

**BigFix Remote Control
Version 10 Fix Pack 7 Readme**



Contents

- Chapter 1. About this Fix Pack..... 1**
 - What is new in this Fix Pack..... 1
 - What is new in previous Fix Packs..... 2
 - Fixes included in this Fix Pack..... 9
 - Fixes included in previous Fix Packs..... 10
 - Known problems and limitations..... 11
- Chapter 2. Installation information..... 21**
 - Installing..... 23
 - Post installation tasks..... 27
- Chapter 3. Uninstallation information..... 29**
- Appendix A. Support..... 30**
- Appendix B. Notices and trademarks..... 31**
 - Notices..... 31

Chapter 1. About this Fix Pack

This readme file provides important information about Fix Pack 7 for BigFix Remote Control Version 10.0.0.

What is new in this Fix Pack

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 7.

Managed mode support for macOS target

This feature adds the support for macOS targets in Managed mode. With this feature macOS targets now support the full set of Remote Control session capabilities (managed, peer-to-peer, unattended and on-demand).

The Remote Control target creates the status icon on the Menu bar at the top of the screen instead of the icon on the Dock as in previous releases.

For a better user experience when establishing sessions with macOS targets, it is recommended to use a Remote Control Controller of version 7 or higher.

Apple M1 architecture support for macOS target

This feature provides support for Apple M1 architecture. Both architectures use the same package and tasks to deploy the Remote Control target.

Enhancements to target group assignments

It is possible to assign targets to target groups by using the *GroupLabel* target parameter thus letting the target define the target groups it belongs to.

This assignment can occur during initial target registration or during subsequent target triggered call homes. To enable the GroupLabel processing during initial target registration set the `allow.target.group.override` to Yes.

To enable the GroupLabel processing during triggered call homes set the `allow.override.at.triggered.callhomes` to Yes. Both properties are in the `trc.properties` file on the server. It is not possible to remove Target group assignment using the GroupLabel parameter.

The *GroupLabel* parameter can include a list of groups separated by “;” like Group1;Group2.

Deployment Status Dashboard Enhancements

A new widget on the Deployment Status Dashboard allows to monitor certificate expirations. By default the widget shows expiration of Broker certificates loaded in the “Trusted Certificates” of the server. When using CA signed certificates the widget will show the expiration date of the Broker root certificate. You can use the Add Certificate button to also add the actual broker certificate or the actual Remote Control Server certificate to better track the overall environment certificate expiration.

Update of WAS Liberty and IBM Java

IBM WAS Liberty version is 22.0.0.10 and IBM Java SDK 8.0-SR7-FP16 is used in this product update.

Withdrawal of license verification

Remote Control no longer provides a feature to verify compliant product licensing. To verify product compliance please refer to the appropriate pages of the BigFix console. The Admin -> Licensing page is no longer available.

What is new in previous Fix Packs

What's new in Fix Pack 6

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 6.

Adoption of WAS Liberty in place of Open Liberty

IBM WAS Liberty version 21.0.0.12 is used in this product update.

Changes in Java Adoption

- Adoption of the 64-Bits IBM Java SDK on Windows and Linux Remote Control Servers in place of the 32-Bits.
- Adoption of IBM Semeru Runtime Open Edition JRE on Windows, macOS and Linux Remote Control Controllers.
- Adoption of a 64-Bits JRE on the Linux Controller.

Adoption of Bouncy Castle JCE FIPS Provider

The Bouncy Castle JCE FIPS Certified provider is used on Windows, macOS and Linux Remote Control Controllers.

This enhancement enables the Controller on macOS to operate in FIPS compliance.

Adoption of log4j version 2

The log4j has been upgraded to version 2.17.1. The Remote Control Server is the only product component that uses log4j.

Deployment Status Dashboard Enhancements

A new widget on the Deployment Status Dashboard allows to monitor error conditions on the Remote Control Server Application.

What's new in Fix Pack 5

A summary of changed or new features and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 5.

Unattended Target Support

The Unattended target support is a product feature that allows you to take remote control sessions of targets that are connected through a Broker without the need to provide a connection code. In strict remote control terminology, an Unattended target is a Managed target that performs call home through a Broker.

