BigFix Remote Control Version 10.1 Fix Pack 5 Readme

Contents

Chapter 1. About this Fix Pack

This readme file provides important information about Fix Pack 5 for BigFix Remote Control Version 10.1.0.

What is new in this Fix Pack

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.1.0 Fix Pack 5.

Web Based Controller

This release introduces the Web Controller, allowing operators to start an active or monitor Broker Session directly from a browser via the Remote Control Lite Web Portal (LWP). This eliminates the need to install the standalone Controller application. Please note that this initial version has limited functionality compared to the standalone application: we plan to extend this new component by adding new features over time. For more details, refer to Known problems and limitations *(on page 23)*.

Rest API for Integration with Remote Control

New REST APIs enable integration with external products. These APIs allow users to check available Session Modes for specific computers and retrieve session details, recordings and history. Swagger UI is available to get the documentation and to test the new REST APIs.

Single Sign-On (SSO) for Lite Web Portal (LWP)

SSO is now available for the Lite Web Portal, allowing users to log in seamlessly without manually entering credentials each time.

New Application Server and Java runtime

IBM WAS Liberty has been replaced with Open Liberty version 25, and the Java runtime has been upgraded to IBM Java Semeru version 25. The default keystore now is PKCS#12 (.p12). The Server now uses FFmpeg to export recordings so JMF and XVID are no longer needed. For more details, refer to Known problems and limitations *(on page 23)*.

New Java runtime and FIPS 140-3 support for the Controller

The Java runtime has been upgraded to IBM Java Semeru version 25. Now the Controller supports the FIPS 140-3 module. The Bouncy Castle dependency has been removed. For more details, refer to Known problems and limitations *(on page 23)*.

Azure SQL Managed Instance

The Remote Control Server database can now be hosted using the Azure SQL Managed Instance cloud service.

Fixed vulnerabilities

CVE-2026-33870 and CVE-2026-33871: affecting the Remote Control Server, which could allow request smuggling or Denial of Service (DoS) attacks.

- Affected component: Remote Control Server
- Affected version: Remote Control version 10.1.0 FP4 and earlier

Update of IBM WAS Liberty, IBM Java, and OpenSSL

This product release adopts the following:

- Open Liberty version is 25.0.0.12
- Semeru Java version is 25.0.2.1
- OpenSSL version is 3.5.5

What is new in previous Fix Packs

What's new in 10.1.0 Fix Pack 4

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.1.0 Fix Pack 4.

Elevated privileges to run command tools

New command tools can be added to the Controller and run with elevated privileges, enabling the operator to execute commands on the Target even if the end user has insufficient permissions. The system now supports starting a process as a different user and elevating their privileges, bypassing restrictions on the current user. A credential panel will appear to authorize the tool's process start up.

Pin the chat session window into the Controller

The Controller now allows to pin the chat session windows directly into the main window or use it as a detached window.

Rename the main window into the Controller

It is possible to rename the title of the main window of the Controller.

Automatic re-establishment of a session in case of manual reboot

When the user performs a reboot of the Target machine the Controller will automatically re-establish the session. This feature is only available on Windows Targets with the installed agent and is not available for the On Demand Target.

Fixed vulnerabilities

CVE-2025-59849: Insecure Content Security Policy (CSP) configuration in the Lite Web Portal. Affected component: Server.

CVE-2025-55254: Path-relative style-sheet import (PRSSI) potential vulnerability in the Lite Web Portal. Affected component: Server.

Update of IBM WAS Liberty, IBM Java, and OpenSSL

This product release adopts the following:

- IBM WAS Liberty version is 25.0.0.10
- IBM Java SDK version 8.0-SR8-FP51
- IBM Semeru JRE version 8.0u472
- OpenSSL version 3.5.4

What's new in 10.1.0 Fix Pack 3

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.1.0. Fix Pack 3

AES 256 enabled by default

With the new version of the IBM WAS Liberty application server, AES 256 is the standard cryptographic algorithm that superseded the AES 128. It is highly recommended to update the passwords for the SSL and SAML keystores and for the database connection. With FIPS enabled, it is not possible to use an AES 128 encrypted password; it must be encrypted with AES 256.

