HFR and WFO Update Package

Installation Guide

Version 15.X

April 01, 2019
Revision 1.05

Notice

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

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by Avaya. You agree 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 You.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:
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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://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 AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS THE SOFTWARE (AS DEFINED IN THE AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS), AND WHO PURCHASED THE LICENSE FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. REFER TO THE AVAYA SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS FOR INFORMATION REGARDING THE APPLICABLE LICENSE TYPES PERTAINING TO THE SOFTWARE.

All Rights Reserved

Avaya and/or its licensors retain title to and ownership of the Software, Documentation, and any modifications or copies thereof. Except for the limited license rights expressly granted in the applicable Avaya Global Software License Terms for Verint Software Products, Avaya and/or its licensors reserve all rights, including without limitation copyright, patent, trade secret, and all other intellectual property rights, in and to the Software and Documentation and any modifications or copies thereof. The Software contains trade secrets of Avaya and/or its licensors, including but not limited to the specific design, structure and logic of individual Software programs, their interactions with other portions of the Software, both internal and external, and the programming techniques employed.

Virtualization

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

Third Party Components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for any Software that has distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Software, Documentation or on Avaya's website at: http://support.avaya.com/Copyright (or a successor site as designated by Avaya).

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Security Vulnerabilities

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, any Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

About this guide

This document details the installation procedures for HFR and WFO Update Package regardless the version of the package.

Intended audience

The HFR and WFO Update Package are implemented by services, support organizations, partner, or customer's system administrators.

Document revision history

Revision	Description of changes
1.05	• Added SQL Server 2016 to the *Prepare_F&S Servers* section. • Updated the *Install SQL Server Native Client on F&S server* section.
1.04	• Added an option to back up AD LDS manually. • Added a step to the Rollback section to restore AD LDS from backup.
1.03	HFR3 update: • Added to HFR pre-installation requirements that the Contact OLTP and Contact Database sizes were increased in V15.2 HFR3 due to the events logging feature. These databases must be resized. • Removed the requirement to install Customer Feedback Survey Server KB from the post installation section. • Added a guideline about dependency between the real-time API, Real-time Speech Analytics (RTSA), and Speech Analytics. • Added a requirement to close WFM shift bid auctions before installing the HFR package.
1.02	• Clarified that if additional standalone KB at the same time with the HFR are required, then need to add them to the HFR installation. • If additional standalone KB are required after HFR installation, then use the Hotfix Deployment Tool.

Revision	Description of changes
1.01	Added a generic installation procedure for HFR Package on top of V15.1 and V15.2 releases.
1.00	Initial release

Chapter 1

HFR Package installation

Before installing the hotfix rollup package (HFR), review the information on planning and prerequisites, and then select an installation option based on the type of deployment.

Topics

HFR installation overview

The HFR installer automatically detects the installed components, server roles, and hotfixes on each server, compares them with the hotfixes included in the release, and then installs only the newer hotfixes for the relevant server roles of each server.

At the end of HFR installation, if installation of standalone KBs is require on top of the HFR, you can use the Hotfix Deploy Tool or install each standalone KB manually.

Installation guidelines

A dependency for the real-time API exists between Real-time Speech Analytics (RTSA) and Speech Analytics. Install the KBs for the real-time API for *both* products or for neither product. If you install either KB by itself, the RTSA service stops working or fails with an error.

- KB150005: Real-time API for RTSA
- KB150090: Real-time API for Speech Analytics (Recorder Analytics Framework)

Installation methods

Based on your deployment, you can install the HFR package using any of the following methods:

- **Local installation**: Download the HFR package to the target system server, and run the HFR installer on the same server. This option requires 2 GB of free space on each of the target system servers.
- **Local installation from central repository**: Download the HFR package to a central repository, and then run the HFR installer locally on each of the target system servers.
- **Remote installation**: Download the HFR package to a central repository, and run the HFR installer from a remote machine that is not part of the system. Alternatively, you can download to a central repository on the remote server from which you are running the HFR installer.

On Windows 8.1, the **Remote Registry** service is disabled by default. Manually enable the Remote Registry before doing a remote installation.

HFR installation planning

Before you install the HFR package, it is recommended to plan for the installation, taking into account the time required to install the HFR package based on your system deployment and the functionality affected during the installation.

Related topics

HFR installation for distributed sites, page 9
HFR installation time, page 9
Affected functionality, page 10

HFR installation for distributed sites

Customers with deployments spread across multiple physical sites can install the HFR on a site-by-site basis, subject to whether you are installing logical Data Center Zone servers or servers on physical sites.

Logical Data Center Zone servers installation

Install the HFR for all the servers in the logical Data Center Zone (on the Data Center physical site) within a single maintenance window.

If there is no particular reason to install sites before the Data Center, the best practice is to install the Data Center first.

Parallel installation

Parallel installation is not supported for the following deployments:

- Application and Database Platforms on separate servers

  For this deployment, install the HFR first on the Database Platforms, and then on the Application Platforms.

  Before installing the Application servers in the Data Center, stop the WFO service (WFO_ProductionDomain_ProductionServer) on each server in the cluster. Then install the HFR simultaneously on all the servers in the cluster. Once HFR installation is complete, restart each server.

- Deployments with recording redundancy

  For this deployment, to prevent media and CTI data loss, install the HFR first on the primary servers, and then on the redundant servers.

HFR installation time

The time required to install the HFR package depends on the specific deployment and the HFR version from which you are upgrading.