New Deployment Status Dashboard

This new dashboard provides a real time view of the brokers health and activity history. The Dashboard is activated by default when operating with

unattended targets, but can be configured to monitor On Demand and Broker Sessions history.

What's new in Fix Pack 4

A summary of changed or new features and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 4.

Enhanced LDAP synchronization

By default, an LDAP synchronization is performed at every system startup and at every scheduled.interval after that. A synchronization is also performed every time a Reset Application is performed. It is now possible to better control the execution of the LDAP Synchronization task by using the following properties in the **common.properties** file.

```
sync.LDAP.at_reset_application=true
```

Description: Use to enable or disable the LDAP synchronization when the reset application is performed

Values: True/False. Default is True

Definition: When set to False the LDAP synchronization is not performed.

```
sync.LDAP.task_run_days=0
```

Description: Use to enable a fixed time synchronization. The value indicates the frequency in days of the synchronization

Values: Number of days. Default is 0

Definition: 0 - fixed time synchronization is disabled, and the synchronization occurs every scheduled.interval instead

n - Days in interval. 1 for daily

```
sync.LDAP.task_run_time=00:00:00
```

Description: Use to indicate the time of the day a fixed time synchronization has to occur

Values: 24 hours notation of the time in HH:MM:SS

Definition: For Example 02:00:00 to perform the synchronization at 2 AM



Note: When using `usingsync.LDAP.task_run_time` the actual task execution time is affected by the `scheduled.interval` setting, as the ldap synchronization occurs within the context of the task scheduler. The actual execution time can span from `sync.LDAP.task_run_time` to `sync.LDAP.task_run_time + scheduled.interval`



Note: The server must be restarted to use fixed time synchronization.

TLS Configuration Hardening

Effective from this release the TLS 1.2 protocol is the default protocol used by the product.

Support for TLS 1.2 protocol was added in BigFix Remote Control version 9.1.2 IF0001 (Build number 9.1.2.0113) released 17th March 2016. The TLS 1.2 protocol version was never enforced in Remote Control up to this release for backward compatibility reasons.

With this release, all components of Remote Control (fresh install or upgrade) communicate using TLS 1.2 protocol. There are no backward compatibility issues assuming you are operating the product at least at 9.1.2.0113 version or later.

Customers operating at an earlier version than 9.1.2.0113 should plan to upgrade their environment starting from the Remote Control Server first.

The following exceptions apply:

- **Remote Control Server** that is not configured to operate in FIPS mode is still configured with the default `sslProtocol="SSL_TLSv2"` after a fresh install or upgrade. The value `SSL_TLSv2` in the `ssl.xml` enables TLS v1.0, v1.1, and v1.2 protocols. You can manually change this value to `"TLSv1.2"`. In this case all other components that the Remote Control server communicates with must be configured to support TLS 1.2 (LDAP Servers, Database Server, Mail Servers). Please also note that in a follow on release the default configuration value for the server will be changed to `"TLSv1.2"` at install or upgrade time. If the server is configured to operate in FIPS mode the value is set already to `"TLSv1.2"`.
- **Remote Control Brokers** that are configured with one or more of the following properties `DefaultTLSCipherList`, `DfaultHTTPSCipherList`, `<prefix>.TLSCipherList` and `<prefix>.HTTPSCipherList` where `<prefix>` is the connection prefix used, comment the properties in question to activate the new default TLS 1.2 enforcement.

Support for MS/SQL 2019 and DB2 11.x

These databases are now included among the list of Remote Control supported Databases.

Support for MacOS up to 11.3

Version 11.3 of MacOS is now listed among the list of supported MacOS Platforms.

What's new in Fix Pack 3

A summary of changed or new features and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 3.

License verification

Remote Control introduces a feature to verify licensing, wherein it retrieves license information from BigFix Server and indicates the user if there is any license non-compliance. In case of non-compliance, there is no enforcement with this release, and the product operates normally with warning

messages issued on the user interface to take further action as necessary. It also provides the possibility to update licensing information to avoid noncompliance.

