panel, select the **Enterprise** level, and then select **More Actions**.
4. From the **More Actions** menu, select **Turn Advanced Mode On**.
5. On the left panel, select the application server, then expand the list of server roles and select **Framework Applications**.
6. In the right pane under **Server Ports**, in the **Port** field, type the new port number.
7. Click **Save**.

Enterprise Manager distributes the change. If the distribution is successful, the **Service Restart Request** alarm is raised for the Framework Applications role. In clustered environments, each individual node has an alarm.

Before restarting the service, complete the next procedure, [Adjust system properties \(page 286\)](#).

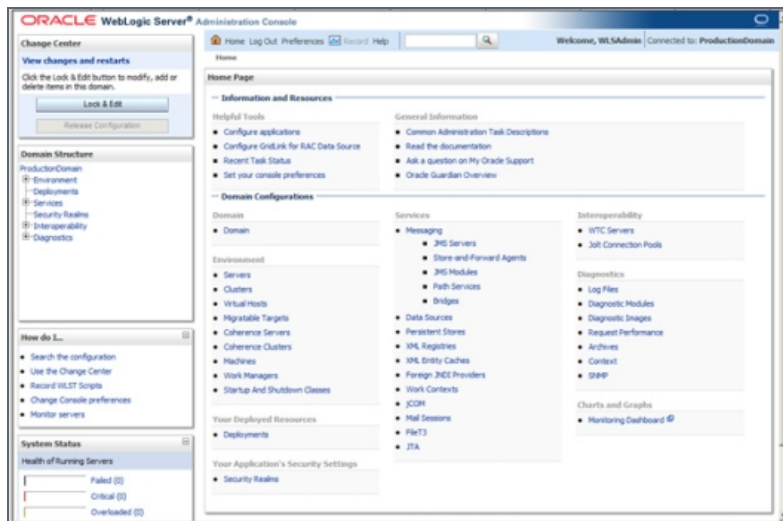
Change the WebLogic server listening port

1. Navigate to the WebLogic Server Console URL, **http(s)://<ServerName>:<current port number>/console**.

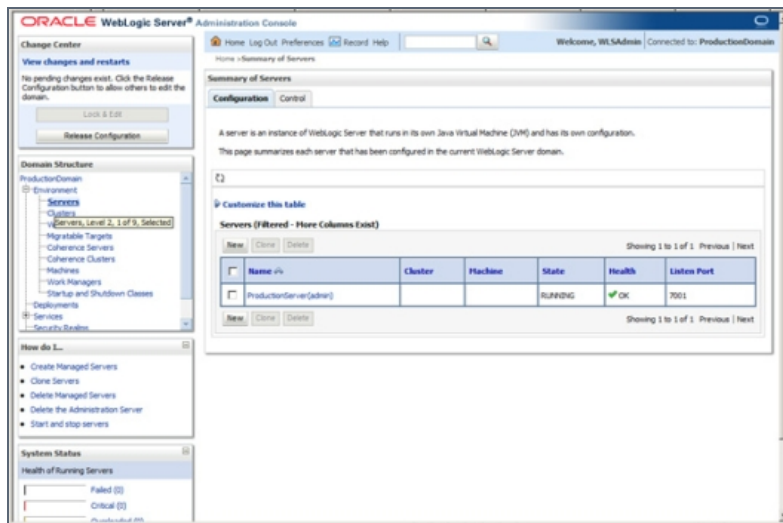


2. Log on using your administration account, such as **WLSAdmin** and password. Note that the user name is case sensitive.

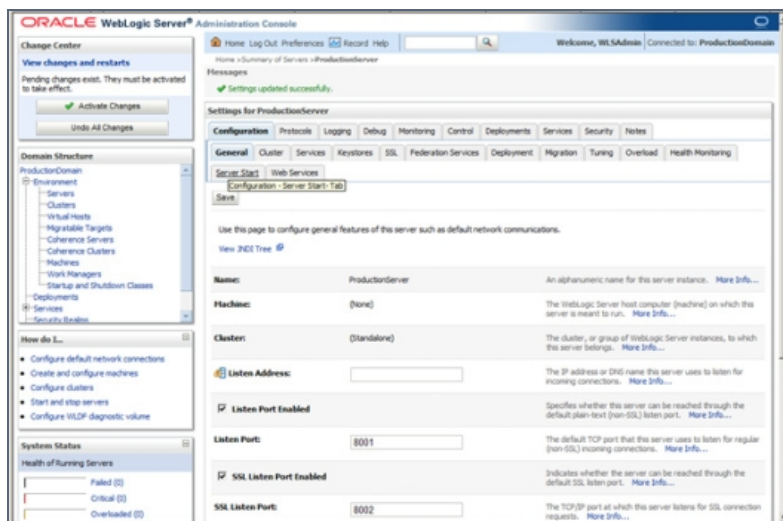
The **Oracle WebLogic Server Administration Console** opens.