Fixed vulnerabilities

CVE-2025-31965: Standard users can view several Admin pages into the Server.

CVE-2024-13176: Timing side-channel in ECDSA signature computation (OpenSSL).

Install Shield 2024 adoption

Install Shield 2024 has been used to build the Windows installers for Controller, Target, Broker, and Gateway.

Update of IBM WAS Liberty, IBM Java, and OpenSSL

This product release adopts the following:

- IBM WAS Liberty version is 25.0.0.6
- IBM Java SDK version 8.0-SR8-FP45
- IBM Semeru JRE version 8.0u452
- OpenSSL version 3.4.1

What's new in 10.1.0 Fix Pack 2

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.1.0. Fix Pack 2

Microsoft Entra ID Support

This release contains the Microsoft Entra ID support for the Remote Control Server. It is now possible to use Microsoft Entra ID to enable the authentication of the users and their associated groups membership into the Remote Control Server.

All configuration information that is required for Microsoft Entra ID authentication is in the new `identity_providers.properties` file. Before you configure, some prerequisite information must be obtained:

- Client ID
- Tenant ID
- Secret

The App Registration needs to be configured with at least the following Microsoft Graph API permissions:

- User.ReadBasic.All
- GroupMember.Read.All

If it is required to read all the properties for each user then the User.Read.All permission can be used instead of User.ReadBasic.All.

A new synchronization task is available in order to synchronize all the users and the groups changes in Microsoft Entra with the Remote Control database. In order to enable Microsoft Entra ID synchronization it is possible to use the new properties that has been added into the `common.properties` file:

- **sync.entraID**
- **sync.entraID.at_reset_application**
- **sync.entraID.task_run_days**
- **sync.entraID.task_run_time**

After successfully configuring all the required parameters with the new Microsoft Entra ID Configuration Utility, the users can log on to the Remote Control server by using the SAML 2.0 Single sign-on (SSO) with Microsoft Entra ID as the Identity Provider (IdP).

For more information, see Remote Control Administrator's Guide.

For Migrating LDAP users and groups to Microsoft Entra ID, see Migrating from LDAP to Microsoft Entra ID in Remote Control Installation Guide.

Usage Notes and Limitations

Only one synchronization task can be enabled at the same time: if the **sync.entraID** property is enabled together with the LDAP synchronization (**sync.LDAP**), then only the LDAP synchronization task will be executed.

Login Disclaimer

A custom Disclaimer can be configured in order to display a title and a content after the login of every user into the Remote Control server. This new feature can be useful in order to display a notice before reaching the homepage.

MacOS Sequoia (version 15) Support

The Remote Control Target now supports macOS Sequoia (version 15).

Linux Target are now supported with native 64-bit version packages only

Linux Remote Control targets, controllers, gateways, and brokers are now available for 64-bit architecture only. They no longer require installing 32-bit compatibility libraries.

Clipboard transfer from the Controller to the macOS Target and vice-versa

Now it is possible to transfer clipboard data from the Remote Control Controller to the macOS Target and vice-versa.

IBM FIPS Provider 140-3 with TLSv1.3 Support

The Remote Control Server is using the IBM Java JCE FIPS 140-3 Cryptographic Module (IBMJCEPlusFIPS). The FIPS 140-3 cryptographic security standard from the US government supersedes the previous version, FIPS 140-2 standard. With the adoption of the IBM Java JCE FIPS 140-3 Cryptographic Module the Remote Control Server now supports FIPS with TLS 1.3.

The usage of NIST SP 800-131A has been deprecated.