Database cleanup

It is now possible to automatically remove offline targets from the database. As the number of targets present in the database is a factor to determine license compliance, it is important to clean up the database periodically. By default, this process runs every 24 hours to perform database cleanup. Cleanup is hooked to dbcleaner process and controlled by the target.offline.max.age property in trc.properties. With this, you can configure if you want to perform automatic offline target cleanup or can also indicate in days for how long an offline target can be kept in the database.

Flash removal from BigFix Dashboards

The Remote Control BigFix Console Content has been updated to remove any dependency on Adobe Flash. Target Configuration Wizard is enhanced to allow single property selection in the configuration update task. You can notice the effect of the improved behavior when importing settings from a previously submitted task. When the task is imported, values that were changed are taken from the task, while the others appear as enabled for change. Select or de-select the properties as needed.

Mouse Wheel support

With mouse wheel support, you can control the mouse pointer and scroll the views displayed on a remote computer, when a remote control session is in place.

Adoption of Open Liberty in place of IBM Liberty

IBM Liberty is replaced with Open Liberty. The adopted OpenLiberty version is 20.0.0.10.

Removal of support for RH 5 and Windows 2008

Remote Control stopped supporting RH 5 and Windows 2008 from Fix Pack 3 release.

What's new in Fix Pack 2

A summary of changed or new features and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 2.

Lite Web Portal

With Fix Pack 2, Remote Control provides a solution where you can open a remote session with an On Demand Target (ODT), without using a VPN, even when the controller and the target are over Internet. This specifically addresses the VPN overloading challenge with Work From Home scenario. For more information, see Lite Web Portal.

Improved user experience while starting ODT on macOS Catalina

Before Fix Pack 2, starting from macOS Catalina (10.15), to use the ODT and to start a remote session, the user had to manually change the execution permission of the downloaded files by executing some OS level commands. With Fix Pack 2, Remote control provides a new type of ODT package for macOS. When enabled, this package allows the user to temporarily install the ODT and execute the session without manually changing the execution permission.

What's new in Fix Pack 1

A summary of changed or new features and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 1.

Session Mode support for macOS

With Fix Pack 1, Chat Session Mode and Guidance Session Mode are now supported for macOS Targets. It is also possible to use the Chat function while in session.

Enter Connection Code dialog

A new programmable interface is added to the Remote Control Target to facilitate the operations surrounding the “Enter Connection Code” target dialog function.

More control over Proxy configuration in Controller

The controller uses the proxy defined at system level by default. In some conditions, this may not be desirable. Creating a file named “override.proxy” in the controller install folder changes the default behavior and the system proxy is ignored.

Fixes included in this Fix Pack

Fix Pack 7 of BigFix Remote Control Version 10.0.0 contains the following fixes:

- KB0100656: Managed mode controller connection fails
- KB0099719: Unable to connect when system proxy is used
- KB0099404: High CPU load of Broker on RHEL 8
- KB0099153: Issues in "Configuring the server for single sign-on after installation" topic
- KB0099081: Connection not secure message on browser
- KB0098999: Incorrect documentation for log4j.logger.com.bigfix
- KB0098983: Missing information in certificate install documentation
- KB0098732: Compressed option for recording export function failing
- KB0098501: Controller messages with Thai Language are not working
- KB0098495: Target crashing because of PAC file processing failure
- KB0098341: Error using untrusted certificate when installing
- KB0089204: Remote Control may fail to retrieve license information from the BigFix License Server
- KB0100548: Target machine cannot rejoin existing broker session

Fixes included in previous Fix Packs

Fixes included in Fix Pack 6

- KB0096571: Default target group assignment may reset on rules computation
- KB0095998: Page may timeout on large reports
- KB0095702: Server SSO - Update errorPage.jsp
- KB0094397: Update supported browsers versions from installation manual
- KB0090982: Action on filtered targets or user is applied to ALL items
- KB0084756: Disabling of command menu entries may be lost on session mode change
- KB0097233: Certificate Import (New Trusted Certificate) fails with internal server error 500

Fixes included in Fix Pack 5

Fix Pack 5 of BigFix Remote Control Version 10.0.0 contains the following fixes:

