

**BigFix Remote Control Version
9.1.4 Fix Pack 6 Readme**



Special notice

Before using this information and the product it supports, read the information in Notices.

Edition notice

This edition applies to version 9.5 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

- Chapter 1. About this Fix Pack..... 1**
 - What is New in this Fix Pack..... 1
 - What is New in previous Fix Packs..... 1
 - Fixes included in this Fix Pack..... 5
 - Fixes included in previous Fix Packs..... 5
 - Known problems and limitations..... 7
- Chapter 2. Installation information..... 12**
 - Installing..... 14
 - Post installation tasks..... 18
- Chapter 3. Uninstallation information..... 20**
- Chapter 4. Support..... 21**
- Chapter 5. Notices and trademarks..... 22**
 - Notices..... 22

Chapter 1. About this Fix Pack

This readme file provides important information about Fix Pack 6 for BigFix Remote Control Version 9.1.4.

What is New in this Fix Pack

A summary of changed or new features and enhancements included in BigFix Remote Control V9.1.4 Fix Pack 6.

New version of Liberty Profile

With Fix Pack 6, a new version of WebSphere Application Server 19.0.0.4 Liberty Profile is provided.

macOS 10.15 Catalina support for controller and target components

With Fix Pack 6, macOS 10.15 Catalina operating system is supported for controller and target components.

How to find HCL product installers

To obtain the BigFix Remote Control installation files, access the license portal at <https://HCLSoftware.flexnetoperations.com/flexnet/operationsportal/logon.do>. For more information, refer to the article at https://hclpnpsupport.service-now.com/csm?id=kb_article&sysparm_article=KB0010149

Note:

IBM Passport Advantage® and Fix Central® have been replaced by FlexNet Operations®.

What is New in previous Fix Packs

A summary of changed or new features and enhancements included in Fix Pack 5.

New version of Liberty Profile

With Fix Pack 5, a new version of WebSphere Application Server 19.0.0.1 Liberty Profile is provided.

New Signature for Virtual Smart Card Reader Driver

Fix Pack 5 includes the Virtual Smart Card Reader Driver Version 9.1.5.0500 signed with new certificates.

The certificates used in the Virtual Smart Card Reader Driver Version 9.1.3.0019 will expire on 2019, 26 May.

The existing deployed device drivers will continue to work with the old certificates, however, if you deploy the new Virtual Smart Card Reader Driver or if you upgrade the Remote Control Target to Fix Pack 5, new certificates will be required.

In details, these were the changes performed to support the new certificates:

- In the deployment category New tasks, **Install IBM BigFix Remote Control Certificates for the Virtual Smart Card Reader Driver version 9.1.4.0500** and **Install IBM BigFix Remote Control Virtual Smart Card Reader Driver version 9.1.4.0500 and certificates** can be used to install the driver and the certificates as required.

The new certificates must be installed as follows:

- The `ibm_corporation.crt` file to the Trusted Publishers store
- The `TrustedRoot.crt` and `verisign-universal.cer` files to the Trusted Root Certificate Authorities store
- The tasks installing older versions of the driver and the old certificates are moved to the Maintenance category and are named **Install Certificates for the Virtual Smart Card Reader Driver version 9.1.3.0019, for BigFix Remote Control** and **Install Virtual Smart Card Reader Driver version 9.1.3.0019, for BigFix Remote Control**.

The certificates for version 9.1.3.0019 were installed as follows:

- The `ibm-uk-2016-sha1.cer` and `ibm-uk-2016-sha256.cer` files to the Trusted Publishers store.

- The `verisign-root-g5.cer` and `verisign-universal.cer` files to the Trusted Root Certificate Authorities store.
- The new task **Updated BigFix Remote Control Target with Virtual Smart Card Reader Driver is now available** was added to the update category. You can use this task to update both the Remote Control Target and the Virtual Smart Card Reader Driver. This task will also install the certificates that are needed by the version of the Virtual Smart Card Reader Driver and will remove the certificates that were used in earlier versions of the Virtual Smart Card Reader Driver.
- The **BigFix Remote Control - Virtual Smart Card Reader Driver Status** analysis was modified as follows:
 - It displays now the version of the Virtual Smart Card Reader Driver.
 - It reports the certificate status depending on the Virtual Smart Card Reader Driver version.