3. On the left panel, click **Lock & Edit** and, on the right panel, in the **Environment** area, click **Servers**. The page refreshes, and on the right panel, in the **Customize this table** area, a table displays showing **ProductionServer(admin)** under the **Name** column.



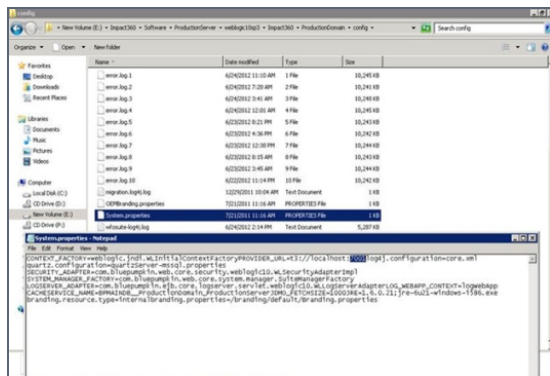
4. In the table, click **ProductionServer(admin)**.
The page refreshes, and on the right panel, the **Settings for ProductionServer** area displays, including a set of tabs.
5. On the right panel, click the **Configuration > General** page.



6. Change the value in the **Listen Port** field.
Values must match the value you set for the port earlier in this procedure.
7. Click **Save**.
8. Near the top of the left panel, click **Activate Changes**.
The WebLogic server immediately starts listening at the new ports you specified.
You may be forced to log out from the WebLogic administration console at this point, which is normal.
9. Restart **WFO service** on the application server.

Adjust system properties

1. Navigate to the file **%VERINT_WEBLOGIC_DOMAIN_HOME%\config\System.properties** and open it with a text editor, such as Notepad.



2. In the file, edit the **PROVIDER_URL=t3://localhost:** value with the new port number.
3. Restart the **WFO_ProductionDomain_ProductionServer** service to complete the update process.



In a clustered deployment, this step needs to be repeated for each server.

Verify successful change to WebLogic ports

Verify that the WebLogic Server, Enterprise Manager, and Framework Applications function correctly with the new port values, and that there are no outstanding alarms related to changing the ports.

Disabling TCP/IP and IP monitoring services

Windows Simple TCP/IP and IP monitoring services can be vulnerable. Step-by-step instructions are provided for customers who want to disable these services. Instructions are also provided to re-enable the services after they have been disabled.

Topics

Disable TCP/IP and IP Monitoring services workflow	288
Rollback the configuration changes workflow	293

Disable TCP/IP and IP Monitoring services workflow

Follow this workflow to disable TCP/IP and IP monitoring services.

Workflow

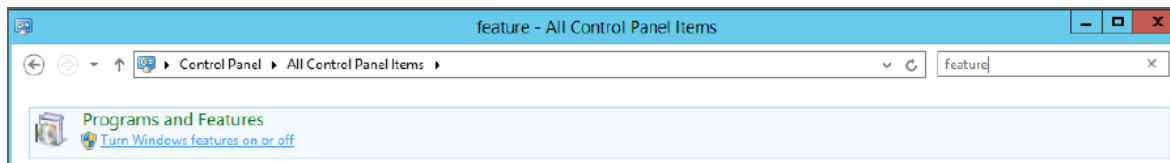
1. [Disable Windows TCP/IP services \(page 288\)](#)
Disable the Windows TCP/IP services from the Windows Control Panel on each application server in the application server cluster.
2. [Disable the Monitoring services \(page 290\)](#)
To disable the Monitoring services, update the **tangosol-coherence.xml** file on all application servers in the application server cluster.
3. [Restart application servers after disabling services \(page 291\)](#)
Restart all application servers in the application server cluster.
4. [Confirm the TCP/IP service is disabled \(page 291\)](#)
Verify that the TCP/IP service is disabled by accessing the coherence logs.
5. [Sanity tests after disabling services \(page 292\)](#)
Perform three tests to verify that the coherence cache is working after making the configuration changes described so far.