- KB0090147 - Broker service stopping due too many open sessions
- KB0092788 - Remote Control Server Verion10 FP4 upgrade or Install hangs at 89%
- KB0088343 - BigFix Remote Control search issue

Fixes included in Fix Pack 4

Fix Pack 4 of BigFix Remote Control Version 10.0.0 contains the following fixes:

- KB0086512 - Application Reset may cause a series of unnecessary LDAP Synchronizations
- KB0087383 - Controller Install / Upgrade task may fail
- KB0086742 - Remote Control upgrade installer cannot connect to the SQL database
- KB0088685 - Missing signature for Windows OnDemand target executable

Fixes included in Fix Pack 3

There are no fixes included in Fix Pack 3

Fixes included in Fix Pack 2

Fix Pack 2 of BigFix Remote Control Version 10.0.0 contains the following fixes:

- KB0081758 – “BigFix Remote Control” entry in the right click menu is grayed-out for macOS computers
- KB0081193 – Update browsers versions list in Install Guide
- KB0081018 – The Controller is not associated with .trjws files on macOS
- KB0081017 – V10 java signed jars lack intermediate certificates

Fixes included in Fix Pack 1

Fix Pack 1 of BigFix Remote Control Version 10.0.0 contains the following fixes:

- KB0078748 – Broker session does not start with user name containing special chars
- KB0079215 – During On Demand remote control session desktop background is permanently removed if set in policy
- KB0079778 – Controller can not start a Broker connection in presence of a proxy server
- KB0079998 – How to bypass UAC prompt (Doc)


Known problems and limitations

Fix Pack version of BigFix Remote Control V10.0.0	Known problems and limitations
Fix Pack 7	<ul style="list-style-type: none"> • Export function in compressed form (.avi) does not work if the display resolution of the target at the time of recording is not a multiple of 4 <p>The screen resolution of the target at capture time must be in sizes of multiples of 4 pixels. This restriction comes from the JMS encoder. To resolve this issue, change the screen resolution of the target to 1920 x 1080.</p>

Fix Pack version of BigFix Remote Control V10.0.0	Known problems and limitations
	<ul style="list-style-type: none"> <p>• macOS Managed Support – Clipboard functions disabled</p> <p>Security settings on the macOS platform do not allow a process running in the background to access the clipboard. For this reason, the clipboard functions icon on the controller is currently disabled.</p> <p>To transfer text from/to the target, you can use the chat function that shows the text clearly.</p> <p>• macOS Managed Support – Open file transfer folder</p> <p>The in session file transfer folder for macOS target is created under the user folder <code>/Users/<user>/File Transfer</code>.</p> <p>The function to open this folder from the target GUI, or from the controller file transfer menu icon during an active session does not work on recent macOS versions.</p> <p>You can access the file transfer folder by opening Finder. You can set Finder > Preferences > Side Bar and add the user home folder to favorites. You can then easily access the file <code>File Transfer folder</code> by simply opening Finder.</p> <p>• macOS Managed Support – File Transfer Session Mode Limitations</p> <p>During a File Transfer Session, access to some target folders may be limited. For example, some user-level folders such as Downloads, Documents, and Pictures are not accessible from the File Transfer Controller interface. This is because the process responsible for listing those folder content on the target is not allowed to list the content of those folders.</p>

Fix Pack version of BigFix Remote Control V10.0.0	<p style="text-align: center;">Known problems and limitations</p>
	<p>At the same time, it is possible to transfer files from the controller to those folders as the file transfer process on the target operates under the user's authority.</p> <ul style="list-style-type: none"> • macOS Managed Support – Switch user or Logoff <p>If the user is logged off during an active session, sometimes (depending on the processor speed) the target screen capture process fails to capture the login screen. In this event, the Controller screen will show a still background image.</p> <p>You can recover from the situation by selecting another session mode from the controller drop-down menu (for example File Transfer) and then switching back to Active session mode.</p> <ul style="list-style-type: none"> • macOS Managed Support – Remote Control Icon on the DOCK after upgrade <p>The Remote Control target upgrade from the earlier version may leave the Remote Control target icon on the Dock bar.</p> <p>The icon is no longer used and the user can remove it by clicking the icon and selecting Options > Remove from Dock.</p> <p>The new version of the Remote Control target creates the status icon on the Menu bar at the top of the screen.</p> <ul style="list-style-type: none"> • macOS Managed Support – Start of target process as user <p>If there is no Remote Control process running, clicking on the Remote Control Target application icon on the Launchpad causes the target to start under the user authority instead of the root authority.</p>