Refer to the product documentation for more information.

A summary of changed or new features and enhancements included in Fix Pack 4.

Support of macOS 10.14 Mojave for Controller and Target components

With Fix Pack 4, the support of the macOS 10.14 Mojave operating system was introduced for the Controller and Target components.

A summary of changed or new features and enhancements included in Fix Pack 3.

Search for Offline Targets

To the server user interface, a new function was added to search for targets that are offline since a specified amount of time. From the Target drop-down menu, select Offline. In the panel, enter the period of time specified in days. For example, if you enter 10, all the targets that have not performed a call home in the last 10 days are listed. The list of targets displays the targets that match the indicated criteria.

Shortcut to Open Active Session

To the server user interface, a new function was added to enable you opening an Active Session after selecting the target from the target list. When opening the session with the "Start Active Session link, the policy summary panel is not displayed. Nevertheless, the same policies that are shown with "Start Session" do apply. The Start Active Session link is enabled despite the target status.

A summary of changed or new features and enhancements included in Fix Pack 2.

New version of Liberty Profile

A new version of WebSphere Application Server 17.0.0.4 Liberty Profile is provided.

A summary of changed or new features and enhancements included in Fix Pack 1.

The behavior of file transfer sessions in peer to peer mode has changed for Windows and Linux targets

Up to V9.1.4, when a file transfer session was established in peer-to-peer mode, the permissions used to access the target file system were set to System access on Windows and root access on Linux. With this Fix Pack, the permissions set and used on the target file system are those of the logged on user.

New target configuration options for peer to peer File transfer session permissions

BigFix Remote Control V9.1.4 Fix Pack 1 introduces a new target configuration option to implement the new behavior during file transfer sessions in peer-to-peer mode. When you upgrade to Fix Pack 1, the new **EnableFileTransferSystemAccess** target configuration option is automatically set to No on the target, and the permissions used during the sessions are those of the logged on user. To restore the old behavior on one or more targets, you can change the value to return to the old behavior in one of the following ways:

- By setting the option to "yes" using the target configuration wizard.

- By running Fixlet 102 on Linux, or Fixlet 103 on Windows (Define File Transfer Access to system Files for BigFix Remote Control Targets) on the selected targets.
- By changing the property manually on one or more targets.

The options that you set in the target configuration can be displayed by activating the **Remote Control installation and Security Options** analysis.

See the Known Limitations section for details on issues concerning this new feature.

Fixes included in this Fix Pack

Fix Pack 6 of BigFix Remote Control Version 9.1.4 contains the following fixes:

- APAR IJ15096 - TRC Transfer Mode pop-up window
- APAR IJ16792 - Time Zone in System Info Panel is incorrect
- DA KB0073615 – Web Reports for TRCEvents no longer shown

Fixes included in previous Fix Packs

Fix Pack version of BigFix Remote Control 9.1.4	Fixes
Fix Pack 5	APARS fixed: <ul style="list-style-type: none"> • APAR IJ14428 - Unable to open Controller after upgrade from Fixlet. • APAR IJ14290 - Remote Control Smart Card Reader Driver Certificate Expiration.
Fix Pack 4	APARS fixed: <ul style="list-style-type: none"> • APAR IJ10584 - The parent group policy is not applied to the nested groups.

Fix Pack version of BigFix Remote Control 9.1.4	Fixes
	<ul style="list-style-type: none"> • APAR IJ12152 - After upgrading TRC to 9.1.4 Remote Control session fails with user authentication. • APAR IJ12692 - Broker service keeps crashing. • APAR IJ10691 - Remote Control Vulnerabilities Alerts (Password field with autocomplete enabled).
Fix Pack 3	<p>APARS fixed:</p> <ul style="list-style-type: none"> • APAR IJ07764 - The password reset does not work after receiving the temporary password by email. • APAR IJ07868 - Bigfix Remote Control target component causes NT domain account lockout on single incorrect login. • APAR IJ07910 - The target machine user lost focus when the controller operator uses the Guidance tools. • APAR IJ08131 - The target cannot register to the server through a broker session. • APAR IJ08831 – Preinstalled controller fails to start on Windows 10.
Fix Pack 2	<p>APARS fixed:</p> <ul style="list-style-type: none"> • APAR IJ04289: Incorrect Platform specifications for the Remote Control gateway component • APAR IJ04362: Collaboration controller might fail to start with on demand target sessions.
Fix Pack 1	<p>APARS fixed:</p> <ul style="list-style-type: none"> • APAR IV96402: Display fails to restart when logging out of windows, causing red dialog on controller.