If you are upgrading remotely across slow network connections, the installation time per server may be longer than the time listed in the table.

Server	Installation time
Consolidated platform: hosting databases, applications, and recorders	2.5 hours
Data Center platform: hosting databases and applications	2 hours
Database platforms	1.5 hours
Application platforms	2 hours
Recorders	1 hour
All other platforms	1 hour

Affected functionality

The functionality affected during HFR installation depends on your system deployment.

Data Center zone installation
Application functionality is not available.

Site zone installation
Media is not recorded, and CTI calls are not tagged.

Consolidated platform installation
Application functionality is not available, media is not recorded and CTI calls are not tagged.

HFR pre-installation requirements

Before you begin the installation, verify that your system meets the general requirements for HFR installation, including the specific requirements for the current HFR package.

Requirement	Description
Free space	At least 2 GB of free space on the software drive of each server on which the HFR is to be installed.
Database Sizing	The Contact OLTP and Contact Database sizes were increased in V15.2 HFR3 due to the events logging feature. The increase is gradual and will start after installing HFR3. Customers performing an in-place upgrade from a previous HFR or from V15.1, must resize these databases.
Databases backup	For rollback purposes, create a backup of all databases. **Related Information** Databases backup (*Maintenance Guide*)
System Configuration backup	Back up the existing system configuration including AD LDS (ADAM) **Related Information** System configuration backup (*Maintenance Guide*) Back up ADAM manually *Maintenance Guide*)
Scheduled Windows updates	Windows allows one MSI to run at any given time. Verify that other Windows updates, such as Windows Antivirus, are not scheduled to run during HFR installation.
System configuration	Verify that no configuration changes are pending on the servers on which you want to install the HFRs. Check if the Pending Messages icon is displayed in Enterprise Manager. If servers belonging to the Data Center logical zone are being installed, verify that these servers are not Blocked. All other servers can be Blocked.
SQL Client Tools Connectivity feature	Verify that the SQL Client Tools Connectivity feature is installed on the SQL Servers. In addition, make sure that the version of the Client Tools Connectivity feature matches the installed SQL Server version. **Related Information** *SQL Server Installation and Upgrade Guide*

Requirement	Description
Download HFR installation package	**1** Download the HFR from Avaya Support at: http://support.avaya.com. It is recommended to verify the integrity of the zip files against the included .md5 file using a recognized file manager tool such as Total Commander, Tool Commander, or MD5Summer. **2** Extract the downloaded package to a shared folder on the customer network. **3** Set the shared folder properties as follows: a. Right-click the shared folder, and select **Properties**. b. Click **Sharing**. c. Click **Advanced Sharing**. d. Select **Share this folder**. e. In the **Share** field, type the name of the folder that contains the hotfix. f. Click **Permissions**. The **Permissions for** window is displayed. g. Click **Add**, and select the **Management Service Account**. h. In the **Allow** column, select **Full Control** and click **OK**. i. In the **Permissions** for folder window, click **OK**.
Download standalone KBs	If you need to install standalone KBs at the same time when HFR is installed, download all KBs to be installed to the correct folder: **\Components\Hotfix Deployment\Hotfixes** Verify that all the standalone KBs are not older than the KBs included in the current HFR. Installing a standalone KB older than the current KBs will fail during the deployment process.
Prepare Forecasting and Scheduling Servers	In deployments that include standalone Forecasting and Scheduling Servers or SQL 2008 R2, the SQL Server Native Client (SQLNCL11) is required to be installed. For SQL Server 2012, 2014, and 2016, see: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server For SQL Server 2008 R2 (X64): http://go.microsoft.com/fwlink/?LinkID=239648&clcid=0x409

Requirement	Description
Verify connectivity and the Management Service Account	**1** Sign in to the Enterprise Manager. **IMPORTANT |** Do not install the HFR unless you can Sign in to the Enterprise Manager. **2** Verify there is connectivity between the Application or Recorder server and the server hosting the Weblogic components and database; otherwise, certain hotfixes, which require access to these components, will fail to apply. **3** Verify the following for the Management Service Account: - user name and password - user is a local administrator on each of the target servers
Close WFM shift bid auctions	WFM shift bid auctions must be closed prior to upgrading the system. If a schedule auction is open when an upgrade is done, any pending requests are invalidated and schedules will have to be refreshed.