Fix Pack version of BigFix Remote Control V10.0.0	Known problems and limitations
	<p>To stop this target process, use the kill command or reboot the system.</p> <ul style="list-style-type: none"> • KB0100656 - Support hostname in Managed Mode trcjws connections <p>When it is necessary, you can also use the target host name in the <code>.trcjws</code> file instead of the IP address. A new property <code>trcjws.use.target.hostname</code> has been added to the <code>trc.properties</code> file on the server to control the <code>.trcjws</code> content.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> ◦ 0 (zero) - No host name addition (Default) ◦ 1 - Add the host name to the IP address ◦ 2 - Host name Only <ul style="list-style-type: none"> • KB0098501: Chat messages in Thai Language is not working <p>Under certain circumstances, Thai text is not showing properly in the controller chat window. This occurs because of a miss configuration of the Thai language in the Open JDK that was adopted by Remote Control Controllers starting from Fix Pack 6.</p> <p>To remediate the problem, complete the following steps:</p> <ol style="list-style-type: none"> 1. Navigate to the <code>lib</code> folder of the controller JRE located in <code>C:\Program Files (x86)\BigFix\Remote Control\Controller\jre\lib</code> 2. In the <code>lib</code> folder, there is a file named <code>fontconfig.properties.src</code>. Make a copy of this file and name it as <code>fontconfig.properties</code>.

<p>Fix Pack version of BigFix Remote Control V10.0.0</p>	<p style="text-align: center;">Known problems and limitations</p>
	<p>3. Edit the <code>fontconfig.properties</code> file:</p> <ul style="list-style-type: none"> ◦ Set <code>allfonts.thai=Tahoma</code>. <i>Tahoma</i> font is better suited to show Thai characters than <i>Lucida Sans Regular</i>. <p>You can also use your own Thai font if you so desire, in this case, create a folder named <code>fonts</code> in the <code>lib</code> folder and copy your <code>.ttf</code> or <code>.otf</code> font file, then use the proper font name in the <code>allfont.thai</code> property.</p> <ul style="list-style-type: none"> ◦ Add Thai language by setting <code>sequence.allfonts=alphabetic/default,dingbats,symbol,thai</code> <p>4. Save the <code>fontconfig.properties</code> file.</p> <p> Note: The <code>fontconfig.properties</code> file is preserved in case of controller upgrades.</p>
<p>Fix Pack 6</p>	<ul style="list-style-type: none"> • KB0095998: Page may timeout on large reports <p>When running the All Target query with a large row per page, the page load may timeout because of the amount of data that is loaded. To mitigate the issue a new query named <code>All Targets (Slim Output)</code> has been added.</p> <p>To use the Slim Output query, as the default homepage you can edit the <code>trc.properties</code> file and change the default.query property from 251 to 255.</p> <p>Alternatively, you can define a custom report to tailor the query and then assign the new query as the default home-</p>