Disable Windows TCP/IP services

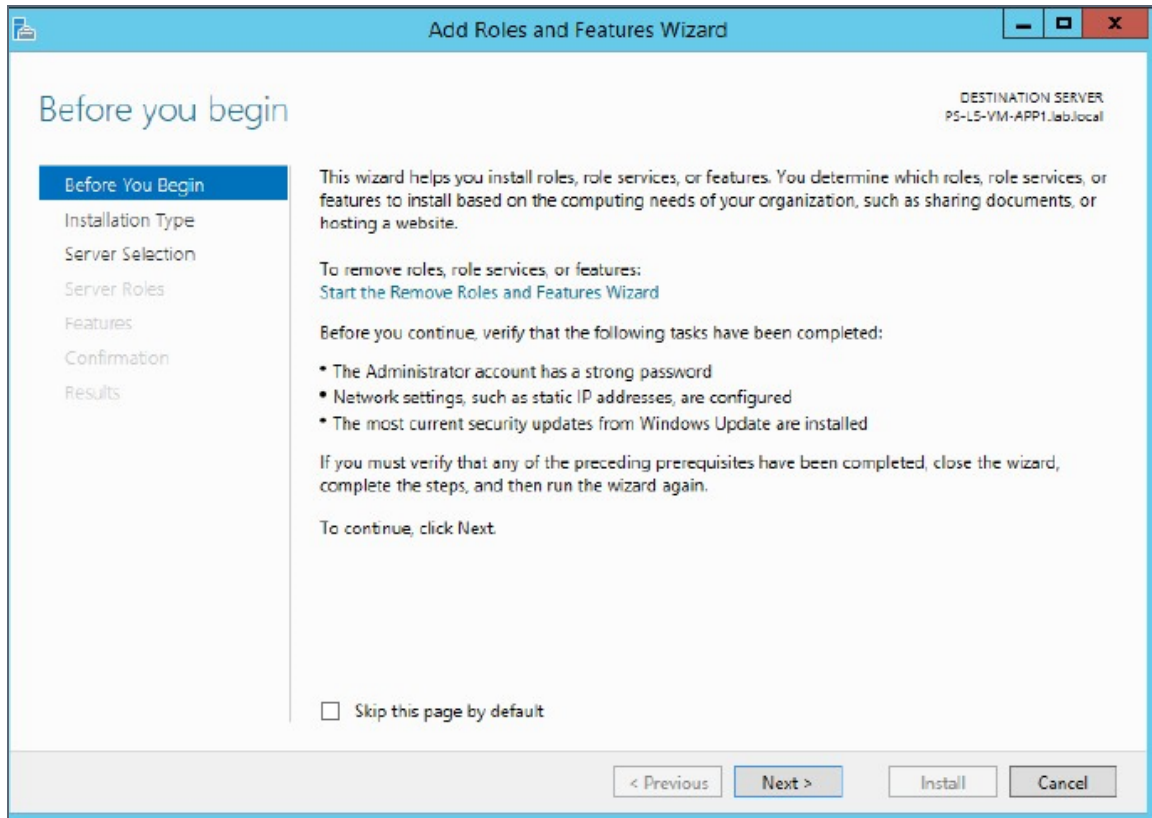
Disable the Windows TCP/IP services from the Windows Control Panel on each application server in the application server cluster.