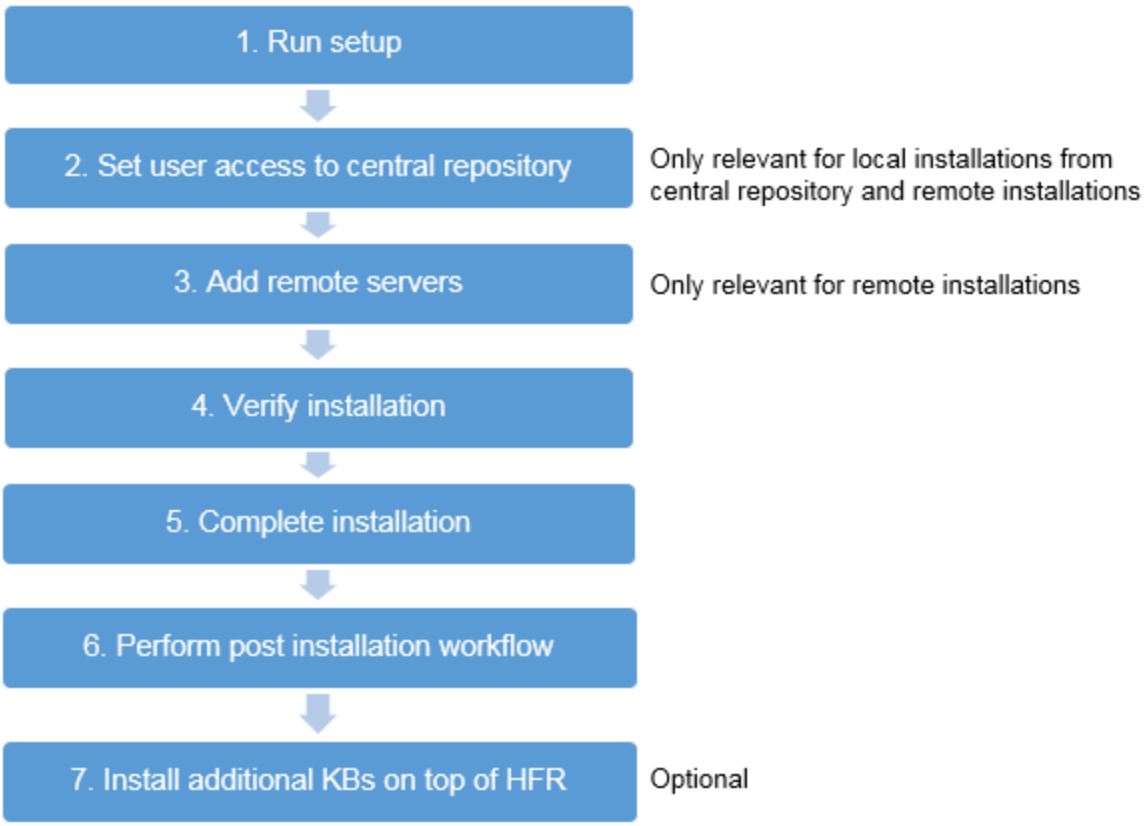
Install HFR package

The installation wizard guides you through the steps required to install the HFR package. You may have to perform additional steps if you are installing remotely, or locally from a central repository.

If you have also downloaded standalone KBs to the relevant folder, the Hotfix Deploy tool automatically installs all the KBs at the end of the HFR installation, without requiring any intervention on your part.

If you do not run the Installer from the same server used in the previous installation, do not install the local and remote servers simultaneously because during the installation process, the server requires a restart.

HFR package installation at a glance



During installation the server is rebooted one or more times. To perform unattended reboots, the installer configures Windows *AutoAdminLogon*.

If the customer has configured **Legal Notices** to pop-up with *AutoAdminLogon*, the reboot operations require manual acknowledgement of the **Legal Notices**.

Procedure

1 Run setup:

Based on the type of HFR installation, do one of the following:

- Local installations: run **Setup.exe** from the HFR package.
- Local installations from a central repository or for remote installations:
  - Browse to the repository and set it as a shared folder.
  - From the Installer menu, select **Tools > Repository Settings**.
  - In the Repository Settings window, type the User name (domain short name and user name) and Password and click **OK**.
  - Run **\\<full path of the shared storage location>\Setup.exe**.

2 In the Welcome window, enter the Installation Account **User name** (domain short name and user name) and **Password**. Select **Remember My Password**, and then click **Apply**. (The uccount must have Local Admin Rights.)

3 Set user access to central repository:

Required only for local installations from a central repository and remote installations.

See Set user access to central repository, page 16.

4 In the Select Platform window, verify that the relevant HFR option is selected (default).

5 Add remote servers:

Required only for remote installations. See Add remote servers to the network pane, page 30.

6 In the Install Setup window, select the target server for installation:

a. From the **Network** pane, select a server on which to install the HFR.

b. Verify that the  icon is prefixed to the server name indicating that it is ready for installation.

c. From the **Group** list, select the relevant HFR to install.

d. Verify that the **Install/Upgrade** option is selected.

e. To manually reboot the server, set **Reboot after completing the installation** to **No**.

The default option is set to Yes, which automatically reboots the server after HFR and KB installation.

f. If you have downloaded standalone KBs to \Components\Hotfix Deployment\Hotfixes\, verify that **Hotfix Deployment** and all its sub-components are selected in the Install Setup tree.

g. If you have added remote servers, repeat *Step a* through *Step e* for each server to be upgraded.

h. Click **Next** to continue.

7 In the Final Check window, click **Next** to continue.

8 In the Ready to Install window, do the following:

a. If a Prerequisite/Dependency Error message opens, follow the instructions in the message to resolve the error.

b. Verify that the following options are selected:
   - **Display a prompt before restarting the target machine**: Selected by default. If you do not want to display a prompt for every restart during installation, clear this option.
   - **Set log level to DEBUG mode**: Selected by default to activate debug mode for the installation log for troubleshooting purposes. To disable debug mode for the installation log, clear this option.

c. To create a platform settings report, select the option and then click **Browse** to select a location on the network for the report file. The default file name for the report is IP_platformName_ date.html.


You can also generate the platform settings report manually, after the installation is complete. See *Step 10*.

9 Complete installation:

a. Click **Install** to start the installation process.

The Platform/Site Progress window opens displaying the installation status and log files for each component.

b. Wait until the servers restart automatically.

When the installation is completed successfully a confirmation message appears. The computer's indication in the left pane displays a green check mark.