Fix Pack version of BigFix Remote Control V10.0.0	<p style="text-align: center;">Known problems and limitations</p>
	<p>page for the user groups of choice. After the log in, you can return to the default homepage by clicking on the HCL icon on the left of the menu bar.</p>
Fix Pack 5	None known.
Fix Pack 4	<ul style="list-style-type: none"> • Browser or Controller connection with the Remote Control server may fail <p>If the server is configured to operate in FIPS mode with the following exception in the messages.log file <code>java.lang.NullPointerException com.ibm.ws.channel.ssl.internal.SSLConnectionLink 238</code>, Browser or Controller connection with the Remote Control server may fail.</p> <p>This is a side effect of the adoption of IBM Java 8.0.6.26. If the issue persists, do the following:</p> <ol style="list-style-type: none"> 1. Stop the Remote Control Server. 2. Open the <code>..\TRC\java\jre\lib\security\java.security</code> file and add the RSAPSS value as the last entry of the <code>jdk.tls.disabledAlgorithms</code>. <p>The updated property list should look as follows:</p> <pre>jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5with-RSA, DH keySize < 1024, DESede, \ EC keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC, RSAPSS</pre> <ol style="list-style-type: none"> 3. Start the Remote Control Server. <ul style="list-style-type: none"> • The Join Broker Session operation may fail <p>When the secondary controller connects to the primary controller and the environment is configured to operate in FIPS mode, the Join Broker Session operation may fail. The prima-</p>

Fix Pack version of BigFix Remote Control V10.0.0	<p style="text-align: center;">Known problems and limitations</p>
	<p>ry controller may show an exception like the foll following exception in the messages.log file:</p> <pre style="background-color: #f0f0f0; padding: 10px;">SEVERE - The connection was refused with pkt type [260]</pre> <p>This is a side effect of the adoption of IBM Java 8.0.6.26. If the issue persists, do the following:</p> <ol style="list-style-type: none"> 1. Open the <code>..\Controller\jre\lib\security\java.security</code> file and add the <code>RSAPSS</code> value as the last entry of the <code>jdk.tls.disabledAlgorithms</code>. The updated property list should look as follows: <code>jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, DESede, \ EC keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC, RSAPSS</code> <ul style="list-style-type: none"> • The playback of a session recording via the Server Web Interface may fail to start with no error message shown if the Server is Configured to operate in FIPS mode <p>This is a side effect of the adoption of IBM Java 8.0.6.26. If the issue persists, do the following:</p> <ol style="list-style-type: none"> 1. Save the <code>TRCPlayer.trcjws</code> file as provided by the server. 2. Edit the File and remove the line <code><argument>--force-fips</argument></code> 3. Save the file and execute the <code>TRCPlayer.trcjws</code> file by clicking on it.

Fix Pack version of BigFix Remote Control V10.0.0	Known problems and limitations
Fix Pack 3	<ul style="list-style-type: none"> <li data-bbox="532 447 1260 478">• Unable to initialize SSL connection in messages.log <p data-bbox="553 516 1390 653">When using Chrome or Edge chromium and the RC Server has a self-signed certificate, you may notice error messages in the messages.log</p> <p data-bbox="553 684 1382 873">“CWWKO0801E: Unable to initialize SSL connection. Unauthorized access was denied or security settings have expired. Exception is javax.net.ssl.SSLException: Received fatal alert: certificate_unknown”</p> <p data-bbox="553 905 1377 1041">From the Browser you may experience a certificate validation error of :ERR_CERT_AUTHORITY_INVALID or :ERR_CERT_COMMON_NAME_INVALID.</p> <p data-bbox="553 1073 1386 1314">To use a self-signed certificate with those browsers, make sure the self-signed certificate defines fully qualified host name as Common Name, and specify a valid Subject Alternate Name. In addition, add the certificate to the Root Trusted Certificates store of the client machine.</p> <ul style="list-style-type: none"> <li data-bbox="532 1377 1377 1461">• Issues in visualizing Webreports after upgrading to Fix Pack 3 <p data-bbox="553 1493 1349 1890">In FixPack 3, the Remote Control BigFix Console Content has been updated to remove any dependency on Adobe Flash. Also, "Tivoli Remote Control" site has been re-branded to "Remote Control". Therefore, corresponding webreport was renamed from <code>TRCEvents.beswrpt</code> to <code>RCEvents.beswrpt</code>. This can cause a problem in the webreports, as this cannot find <code>TRCEvents.beswrpt</code> in the Tivoli Remote Control directory.</p>