Procedure

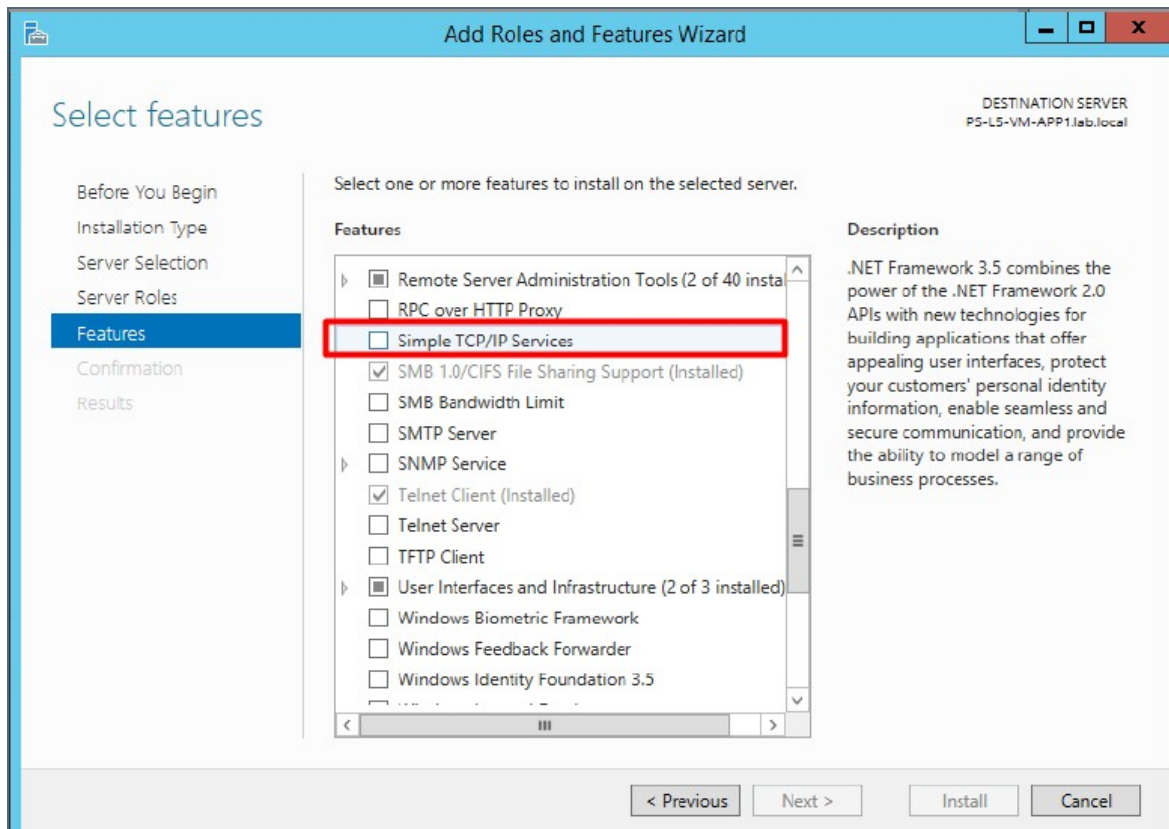
1. On an application server, open Windows Control Panel and select **Programs and Features**.



2. Select **Next** until you reach the **Features** section.



3. Remove the check mark next to **Simple TCP/IP Services**.
4. Complete the Add Roles and Features Wizard.



5. Perform this procedure on each application server in the application server cluster.

What to do next

[Disable the Monitoring services \(page 290\)](#)

Related topics

[Disable TCP/IP and IP Monitoring services workflow \(page 288\)](#)

Disable the Monitoring services

To disable the Monitoring services, update the **tangosol-coherence.xml** file on all application servers in the application server cluster.

Procedure

1. On an application server, access this location:
`%IMPACT360softwareDir%ProductionServer\weblogic\Impact360\ProductionDomain`
2. Open the file **tangosol-coherence.xml** and search for **tangosol.coherence.ipmonitor.pingtimeout**.
3. Change the IP-timeout from **5s** to **0s**. The code section should now look like this:

```
<tcp-ring-listener><ip-timeout system-  
property="tangosol.coherence.ipmonitor.pingtimeout">0s</ip-  
timeout><ip-attempts>3</ip-attempts><priority>6</priority></tcp-ring-  
listener>
```

4. Repeat this procedure on each application server in the cluster.

What to do next

[Restart application servers after disabling services \(page 291\)](#)

Related topics

[Disable TCP/IP and IP Monitoring services workflow \(page 288\)](#)

Restart application servers after disabling services

Restart all application servers in the application server cluster.

Procedure

1. To restart the application servers in a cluster, run the command **Invoke-AppServerCluster** from the Service Implementation Tool. For more information, see the *Service Implementation Tool (SIT) User Guide*.

What to do next

[Confirm the TCP/IP service is disabled \(page 291\)](#)

Related topics

[Disable TCP/IP and IP Monitoring services workflow \(page 288\)](#)

Confirm the TCP/IP service is disabled

Verify that the TCP/IP service is disabled by accessing the coherence logs.

Procedure

1. Open the coherence log located at
%IMPACT360DATADIR%Logs\ProductionServer\Coherence.log.
2. In the coherence log, search for the message **IpMonitor is disabled**. If this message is present, IP monitoring is disabled.