10 (Optional) To manually generate the platform report, do the following:

a. Select **Tools > Reports > Platform Report**.

b. Enter a file name and destination and save the report.

c. Send the Platform Report to your contact person.

11 Verify HFR version from the **Control Panel > Programs and Features**.

Set user access to central repository

Access rights to the central repository are required after restarting the local server. The Installation Account user is used by default. If this account does not have access to the repository, change the credentials to a user with access to the central repository.

Procedure

1 From the Installer menu, select **Tools > Repository Settings**.

2 Type the **User name** (domain short name and user name) and **Password**.

3 Click **OK**.

Add remote servers

If you are running the HFR installation for the first time, the Network pane displays only the local server. If you have already installed HFRs, the Network pane shows the remote servers you added during previous installations.

Add each server on which to install the HFR, one at a time. You can add up to 25 servers in parallel. You can also add all remote servers at once using the SR_ServerTree_Builder.exe tool. See Add remote servers using the SR_ServerTree_Builder.exe, page 31.

The installation option to group servers under a site node is not supported.

Procedure

1. Select **Edit > New Machine**  .
2. In the **Server Address** field, type the IP address of the remote server to add.
3. Type the Installation Account **User name** (domain short name and user name) and **Password**.
4. Clear the **Use Default User** option.
5. Click **Add**.

   The Installer attempts to detect the remote server and connect to it. The following indications can be displayed: Connection in process.

    Detection in process.

    Connection and detection processes are completed successfully.

    The server is ready for installation.
6. If the Installer fails to connect to the remote server, check the status that appears and continue with Troubleshoot remote server connectivity, page 18.

Add remote servers using the SR_ServerTree_Builder.exe

To add multiple remote servers at once to the SR Tool, run SR_ServerTree_Builder.exe on one of the servers configured in the Enterprise Manager.

Procedure

1. Log on to any server in the Enterprise Manager.
2. Open a command prompt.
3. From the root directory of the installation package, run **SR_ServerTree_Builder.exe**.

   The output includes three XML files that you can open from the SR Tool:
   - **Project_All.xml**: Used to install on all servers in the entire enterprise.
   - **Project_DC.xml**: Used to install only on the Data Center servers.
   - **Project_Sites.xml**: Used to install only on the Site servers.
4. From the SR Tool, click **File > Open** and locate the created XML files.
5. Select the required XML file and click **Open**.

Troubleshoot remote server connectivity

If you have connectivity issues when adding servers for remote installations, check the status and then follow the steps listed below to resolve issue.

Icon	Status	Troubleshooting Steps
	Machine not connected	Check network access to the remote server.
	Failed to access remote server	Failed to access the remote server due to one of the following reasons: • User name problem • Access rights Windows Management Instrumentation (WMI) access problem • Check domain, password and DNS registration If the problem persists, check the WMI status to locate and resolve the issue using the WMI Tool. See *WMI Tool* section in the *Installer* help.
	Missing setup prerequisite	Right-click the component and select Install Prerequisite.
	Failed to detect or run the Installer.	Locally run the WMI Tool on the remote server.

Workflow: Post installation

After completing the installation, perform post installation procedures.

Workflow

1. Install additional KBs on top of HFR , page 19

   If additional standalone KBs are not installed at the same time when HFR is installed, use the Hotfix Deployment Tool to install the additional standalone KBs.
2. Clear cache on Application Servers Cluster, page 33

   On Application Servers Cluster, the cache coherence initializes the current version of the software. After update or removal, to prevent functionality issues, the cache must be cleared on all the Application Servers in the cluster at the same time.
3. Distribute configuration to the Reporting Server, page 33

   The configuration updates due to the package installation must be distributed to the Reports Server.
4. Distribute configuration to Archive Database server role, page 20

   For a successful migration of CENTERA archive, distribute the configuration for Archive Database server role.
5. Disable file upload in coaching, page 34

   To address a security issue, disable uploading file attachments in coaching sessions.
6. Latest Secure Gateway KB installation, page 34

   To avoid potential security risks, install the latest Secure Gateway KB.
7. Service alarms restart, page 21

   If a service restart alarm is raised in the Portal, restart the service in the next scheduled maintenance window.

Install additional KBs on top of HFR

If additional standalone KBs are not installed at the same time when HFR is installed, use the Hotfix Deployment Tool to install the additional standalone KBs. Make sure to install the mandatory KBs. Other KBs are optional.

You cannot use the same HFR kit to only run Hotfix Deployment. HFR kit validates against the HFR installed version and raise a Validation Error that the current installed HFR version is higher or equal to the version you attempt to install.

Procedure

1. Download **Hotfix Deployment Tool**.
2. Copy all the KBs you want to install into the folder:

   \Components\Hotfix Deployment\Hotfixes\
3. In the Install Setup window, select the Hotfix Deployment Tool.

   The sub-folders are automatically selected and the list of KBs pending installation is displayed.
4. Click **Next** to continue.

Clear cache on Application Servers Cluster

On Application Servers Cluster, the cache coherence initializes the current version of the software. After update or removal, to prevent functionality issues, the cache must be cleared on all the Application Servers in the cluster at the same time.

Procedure

1. Stop the **WFOProduction** and **watchdog** services on each of the Application Servers in the cluster.
2. Once the services are stopped on all the Application Servers, start the **WFOProduction** and **watchdog** services one by one on each of the Application Servers.