Fix Pack version of BigFix Remote Control 9.1.4	Fixes
	<ul style="list-style-type: none"> • APAR IV97177: Including the BigFix Remote Control Target Installation task in a BigFix baseline with other components causes the task to fail. • APAR IJ00344: Character Ñ in the user name cause controller startup failure. <p>Problems fixed:</p> <ul style="list-style-type: none"> • Remote Control server returns 500 error when resizing columns • LDAP password encryption corrupted when using configuration utility • Using \$ character in password on server causes 500 Internal • With SSO enabled, if the user authenticates correctly but it is not found in the RC DB, the server enters in a loop • Error 403 at initial logon with Smartcard.

Known problems and limitations

Fix Pack version of BigFix Remote Control 9.1.4	Known problems and limitations
Fix Pack 6	<ul style="list-style-type: none"> • When establishing a peer to peer remote session with a macOS 10.15 Catalina <p>After the installation, when a controller connects to the macOS target for the first time, a panel is displayed asking to enable the permissions. The required permissions are: Accessibility and Screen Recording. To enable both permissions you need to establish</p>

Fix Pack version of BigFix Remote Control 9.1.4	Known problems and limitations
	<p>connection to the macOS target twice. If you do not provide the needed permissions, the controller screen does not show the MacOS target desktop.</p>
Fix Pack 5	None.
Fix Pack 4	<ul style="list-style-type: none"> • When establishing a peer to peer remote session with a macOS 10.14 Mojave target in active mode, the target screen is visible but the mouse is not working. <p>This problem is described in the following article: https://support.logitech.com/en_us/article/Logitech-Options-permission-prompts-on-macOS-Mojave</p> <p>To prevent this issue, perform these steps:</p> <ol style="list-style-type: none"> 1. On the mac OS target, open the System Preferences panel. 2. Click Security & Privacy. 3. In the left panel, click Accessibility. 4. Select Click the lock to make changes. 5. Enter the Administrator credentials. 6. On the Privacy tab, select the check box named Remote Control Target. <p>After completing these steps, no target restart is required.</p>
Fix Pack 3	<ul style="list-style-type: none"> • The Preinstalled Controller might fail to start on Windows 10 (Release ID 1709 or higher). This situation might occur also when the operating system is upgraded. <p>To address this problem, the new Fixlet 104 named "TROUBLESHOOTING - APAR IJ08831 Repair pre-installer controller on Windows 10 is available in the Maintenance category. This Fixlet will be relevant on targets that are likely to experience the problem.</p>

Fix Pack version of BigFix Remote Control 9.1.4	Known problems and limitations
	<ul style="list-style-type: none"> • Downloading the on-demand targets (ODT) by using the Firefox plug-in does not complete successfully as the plug-in is not compatible with the latest browser versions. This is because the Firefox browser, starting from Version 57, is unable to install extensions which were not built with the WebExtensions APIs. Only this on-demand target installation method (Firefox plug-in) is affected by the issue. The current workaround is: Install the On-demand targets by using Java Web Start or other on-demand target installation methods. • Some folders or files stored in the <code>C:\Windows\System32</code> directory are not visible during a file transfer session. This problem is caused by the file system redirector which automatically redirects the accesses from <code>%windir%\System32</code> to <code>%windir%\SysWOW64</code> for all 32-bit processes running on a 64-bit platform. The problem applies to the Controller and the Target because they are both running as a 32-bit application (the Controller runs on a 32-bit Java Virtual Machine). This problem is described in the following Microsoft article: https://docs.microsoft.com/en-us/windows/desktop/winprog64/file-system-redirector Both local and remote files during a file transfer session show the path <code>C:\Windows\System32</code> while the real path used is <code>C:\Windows\SysWOW64</code>. As a workaround for this issue, you can access the following hidden folder: <code>C:\Windows\Sysnative</code>