What to do next

[Sanity tests after disabling services \(page 292\)](#)

Related topics

[Disable TCP/IP and IP Monitoring services workflow \(page 288\)](#)

Sanity tests after disabling services

Perform three tests to verify that the coherence cache is working after making the configuration changes described so far.

Test 1

1. Sign in to AppServer1 and create an organization called **Cache Test**.
2. Sign in to AppServer2 and look for the organization you just created. You should see the **Cache Test** organization.

Test 2

1. Sign in to AppServer3 and search for the **Cache Test** organization.
2. Delete the **Cache Test** organization and then check the other application servers. You should not see the **Cache Test** organization on any of the other servers.

Test 3

1. Go to **System Monitoring** and access the **Cache** page.
2. Verify that all application servers in the cluster are listed under the **Host** column. Also verify that the **Synchronized** column has the **Yes** value for each application server.

Related topics

[Disable TCP/IP and IP Monitoring services workflow \(page 288\)](#)

Rollback the configuration changes workflow

If you have disabled the TCP/IP and IP Monitoring services, you can perform the procedures in this workflow to roll back those configuration changes. These procedures re-enable the TCP/IP and IP Monitoring services.

Workflow

1. [Enable the TCP/IP service \(page 293\)](#)
Enable the Windows TCP/IP services from the Windows Control Panel on each application server in the application server cluster.
2. [Enable IP monitoring \(page 294\)](#)
To enable the Monitoring services, update the **tangosol-coherence.xml** file on all application servers in the application server cluster.
3. [Restart application servers after rolling back configuration changes \(page 294\)](#)
Restart all application servers in the application server cluster.
4. [Confirm the TCP/IP service is enabled \(page 295\)](#)
Verify that the TCP/IP service is enabled by accessing the coherence logs.
5. [Sanity tests after rolling back configuration changes \(page 295\)](#)
Perform three tests to verify that the coherence cache is working after making the configuration changes described so far. For instructions see, [Sanity tests after disabling services \(page 292\)](#).

Enable the TCP/IP service

Enable the Windows TCP/IP services from the Windows Control Panel on each application server in the application server cluster.

Procedure

1. On an application server, open the Windows Control Panel and select **Programs and Features**.
2. Select **Next** until you reach the **Features** section.
3. Select **Simple TCP/IP Services** so that a check mark appears for the setting.
4. Complete the Add Role and Features wizard to enable the TCP/IP Services on the application server.
5. Repeat this procedure on the other application servers in the cluster.

What to do next

[Enable IP monitoring \(page 294\)](#)

Related topics

[Rollback the configuration changes workflow \(page 293\)](#)

Enable IP monitoring

To enable the Monitoring services, update the **tangosol-coherence.xml** file on all application servers in the application server cluster.

Procedure

1. On an application server, access this location:
`%IMPACT360softwareDir%ProductionServer\weblogic\Impact360\ProductionDomain`
2. Open the file **tangosol-coherence.xml** and search for **tangosol.coherence.ipmonitor.pingtimeout**.
3. Change the IP-timeout from **0s** to **5s**. The code section should now look like this:

```
<tcp-ring-listener><ip-timeout system-property="tangosol.coherence.ipmonitor.pingtimeout">5s</ip-timeout><ip-attempts>3</ip-attempts><priority>6</priority></tcp-ring-listener>
```
4. Repeat this procedure on each application server in the cluster.

What to do next

[Restart application servers after rolling back configuration changes \(page 294\)](#)

Related topics

[Rollback the configuration changes workflow \(page 293\)](#)

Restart application servers after rolling back configuration changes

Restart all application servers in the application server cluster.

Procedure

1. To restart the application servers in a cluster, run the command **Invoke-AppServerCluster** from the Service Implementation Tool. For more information, see the *Service Implementation Tool (SIT) User Guide*.

What to do next

[Confirm the TCP/IP service is enabled \(page 295\)](#)

Related topics

[Rollback the configuration changes workflow \(page 293\)](#)

Confirm the TCP/IP service is enabled

Verify that the TCP/IP service is enabled by accessing the coherence logs.

Procedure

1. Open the coherence log located at
`%IMPACT360DATADIR%Logs\ProductionServer\Coherence.log`.
2. In the coherence log, search for the message **IpMonitor is disabled**. If this message is not found, IP monitoring is enabled.

What to do next

[Sanity tests after rolling back configuration changes \(page 295\)](#)

Related topics

[Rollback the configuration changes workflow \(page 293\)](#)

Sanity tests after rolling back configuration changes

Perform three tests to verify that the coherence cache is working after making the configuration changes described so far. For instructions see, [Sanity tests after disabling services \(page 292\)](#).