Distribute configuration to the Reporting Server

The configuration updates due to the package installation must be distributed to the Reporting Server.

Procedure

1. Go to **System Management > Enterprise > Settings**.
2. Select the server hosting the **Reporting Services** server role.
3. In the Description field, type **test** and click **Save**.

   Wait 5–10 for the configuration and distribution to complete. When complete, all pending messages must be cleared.

Distribute configuration to Archive Database server role

For a successful migration of CENTERA archive, distribute the configuration for Archive Database server role.

Procedure

1. In Enterprise Manager, select the **Archive Database** server role and click **Save**.

Disable file upload in coaching

To address a security issue, disable uploading file attachments in coaching sessions.

Procedure

1. Add the BPCONFIG key witness/coaching/global/noFileAttachments as follows:

   Run this script on the BPMAINDB database server.

```
USE BPMAINDB
IF NOT EXISTS (SELECT 1 FROM BPCONFIG WHERE NAME =
witness/coaching/global/noFileAttachments')
BEGIN
DECLARE @nextkey INT
 EXEC Bp_nextkey 'BPCONFIG', @nextkey output, 1
 INSERT INTO BPCONFIG (ID, NAME, VALUE ) values (@nextkey,
```

```
'witness/coaching/global/noFileAttachments','true')
END
```

No need to restart the application service for the BPCONFIG key to take effect.

Latest Secure Gateway KB installation

To avoid potential security risks, install the latest Secure Gateway KB.

If you do not install the Secure Gateway KB, users bypass the logon page and are able to see all test pages. When users try to browse to real pages, they are redirected to the logon page.

The Secure Gateway KB is not included in the update package. Download the Secure Gateway KB zip file from an appropriate location.

Related information

Secure Gateway KB

Service alarms restart

If a service restart alarm is raised in the Portal, restart the service in the next scheduled maintenance window.

There is no impact on functionality while the alarm is on.

HFR installation troubleshooting

If there are issues when installing the HFR package or the standalone KBs, refer to the tables below to identify the symptom and resolve the issue.

HFR installation troubleshooting

Symptom	Resolution
Installation failure.	1 Collect the component and log information from the following folders: - %Impact360SoftwsreDir%<component name>\ - <drive>:\program files (X86)\Server Readiness\Log 2 Compress these folders and send to technical support.
Installation fails at stage of "Adding Code Signing Certificate".	Reboot server and re-run the install.
Issues during remote installation at customer sites with strict security settings: • The Installer cannot connect to all the servers in the Enterprise. • As a result of network issues, "disconnect" errors appear in the log and sporadic components fail.	Do one of the following: • Install locally. • Install locally from a central repository.
• Cannot create users, organizations or groups. • Error appears on accessing the Alarm Status page in the Portal.	HFR package not installed in the correct order.Application platform was installed before the Database platform. 1 Restart the Application Server(s). 2 After the server is up, check System Monitor for any additional service restart alarms.
SR Tool remains in a connecting state (yellow arrow) and does not progress.	Right-click the server and select **Reconnect**.
Errors on installing Java.	Click **Done** and restart the install process again.
Users cannot access Interactions Applications or Speech Analytics Applications	Full User Management (UUM) synchronization in progress. Wait until the full UUM sync has completed.

Symptom	Resolution
The Portal is not accessible. -or- WFO_ProductionDomain_ ProductionServerservice is not fully loaded on one or more Application servers.	EAR was not deployed. Customer: contact support Partber or internal: Deploy the *EAR* manually. See *EAR Manual Deployment*.

Standalone KB deployment troubleshooting

Symptom	Resolution
Error message is displayed while reading the MSI during Hotfix deployment.	• Remove the problematic KB or download the correct version. See the *Hotfix Deploy Tool User Guide*
The installation of an old standalone KB fails and an error message appears.	• Verify that all KBs for installation on top of the HFR are not older than the KBs included in the HFR. • Remove the problematic KB or download the correct version. • Re-run the Hotfix Deploy Tool.
RTSA service stops working or fails with an error	A dependency for the real-time API exists between Real-time Speech Analytics (RTSA) and Speech Analytics. Install the KBs for the real-time API for *both* products or for neither product. If you install either KB by itself, the RTSA service stops working or fails with an error. • KB150005: Real-time API for RTSA • KB150090: Real-time API for Speech Analytics (Recorder Analytics Framework)

HFR installation rollback

You can roll back the HFR version currently installed at any time if there is a problem with the installation. After rollback of an HFR, the system automatically reverts to the previous configuration settings. You must manually restore any configuration settings defined after the HFR installation.

Before you begin

1. Make sure you have access to the database and system backups you created before you applied the HFR.
2. Ensure that there is connectivity between the Site server and the servers in the Data Center zone (prevents hotfixes that require such access from failing).
3. Ensure that you have the Installation Account User name and password. Verify that this account is a local administrator on each of the target servers.
4. Manually uninstall all the KBs installed by the Hotfix Deploy Tool.

If the HFR rollback runs before removing the standalone KBs, the rollback fails and prompts you to first uninstall the relevant KBs.

   a. From the Control Panel, select **Programs and Features**.
   b. Right-click the KB, and then click **Uninstall**.
   c. Repeat for each KB.