Fix Pack version of BigFix Remote Control V10.0.0	<p style="text-align: center;">Known problems and limitations</p>
	<p>Do the following to address this issue:</p> <ul style="list-style-type: none"> ◦ Check if analyses 6, 12 and 20 in Remote Control site are activated and restart WebReports service. ◦ If you are using Internet Explorer, set at least Emulation 10 after cleaned up the browse cache. ◦ Try with a different browser. <p>If the issue still persists, do the following:</p> <ol style="list-style-type: none"> 1. Stop the WebReports service. 2. Rename the folder "Tivoli Remote Control" under the SiteData folder (complete path: <code>C:\Program Files (x86)\BigFix Enterprise\BES Server\BESReportsServer\wwwroot\SiteData\<BES Server FQDN>\Sites\Tivoli Remote Control</code>). 3. Start the Web Reports service
Fix Pack 2	<ul style="list-style-type: none"> • Lite Web Portal with pre-installed Controller Only <p>For performance and security reasons, it is required to use a pre-installed controller to start a remote session through Lite Web Portal. This is because, it is not advisable to download trc_console.jar at runtime over the internet.</p> <ul style="list-style-type: none"> • Single Sign-on (SSO) for Lite Web Portal is not supported in this release <p>An SSO log on session via SAML2 requires the web browser to see both the TRC Server and the Identity Provider. This is not possible in the operating condition where Lite Web Portal operates today. This can be reconsidered in the future releases based on the customers' requirements.</p>

Fix Pack version of BigFix Remote Control V10.0.0	Known problems and limitations
	<p>Customers operating in SSO might have an LDAP configured and the validation of the credentials might occur via LDAP. If not, a password must be defined in the local remote-control database at the user level.</p> <ul style="list-style-type: none"> • Lite Web Portal does not support upload of registration from Controller <p>The reason is that there is no advantage as the upload will occur via Broker, and that is the same upload path that the target will follow. To save session registration, set policy to register on the target and upload the recording from there.</p>
Fix Pack 1	None known.

For other known issues and limitations, see the Release Notes in the BigFix Remote Control Knowledge Center: https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Rel_Notes/release_notes_10.html

Chapter 2. Installation information

Read the following sections before you install BigFix Remote Control Version 10 Fix Pack 2

Prior to installation

Installing the fix pack after installing the version 10 GA level (10.0.0.0029)

If you are installing the fix pack immediately after installing the version 10 GA Level (10.0.0.0029), 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 10.0.0 Windows Server Installation with a WebSphere Application Server 19.0.0.11 Liberty Profile

1. Decompress BigFix_Rem_Cntrl_V10_Image3.tar 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/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_server_installer.html

BigFix Remote Control 10.0.0 Linux Server Installation with a WebSphere Application Server 19.0.0.11 Liberty Profile

1. Untar BigFix_Rem_Cntrl_V10_Image_3.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/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_server_installer.html

Manual Installation

If you are using BigFix_Rem_Cntrl_V10_Image_3.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 10.0.0 WebSphere Application Server (WAS), AIX, Linux, Solaris and Windows Server Installation



Important: Back up your video recordings and customized properties files

Untar BigFix_Rem_Cntrl_V10_Image_3.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/10.0/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/10.0/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/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_comp_install.html

Windows components:

1. Unzip BigFix_Rem_Cntrl_V10_Image_3.tar
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 `BigFix_Rem_Cntrl_V10_Image_3.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/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst-addiitional_install.html

3. Use the following files to install the components.
 - **Target:** `trc-target-10.0.0.i386.rpm` or `trc-target-10.0.0.src.rpm`
 - **Controller:** `trc-controller-10.0.0.noarch.rpm` and `trc-controller-jre-10.0.0.i386.rpm`
 - **Gateway:** `trc-gateway-10.0.0.i386.rpm` or `trc-gateway-10.0.0.src.rpm`
 - **Broker:** `trc-broker-10.i386.rpm` or `trc-broker-10.src.rpm`
 - **CLI:** `trc-cli-10.i386.rpm` or `trc-cli-10.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/10.0/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/10.0/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 10.0.0.0029 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/10.0/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.

Appendix A. Support

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

- [BigFix V10.0 Lifecycle Documentation](#)
- [HCL Software Support](#)
- [HCL portal for BigFix Support](#)
- [BigFix Developer](#)
- [BigFix Forum](#)

Appendix B. 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.