Related topics

[Rollback the configuration changes workflow \(page 293\)](#)

Full-text search

Full-text search (FTS) enables you to search for terms or phrases in transcribed interactions and text interactions.

Topics

Full-text search overview	297
Workflow: Full-text search deployment	298
Configure and manage stopwords and stoplists for full-text search	301

Full-text search overview

Full-text search (FTS) enables you to search for terms or phrases in transcribed interactions and text interactions. FTS is optional and is only supported on database servers that meet the hardware requirements specified in the *CFE Guide*.

FTS is based on the following:

- FTS feature installed on the computer running SQL Server.
- FTS components installed by the WFO installation.

Related topics

[Workflow: Full-text search deployment \(page 298\)](#)

Related information

Customer Furnished Equipment (CFE) Guide

Workflow: Full-text search deployment

In a new installation, if the FTS feature is installed with the SQL Server **before** the system installation, then FTS is enabled by default on the system, and only requires license activation.

If the FTS feature is installed with the SQL Server **after** the system installation, such as after system upgrade, then FTS must be enabled manually by running SQL scripts and activating the license.

Workflow

1. Verify that the Full-text search feature is installed on each computer that runs an SQL Server instance and hosts the Contact OLTP Database and Contact Database roles.
2. [Enable full-text search \(page 298\)](#): Enabling full-text search installs components required for this feature.
3. [Activate the Full-Text Search license \(page 299\)](#): To use the Full-Text Search feature, activation is required in the WFO portal.

Enable full-text search

This procedure is only required if the Full-text search feature is added after the system installation.

Enabling full-text search installs components required for this feature by running FTS SQL scripts on each computer that runs an SQL Server instance and hosts the *Contact OLTP Database* and *Contact Database* roles.

These components include:

- Full-text catalog
- Stop list
- FTS index



This procedure is intended for system engineers. As a customer, contact your service representative.

Before you begin

1. Download the *FTS Scripts* as follows:
 - a. From **VerintConnect** home page, go to **Tools & Resources > WFO Patches, Desktop Apps, Tools**. (*Internal or Partner*. Not available for *Customer*)
 - b. In the upper left corner, from the **Select version stream and press View Report:** list, select **15.2**.
 - c. Click **View Report**.
 - d. Click **Tools Page: 15.2** link.

- e. Download the *FTS Scripts* package. It contains the following SQL scripts:
 - Enable_FTS_on_Contact_OLTP_Database
 - Enable_FTS_on_Contact_Database