Procedure

1. Log on to the local server with the Installation Account.
2. From the Start menu, select **Run**, type: **\\<full path of the shared storage location>\Setup.exe**, and click **OK**.
3. In the Welcome window, enter the Installation Account **User name** (domain short name and user name) and **Password**. Select **Remember My Password**, and then click **Apply**.
4. In the Select Platform window do the following:
   a. From the Network pane, select a server to remove. The server indication must be  (ready).
   b. From the Group list, select the HFR you installed.
   c. Select the **Remove** option and click **Next**.

      The Remove Setup window opens. The window displays the list of components installed by the Installer.
   d. Click **Next**.
5. In the Final Check window, click **Next**.
6. In the Ready to Remove window, select the following options:
   - **Display a prompt before restarting the target machine**: Selected by default. If you do not want to display a prompt for every restart during rollback, clear this option.
   - **Set log level to DEBUG mode**: Selected by default to activate debug mode for the installation log for troubleshooting purposes. To disable debug mode for the installation log, clear this option.

7 In the **Report** area, select the option to create a platform settings report, and then click **Browse** to find a location on the network where the report file will be generated. The structure of the default file name is IP_platformName_date.html.

8 To start the removal process, click **Remove**.

The Platform Progress window opens displaying the installation status and log files for each component. Components installed last are removed first.

9 If a Microsoft standard security legal notice opens when restarting the server, click **OK** to continue.

10 Perform the following **post-rollback** steps:

a. Restore the databases that you have backed up before the upgrade to HFR.

b. Restore the AD LDS backup folder.

c. If you roll back to V15.2 GA, increment the message ID sequence. In the SQL Server Management Studio, run:

```
IF OBJECTPROPERTY(OBJECT_ID('EM_INCREMENT_MESSAGE_ID_SEQUENCE'),
'IsProcedure') = 1 DROP PROCEDURE EM_INCREMENT_MESSAGE_ID_
SEQUENCE
GO
CREATE PROCEDURE EM_INCREMENT_MESSAGE_ID_SEQUENCE AS
BEGIN
 DECLARE @number_of_days INT,@Nextkey BigInt,@Numkeys Int Exec
dbo.BP_NEXTKEY 'INSTALLMESSAGESEQUENCE',@Nextkey Output,50000
 END
GO
GRANT EXECUTE ON EM_INCREMENT_MESSAGE_ID_SEQUENCE TO PUBLIC
GO
```

d. In the SQL Server Management Studio, run:

```
execute bpmaindb.dbo.EM_UPDATE_IDS_UPON_RESTORE_DB
```

e. Restart the Database machines on which the HFR is rolled back.

f. Stop the WFO service on each application server.

g. Run command prompt as administrator and execute:

```
cscript.exe %IMPACT360SOFTWAREDIR%WFODeployer\DeployWfo.vbs <WLS Admin>
<WLS Admin Password> true true
```

h. Restart each application server.

i. If WLSMon was previously enabled to monitor Weblogic operational status, contact Support to restore this functionality.

Related information

Restore Databases (*Maintenance Guide*)

Restore the AD LDS backup folder (*Maintenance Guide*)

Chapter 2

WFO Update Package installation

This package contains the latest hotfixes (KBs) released over V15.1 GA. The package provides defect resolution for known issues. The hotfixes address customer-reported defects, which have been tested extensively.

Topics

WFO Update Package installation overview

The installation tool (SR Tool) automatically detects the installed components, server roles, and hotfixes on each server, compares them with the package hotfixes, and then installs only the newer on each server.

Installation guidelines

This section defines the process and policy for installation of this package:

- It is recommended running the SR Tool from a local server that is not part of the deployment (allocated temporarily for this purpose only). If a temporary local server is not available, run the SR Tool from a local server with the least time-consuming installation (for example, the Application server).
- Do not install the local server and remote servers simultaneously, because during the installation process the server requires a restart.
- Install the local server either before or after the remote server installations.
- Due to a dependency of the Application platform on the Framework Database server role, in deployments L3-L6, install the Database Servers before the Application Server.
- The Customer Feedback Survey server and the Speech Analytics Transcription cluster servers must be upgraded at the same time. (only relevant to Avaya).

Downtime

Installation on a live system involves downtime. The estimated downtime is 60–90 minutes per platform and can vary per system.

During downtime, the system has the following limitations:

- Audio is not recorded while the package is installed on the Recorder servers (not relevant to Avaya).
- CTI data is not tagged while the Site platforms are updated (not relevant to Avaya).
- Search, playback, and other application functionality are not available.
- No archive operation is performed during the installation.

Workflow: Install package

Install the package on the Data Center servers and on the Site servers.

Workflow

1. Pre-installation requirements, page 28

   Before you begin the installation, verify that your system meets the pre-installation requirements.
2. Run the SR Tool, page 29

   The SR Tool guides you through the steps required to install the update package.
3. Set default user account to access installation files, page 30

   The SR Tool requires a user account with access rights to the shared folder where the update package installation files exist.
4. Add remote servers to the network pane, page 30

   The first time you run the SR Tool, the Network pane only displays the local server. You can install remote servers in a single run of the SR Tool. You can install up to 10 servers in parallel.
5. Install on multiple servers, page 31

   You can load machine definitions from a CSV/XML File for installing on multiple servers in a single run.
6. Select a server and start the installation, page 31

   Select the server on the network pane relevant to the WFO update package and start the installation process.

Pre-installation requirements

Before you begin the installation, verify that your system meets the pre-installation requirements.