Fix Pack version of BigFix Remote Control 9.1.4	Known problems and limitations
	<p>in order to view the same files and folders structure listed in the command line or displayed in the File Explorer.</p> <ul style="list-style-type: none"> • Open the Controller and connect to the mac OS target. The screen is locked (black) and you cannot take control of the mac OS target. <p>To prevent this issue, perform these steps:</p> <ol style="list-style-type: none"> 1. On the mac OS target, open the Energy Saver panel. 2. Select the check box named Prevent computer from sleeping automatically when the display is off.
Fix Pack 2	<ul style="list-style-type: none"> • When the EnableFileTransferSystemAccess property is set to "no" the file transfer process is started as the logged on user and the File Transfer permissions on the target are inherited from that user. This means that if the logged on user is Administrator (on Windows), root (on Linux) or an equivalent elevated user there are no restrictions on the file system and this is equivalent to having the EnableFileTransferSystemAccess property set to "yes" , and in this case a logged on user is not required. <p>However there is an exception for Windows systems. If the UAC is enabled and the EnableFileTransferSystemAccess property is set to "no", even if the logged in user is an Administrator or an equivalent privileged user (the file transfer process is owned by that user) then the permissions inherited are those of a normal user. This means that folders and files which requires administrative privileges are not either writable or readable.</p> <p>This is because the UAC prevent every process owned by whatever user from gaining elevated privileges unless the user itself explicitly start the process and request elevated privileges. This imply an interaction with the windows UI system. Depending on the UAC</p>

Fix Pack version of BigFix Remote Control 9.1.4	Known problems and limitations
	settings the UI ask the user to provide acceptance for the operation and in some cases also the credentials of an administrative user. Since the file transfer process is started automatically and there is no interaction with the target machine operator, when the UAC is enabled the file transfer process is always started with unprivileged permissions.

For other known issues and limitations, see the Release Notes in the BigFix Remote Control 9.1.4 Knowledge Center: https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Rel_Notes/release_notes_914FP1.html

Chapter 2. Installation information

Read the following sections before you install BigFix Remote Control Version 9.1.4 Fix Pack 6.

Prior to installation

Installing the fix pack after installing the version 9.1.4 GA level (9.1.4.0052)

If you are installing the fix pack immediately after installing the version 9.1.4 GA Level (9.1.4.0052), log on to the GA Level application after it has installed to ensure that the database initialization has completed before applying the fix pack.

 **Note:** It is not necessary to install the GA version prior to installing this fix pack.

Back up your properties and recordings files

If you have the server component installed and running you must backup your existing property files before installing the fix pack and also backup any recordings files that you have.

Back up the following property files:

- common.properties
- ldap.properties
- trc.properties
- controller.properties
- log4j.properties
- ondemand.properties

These files are found in the following path for Windows based systems:

```
[TRCInstallDir]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF  
\classes\
```

These files are found in the following path for Unix based systems :


```
[TRCInstallDir]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/
classes/
```

where [TRCInstallDir] is the BigFix Remote Control Server installation directory.

The video recordings folder is defined in the rc.recording.directory property in the trc.properties file. The default locations are:

In manual Installations on Windows:

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\rc_recordings
```

In automated Installations:

- In Linux: [TRCInstallDir]/wlp/usr/servers/trcserver/rc_recordings
- In Windows: [TRCInstallDir]\wlp\usr\servers\trcserver\rc_recordings

Back up any certificate files

This step is necessary only if you have previously manually installed a certificate. It applies only to an automated server installation.

The certificates are stored by default in a keystore file **key.jks** in the following paths:

- Windows:

```
[TRCInstallDir]\wlp\usr\servers\trcserver\resources\security\key.jks
```

- Linux:

```
[[TRCInstallDir]/wlp/usr/servers/trcserver/resources/security/key.jks
```

If the default keystore file location or keystore password are changed, also back up the file **memory.xml** stored in the following paths:

- Windows:

```
[TRCInstallDir]\wlp\usr\servers\trcserver\memory.xml
```

- Linux:

```
[TRCInstallDir]/wlp/usr/servers/trcserver/memory.xml
```

Installing

Although it is not required, it is suggested that when you apply a fix pack that you upgrade all of your components to the latest level.

BigFix Remote Control 9.1.4 Windows Server Installation with a WebSphere Application Server 17.0.0.4 Liberty Profile

1. Decompress 9.1.4-TIV-IBRC914-WIN-IF0006.zip and navigate to `trc_server_setup.exe`
2. Run `trc_server_setup.exe`
3. Follow the instructions displayed on your screen to install the fix pack
4. If more detailed information is required, refer to the BigFix Remote Control Installation Guide and the chapter that describes installing the server using the server installer:
https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_server_installer.html

BigFix Remote Control 9.1.4 Linux Server Installation with a WebSphere Application Server 17.0.0.4 Liberty Profile

1. Untar 9.1.4-TIV-IBRC914-LINUX-IF0006.tar and navigate to `trc_server_setup.bin`
2. Run `trc_server_setup.exe`
3. Follow the instructions displayed on your screen to install the fix pack
4. If more detailed information is required, refer to the BigFix Remote Control Installation Guide and the chapter that describes installing the server using the server installer:
https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_server_installer.html

Manual Installation

If you are using 9.1.4-TIV-IBRC914-MULTI-IF0006.tar to perform a manual installation of this release, note:

A manual installation can only be performed on a system that has the previous release of BigFix for Remote Control already installed.

The following sections describe the different manual installations.

BigFix Remote Control 9.1.4 WebSphere Application Server (WAS), AIX, Linux, Solaris and Windows Server Installation

 **Important:** Back up your video recordings and customized properties files

Untar 9.1.4-TIV-IBRC914-MULTI-IF0006.tar and navigate to \Disk1\InstData\[platform]\VM where [platform] is relevant to your operating system. For example:

```
\Disk1\InstData\windows\VM
```

- AIX: Run `trc_additional_setup.bin`
- Linux: Run `trc_additional_setup.bin`
- Solaris: Run `trc_additional_setup.bin`
- Windows: Run `trc_additional_setup.exe`


For AIX, Linux, and Solaris:

1. Run `trc_additional_setup.bin`.
2. Follow the instructions in the BigFix Remote Control Installation Guide in the chapter that describes how to extract the component installation files: https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst-addiitional_install.html

The new war file will be saved to a place of your choice or the InstallAnywhere default location.

3. Use the WAS Administrative Console to update the war file.

4. Follow the steps in the Post installation section to perform the necessary tasks after the installation.

 **Note:** After a manual installation of the BigFix Remote Control Server on an AIX system, the default admin id and password are case sensitive and should be typed as follows :