Procedure

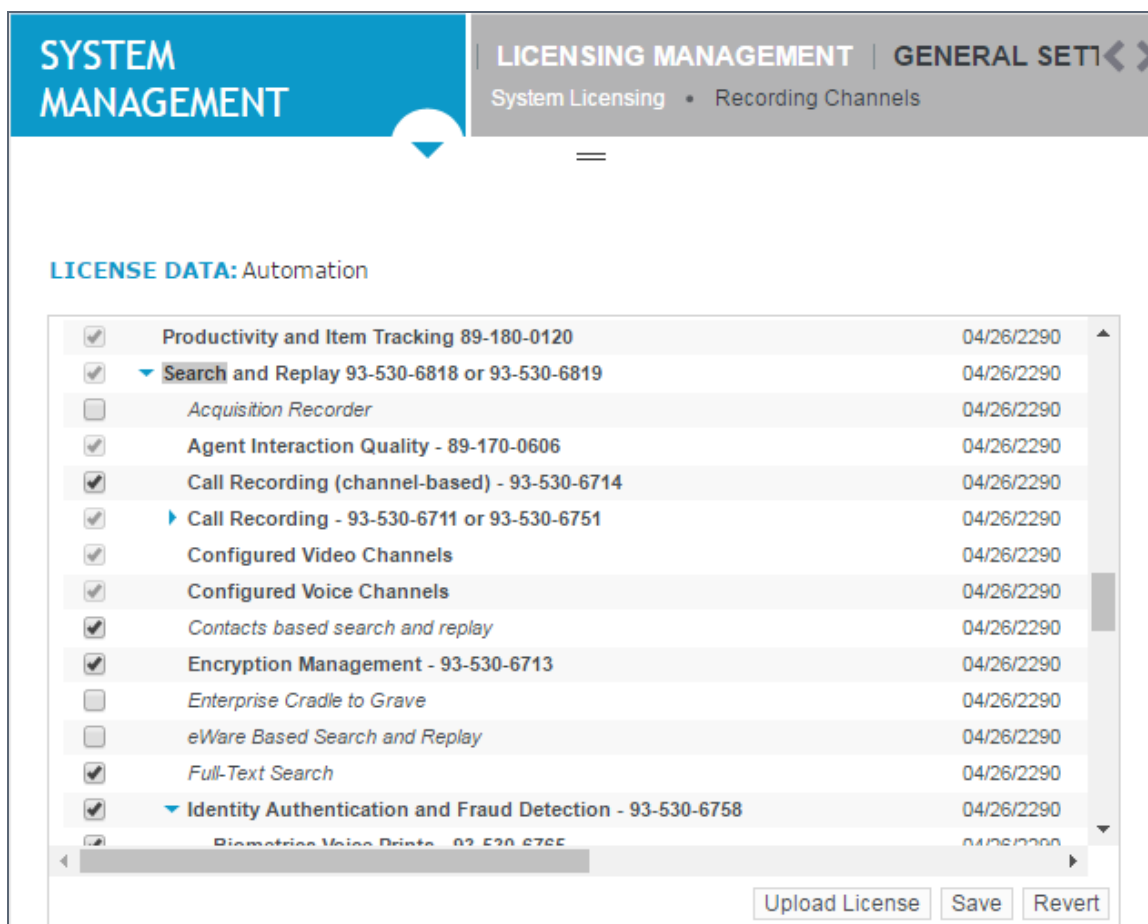
1. Open SQL Server Management Studio.
2. Connect to the SQL Server instance hosting the Contact OLTP Database role using a Login account with sysadmin credentials. Do the following:
 - a. Execute the **Enable_FTS_on_Contact_OLTP_Database** script.
 - b. Verify that the message: 'FTS enablement is successful' is displayed.
3. Connect to the SQL Server instance hosting the Contact Database role using a Login account with sysadmin credentials. Do the following:
 - a. Execute the **Enable_FTS_on_Contact_Database** script.
 - b. Verify that the message: 'FTS enablement is successful' is displayed.

Activate the Full-Text Search license

Full-Text Search license activation is required to initialize the feature on the WFO application.

Procedure

1. Sign in to the portal as administrator.
2. From System Management, select **Licensing Management > System Licensing**.
3. Go to **Recording Platform** and select **Full-Text Search**.
4. Click **Save**.



5. Wait until configuration distribution is completed.
6. Restart the **WFO_ProductionDomain_ProductionServer** service on the Application Servers to implement the Full-Text Search license:
 - a. On the Application Server, open Windows Services.
 - b. Restart the WFO_ProductionDomain_ProductionServer service.
 - c. If the Application Servers are clustered, stop the WFO_ProductionDomain_ProductionServer service on each Application Server in the cluster. Once the service is stopped on all Application Server, start the service one on each Application Server at a time.
7. If servers hosting Speech Transcription Service role exist, restart these services.
8. In the **User Management** application, set the **Full Text Search** privilege for the relevant roles.

Related information

Roles and Privileges (*Workforce Optimization User Management Guide*)

Configure and manage stopwords and stoplists for full-text search

To prevent a full-text index from becoming bloated, SQL Server has a mechanism that discards commonly occurring strings that do not contribute to the search (such as "a," "and," "is," and "the"). These discarded strings are called stopwords.

During index creation, the Full-Text Engine omits stopwords from the full-text index. This means that full-text queries will not search for stopwords. A stoplist is a container of the stopwords.