Requirement	Description
Back up data	Back up data before starting the installation process. For large installations, backing up can take hours. For backup and restore instructions, see the *Workforce Optimization Maintenance Guide*.
Verify access to the system	• Verify that you can sign in to the portal. • Verify that there is connectivity between the Site server and the server hosting WebLogic and database. This verification prevents hotfixes from failing. • Ensure that you have the Management Service Account user name and password. • Verify that the **Management Service Account** is a local administrator on each of the target servers.

Requirement	Description
Scheduled Windows updates	Windows allows one MSI to run at any given time. Therefore, verify that the Windows updates are not scheduled to run during the installation.
Download the update package	Download the package from the appropriate location, and extract it to a shared folder on the network (use the update package name).
Prepare the shared folder	Set the update package shared folder as follows: **1** Right-click the folder, and select **Properties**. **2** Click **Sharing**. **3** Click **Advanced Sharing**. **4** Select **Share this folder**. **5** In the Share name field, type the update package name. **6** Click **Permissions**. **7** Click **Add**, and select the **Management Service Account**. **8** In the Allow column, select **Full Control**, and click **OK**. **9** In the Permissions for folder window, and click **OK**.
Installation in hardened environments	If you install the package in a hardened environment, verify that the **Group Policy** is set to **Allow local scripts and remote signed scripts**.

Run the SR Tool

The SR Tool guides you through the steps required to install the update package.

When running remote installations using a local server that is part of the deployment, the update package must be installed on the local server separately from the remote installations.

During installation the server is rebooted one or more times. To perform unattended reboots, the installer configures Windows *AutoAdminLogon*.

If the customer has configured **Legal Notices** to pop-up with *AutoAdminLogon*, the reboot operations require manual acknowledgement of the **Legal Notices**.

Procedure

1. Log on to the local server with the **Installation Service Account**.
2. From the **Start** menu, select **Run** and type:

   ```
   \\<full path of the shared storage location>\Setup.exe
   ```
3. Click **OK**.

   The SR Tool setup checks the local server and if required installs the required components.
4. In the Welcome window, type the user name (domain short name and user name) and password of the **Management Service Account**.

5 Select **Remember My Password**, and then **Apply**.

During the installation process, some alarms are raised as services are restarted and become unavailable. The system acknowledges these alarms (you can ignore them).

Set default user account to access installation files

The SR Tool requires a user account with access rights to the shared folder where the update package installation files exist.

You can set one of the following user accounts:

- Management Service Account
- Installation Service Account

Procedure

1 From the SR Tool menu, select **Tools > Repository Settings**.

The Repository Settings window is displayed.

2 Type the user name (domain short name and user name) and password of the Management or Installation Service Account.

3 Then, click **OK**.

Add remote servers to the network pane

The first time you run the SR Tool, the Network pane only displays the local server. You can install remote servers in a single run of the SR Tool. You can install up to 10 servers in parallel.

You can also add all remote servers at once using the SR_ServerTree_Builder.exe tool.

Procedure

1 From the toolbar, click the **New Machine** icon  .

2 In the **Server Address** field, type the IP address of the remote server to add.

3 Clear the **Use Default User** option.

4 Type the user name (domain short name and user name) and password of the Management Service Account.

5 Click **Add**.

The SR Tool attempts to detect and connect to the remote server, and provides the following indications:

 Connection in process.

 Detection in process.

 The server is ready for installation.

Related topics

Add remote servers using the SR_ServerTree_Builder.exe, page 31

Add remote servers using the SR_ServerTree_Builder.exe

To add multiple remote servers at once to the SR Tool, run SR_ServerTree_Builder.exe on one of the servers configured in the Enterprise Manager.

Procedure

1. Log on to any server in the Enterprise Manager.
2. Open a command prompt.
3. From the root directory of the installation package, run **SR_ServerTree_Builder.exe**.

   The output includes three XML files that you can open from the SR Tool:
   - **Project_All.xml**: Used to install on all servers in the entire enterprise.
   - **Project_DC.xml**: Used to install only on the Data Center servers.
   - **Project_Sites.xml**: Used to install only on the Site servers.
4. From the SR Tool, click **File > Open** and locate the created XML files.
5. Select the required XML file and click **Open**.

Install on multiple servers

You can load machine definitions from a CSV/XML File for installing on multiple servers in a single run.

Procedure

1. Create a CSV file using Notepad or other standard text editor. Enter a list of IP addresses of the required machines in descending rows, with no separator.
2. Right-click **Project** and select **New Site**.

   Site Setup window appears.
3. In the Default Access section, enter user name and password of the Administrator account on the machines and click **Load Machines**.
4. To verify that user credentials are correct, click **Check**.
5. Click **Next** until the Site Progress window appears.
6. To print and verify that all the sites are set up correctly, click **Report**.

Select a server and start the installation

Select the server on the network pane relevant to the update package and start the installation process.

Procedure

1. From the Network pane, select a server to update with the package.

   The server must be ready for installation  .
2. From the Group list, select the relevant package to install.

3 Verify the **Install/Upgrade** option is selected, and then click **Next**.

A Read Me window opens.

4 Select **I Accept** and click **Next**.

The Install Setup page displays the hotfixes relevant to the server.

The default option for **Reboot after completing the installation** is **Yes**.

If you select **No**, it does not disrupt the installation. It enables rebooting the server at the preferred time.

5 Click **Next**.

6 Once the validation is completed without any warnings and the Final Check window appears, click **Next**.

The Ready to Install window displays configuration options enabling you to configure the install process and generate a report.