```
id = Admin          password = password
```

For Windows:

1. Run trc_additional_setup.exe.
2. Follow the instructions in the BigFix Remote Control Installation Guide in the chapter that describes how to extract the component installation files.
https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst-addiitional_install.html. The new war file will be saved to a place of your choice or the InstallAnywhere default location.
3. Use the WAS Administrative Console to update the war file.
4. Follow the steps in the Post installation section to perform the necessary tasks after the installation.

Component Installation

For more information about installing the components, see https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_comp_install.html

Windows components:

1. Unzip 9.1.4-TIV-IBRC914-WIN-IF0006.zip
2. Use the relevant installation files to install the components.
 - **Target:** `trc_target_setup.exe` or `trc_target.msi`
 - **Controller:** `trc_controller_setup.exe` or `trc_controller.msi`
 - **Gateway:** `trc_gateway_setup.exe` or `trc_gateway.msi`
 - **Broker:** `trc_broker_setup.exe` or `trc_broker.msi`
 - **CLI:** `trc_cli_setup.exe` or `trc_cli.msi`

Linux components:

1. Extract the additional setup utility file from 9.1.4-TIV-IBRC914-MULTI-IF0006.tar
2. Run the file that is relevant to the operating system that you will run the utility on. See the installation guide for a description about how to extract the component installation files:

https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst-addiitional_install.html

3. Use the following files to install the components.

- **Target:** `ibm-trc-target-9.1.4.i386.rpm` or `ibm-trc-target-9.1.4.src.rpm`
- **Controller:** `ibm-trc-controller-9.1.4.noarch.rpm` and `ibm-trc-controller-jre-9.1.4.i386.rpm`
- **Gateway:** `ibm-trc-gateway-9.1.4.i386.rpm` or `ibm-trc-gateway-9.1.4.src.rpm`
- **Broker:** `ibm-trc-broker-9.1.4.i386.rpm` or `ibm-trc-broker-9.1.4.src.rpm`
- **CLI:** `ibm-trc-cli-9.1.4.i386.rpm` or `ibm-trc-cli-9.1.4.src.rpm`

4. Restart the component service for the component that you upgraded. For more information about restarting the component services, see the BigFix Remote Control Installation Guide:

https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_manage_linux_comps.html

BigFix Console Installation

You can use the BigFix Console to deploy the upgraded version of BigFix Remote Control. The Fixlets are available on Remote Control site 55.

The Update node in the Remote Control navigation tree provides two sub-nodes which are operating system specific. These sub-nodes provide the latest levels of the target, controller, CLI and gateway components. If you have an older version of the BigFix Remote Control components already installed in your environment, you can use the Update node to upgrade these components to a newer version.

To upgrade the server component you can create and run a new server installation task by using the BigFix Remote Control Server Installer Wizard.

See the BigFix Remote Control Console Users Guide in the BigFix Remote Control Knowledge Center and the section that describes creating the server installation tasks.

https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_TEMUser_Guide/rcusrmanageconfig.html


Post installation tasks

Complete one or more of these tasks after installation completes, depending on your configuration.


Edit the properties files

After completing the update and confirming that 9.1.4.0210 is installed, edit the new trc.properties and ldap.properties files and update them with the values in your saved files.

Restore your other saved properties files and video recordings.

 **Note:** It is only necessary to update the properties files after a manual upgrade or if the properties files have not been successfully restored after an automated upgrade.

Restore Certificate files

 **Note:** This section should only be carried out if you have previously manually installed a certificate. It also only applies to an automated BigFix Remote Control server installation.

Restore the saved keystore file key.jks. If using the default keystore, it must be restored to:

Windows

```
[TRCInstallDir]\wlp\usr\servers\trcserver\Resources  
\security\key.jks
```

Linux

```
[TRCInstallDir]/wlp/usr/servers/trcserver/resources /  
security/key.jks
```

If the password or the location of the keystore were changed, modify the file `memory.xml` and set the parameters of the element `<keyStore>` with the same values as the `memory.xml` file that was backed up as instructed previously.

The `memory.xml` file can be found at:

Windows

```
[TRCInstallDir]\wlp\usr\servers\trcserver
```

Linux

```
[TRCInstallDir]/wlp/usr/servers/trcserver
```

Chapter 3. Uninstallation information

Read the following sections to uninstall this fix pack.

Uninstallation Steps

To uninstall this fix pack, perform the following steps:

1. Back up and save your properties files. These files are located in the following directories:

- **Windows based systems:** `[TRCInstallDir]\wlp\usr\servers\trcserver\apps\ TRCAPP.ear\trc.war\WEB-INF\classes\`
- **UNIX based systems.**`TRCInstallDir]/wlp/usr/servers/trcserver/apps/ TRCAPP.ear/trc..war/WEB-INF/classes/`

where `TRCInstallDir` is the BigFix Remote Control server installation directory.

2. Back up your database by following the standard procedure as documented by your database provider.
3. Uninstall the BigFix Remote Control Server. To uninstall the Server, complete one of the following steps:
 - a. Within Add/Remove programs select to Uninstall BigFix Remote Control - Server
 - b. Run the uninstall application:

Run the `Uninstall BigFix Remote Control-Server.exe` file which can be found in the BigFix Remote Control server installation directory.
4. Install the previous version of BigFix Remote Control.

For installation instructions, see the BigFix Remote Control Installation Guide: https://help.hcltechsw.com/bigfix/9.5/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_introduction.html

5. Stop the BigFix Remote Control service.
6. Restore your properties files and database.
7. Start the BigFix Remote Control Service.

Chapter 4. Support

For more information about this product, see the following resources:

- [BigFix V9.5 Lifecycle Documentation](#)
- [HCL Software Support](#)
- [HCL portal for BigFix Support](#)
- [BigFix Developer](#)
- [IBM BigFix Wiki](#)
- [BigFix Forum](#)

Chapter 5. Notices and trademarks

The following section includes important information about this document and its use.

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.