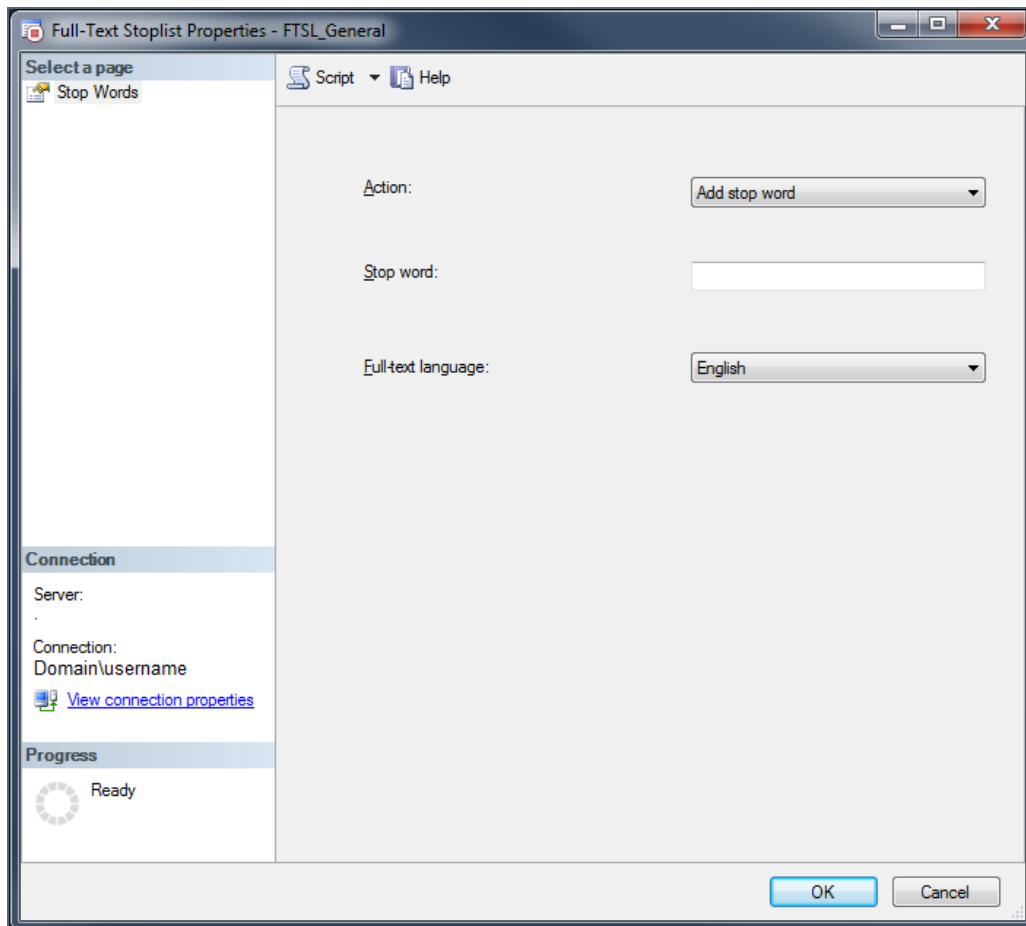
The default stoplists provided by the system are similar to the stoplist provided by Microsoft. The same stoplist is installed on the servers hosting the Contact OLTP Database role and Text Database role.

You can configure and manage the stoplists to meet your business needs. Any update of the stoplist must be done similarly on both databases.

Procedure

1. Open the SQL Server Management Studio.
2. Connect to the computer running the SQL Server instance that hosts the **Contact OLTP Database** role.
3. In the Object Explorer, select **Databases > LocalContact > Storage > Full-Text Stoplists**.
4. Right-click **FTS_General** and select **Properties**.

The Full-Text Search Stoplist Properties is displayed.



5. From Action, select the required action:
 - Add stop word
 - Delete stop word
6. Type the word to add or delete.
7. Select the language to configure its stoplist.
8. Click **OK**.



To display the stopwords of the stoplist for English , in SSMS run the following:
`SELECT * FROM [sys].[fulltext_stopwords] WHERE [language] = N'English'`

9. Repeat steps **5-8** for each stopword you want to configure.
10. Populate the Full-Text index as follows:
 - a. In the Object Explorer, navigate to the **[LocalContact].[dbo].Interactions_text** table.
 - b. Right click the table and select **Full-Text Index > Start Full Population**.
 The index population duration depends on the index size. During the index population, it is possible to perform a search. However, the results reflect the actual index at the moment.

11. Connect to the computer running the SQL Server instance that hosts the **Contact Database** role (CentralContact).
12. In the Object Explorer, select **Databases > TextDB > Storage > Full-Text Stoplists**.
13. Repeat steps **4-9** for the **TextDB** Database.
14. Populate the Full-Text index as follows:
 - a. In the Object Explorer, for each of the the **[TextDB].[dbo].[Interactions_text_month_n]** tables (where **n** is 1 to 12), navigate to the table.
 - b. Right-click the table and select **Full-Text index > Start Full Population**.

The index population duration depends on the index size. During the index population, it is possible to perform a search. However, the results reflect the actual index at that moment.