If a prerequisite or dependency error message appears, follow the message.

7 To configure the install process, select the required options:

- **Display a prompt before restarting the target machine**: To display a prompt for every restart during installation, select this option.
- **Set log level to DEBUG mode**: To provide troubleshooting details in the installation log, select this option.

8 In the report area, select the **platform settings report** option. Click **Browse** to set a location for the report file. The structure of the default file name is IP_platformName_date.html.

9 To start the installation process, click **Install**.

The Platform Progress window opens displaying the installation status and log files for each component.

10 If a Microsoft standard security legal notice opens when restarting the server, click **OK** to continue the installation.

11 If a problem occurs, do the following:

a. Click **Abort**.

The SR Tool completes the installation of the current component and then ends the process. The installation is not completed and the parameter values are not saved.

b. Browse to the following folders:

- <Software Directory Destination>\Software\<component name>\
- \program files(x86)\Server Readiness\Log

c. Compress these folders and send to your contact person.

12 When the installation is completed successfully a confirmation message appears. The computer indication on the left pane displays a green check mark  .

13 Click **Tools > Reports > Full Installation Report**. Enter a file name and destination and save the report. Send the report to your contact person.

14 Restart the servers installed with the package.

15 Verify that this package is installed correctly from Windows Control Panel.

Workflow: Post installation

After completing the installation, perform post installation procedures.

Workflow

1. Install additional KBs on top of HFR , page 19

   If additional standalone KBs are not installed at the same time when HFR is installed, use the Hotfix Deployment Tool to install the additional standalone KBs.
2. Clear cache on Application Servers Cluster, page 33

   On Application Servers Cluster, the cache coherence initializes the current version of the software. After update or removal, to prevent functionality issues, the cache must be cleared on all the Application Servers in the cluster at the same time.
3. Distribute configuration to the Reporting Server, page 33

   The configuration updates due to the package installation must be distributed to the Reports Server.
4. Distribute configuration to Archive Database server role, page 20

   For a successful migration of CENTERA archive, distribute the configuration for Archive Database server role.
5. Disable file upload in coaching, page 34

   To address a security issue, disable uploading file attachments in coaching sessions.
6. Latest Secure Gateway KB installation, page 34

   To avoid potential security risks, install the latest Secure Gateway KB.
7. Service alarms restart, page 21

   If a service restart alarm is raised in the Portal, restart the service in the next scheduled maintenance window.

Clear cache on Application Servers Cluster

On Application Servers Cluster, the cache coherence initializes the current version of the software. After update or removal, to prevent functionality issues, the cache must be cleared on all the Application Servers in the cluster at the same time.

Procedure

1. Stop the **WFOProduction** and **watchdog** services on each of the Application Servers in the cluster.
2. Once the services are stopped on all the Application Servers, start the **WFOProduction** and **watchdog** services one by one on each of the Application Servers.

Distribute configuration to the Reporting Server

The configuration updates due to the package installation must be distributed to the Reporting Server.

Procedure

1. Go to **System Management > Enterprise > Settings**.

2 Select the server hosting the **Reporting Services** server role.

3 In the Description field, type **test** and click **Save**.

Wait 5–10 for the configuration and distribution to complete. When complete, all pending messages must be cleared.

Disable file upload in coaching

To address a security issue, disable uploading file attachments in coaching sessions.

Procedure

1 Add the BPCONFIG key witness/coaching/global/noFileAttachments as follows:

Run this script on the BPMAINDB database server.

```
USE BPMAINDB
IF NOT EXISTS (SELECT 1 FROM BPCONFIG WHERE NAME =
witness/coaching/global/noFileAttachments')
BEGIN
DECLARE @nextkey INT
 EXEC Bp_nextkey 'BPCONFIG', @nextkey output, 1
 INSERT INTO BPCONFIG (ID, NAME, VALUE ) values (@nextkey,
'witness/coaching/global/noFileAttachments','true')
END
```

No need to restart the application service for the BPCONFIG key to take effect.

Latest Secure Gateway KB installation

To avoid potential security risks, install the latest Secure Gateway KB.

If you do not install the Secure Gateway KB, users bypass the logon page and are able to see all test pages. When users try to browse to real pages, they are redirected to the logon page.

The Secure Gateway KB is not included in the update package. Download the Secure Gateway KB zip file from an appropriate location.

Related information

Secure Gateway KB

Update package rollback

If there is a problem with the installation, removing the package is possible at any time.

Procedure

1. Verify that there is connectivity between the Site server and the server hosting WebLogic and database.

   This verification prevents failures of KBs that require such access.
2. Verify that you have the user name and password of the Installation Service Account. Verify that this account is a local administrator on each of the target servers.
3. Log on to the local server as the Management Service Account.
4. For each individual KB that belongs to the update package, open Windows Control Panel and remove each 'Impact360[component name] KBxxxxxx.msi.

   All KBs associated with the update package must be uninstalled.
5. If WLSMon was previously enabled to monitor WebLogic operational status, contact Technical Support to restore this functionality.
6. Stop the **WFOProduction** service on each server. The **WFOProduction** service must be stopped on all application servers before proceeding.
7. Run Command Prompt as Administrator and run the following command:

   `"cscript.exe %IMPACT360SOFTWAREDIR%\WFODeployer\DeployWfo.vbs <WLS Admin> <WLS Admin Password> true true`.
8. Restart the application servers.
9. Restart each target server from which the package was uninstalled.