Hostname Verification

The Remote Control Server now performs hostname verification on SSL certificates. This means that the runtime checks to make sure that the hostname or IP address from the component certificate's Subject Alternative Name (SAN) matches the hostname or IP address used when establishing the connection. New configuration properties are available to accommodate certificates that do not pass this verification step. For more information, refer to Hostname verification for Liberty.

Serviceability Enhancements

This release includes a new warning message that has been added into the Remote Control Server log file if Derby is used as DBMS in order to make the Administrator aware that it is only recommended for Proof of Concept deployments.

Update of WAS Liberty and Java and OpenSSL

This product release adopts the following:

- IBM WAS Liberty version is 24.0.0.12
- IBM Java SDK version 8.0-SR8-FP35
- IBM Semeru JRE version 8.0u432
- OpenSSL version 3.4.0

What's new in 10.1.0 Fix Pack 1

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.1.0. Fix Pack 1

New Command Session Mode

This release introduces a new session mode named Command. This session mode allows a user to take control and interact with the remote system via a controller interface that emulates a terminal. This

session mode is supported for managed and unattended targets. Currently, this session mode is not available in peer-to-peer mode and for on demand sessions with download URL.

Session Policies

There are two new session policies that controls the behavior of this session mode. They are as follows:

- The **command** session policy in the Configuration section. This policy controls whether the command becomes selectable when sessions are established.
- The **Save commands history on server** session policy in the Auditing section. This policy defines whether the history of a command session is stored on the server for auditing purposes. The history is stored in session recordings in ciphered form and is accessible from the session history.

The Command session mode is disabled out-of-the-box.

The Controller Command Interface

The Controller provides a new interface to interact with the target while in command session mode. This interface offers the following two operation modes:

- **Command mode** - In this mode, you send a sequence of single commands to the target system. The interaction terminates when command is completed. In command mode it is possible to automate the execution of remote commands creating a customized set of command files (`.trccli` files).
- **Shell mode** - In this mode it is possible to start a command shell on the remote system and interact with it from the controller.

Usage Notes and Limitations

To use the new session mode, all the components (server, controller, and target) must be at 10.1 Fix Pack 2 (Build version 10.1.0.0126 or higher). Any attempt to use the new session mode with some earlier version component will make it impossible to establish the command session. The range of symptoms in such conditions will vary from gray controller screens to session establishment errors.

Note that while using the command interface on the controller you are interacting with the remote system by sending commands and receiving command responses. The only possible interactions are those that follow this paradigm. For example, it is not possible to start the editor while in command session or to start commands that would take control of the terminal like top. You can temporarily switch to file transfer session mode to edit a file. Commands that are known to fall in this category are blacklisted at the controller level.

If the command interaction requires sensitive information like a password, it is possible to hide such information from the command history by clicking the eye widget in the command input area of the controller. The actual input value will then be replaced by a fixed length string of unique characters. To

override this default behavior, it is possible to set the **show.hidden.commands.in.history** property to true in the `common.properties` file. This way the sensitive information is hidden locally on the controller but is visible in the command history from the server session history.

Session Policies and Command Session Mode

The Command Session mode behavior at session establishment time is conditioned by the session policies as any other session mode.

Connect at logon	User acceptance for incoming connections	Target status	Session establishment
Any	Yes	User logged in[1]	User acceptance prompt is shown[2]
	No	User logged in[1]	Session is established
Yes	Yes	No user logged in	Session is established[3]
	No	No user logged in	Session is established[3]
No	No	No user logged in	Session is refused
	Yes	No user logged in	Session is refused

[1] Includes target locked.

[2] Follow the user acceptance related policies on grace time and action.

[3] A command session is established in this configuration. An active session in this configuration will result in the system logon page to be shown in the controller. Make sure you review the policy settings when enabling the command session mode to ensure your session establishment requirements are meet.

Important Information for customers currently using the wrcmdprc command line.

Customer currently using the **wrcmdprc** command line interface should pay attention to the following information to prevent environment disruption:

- Starting from this release, the authorization to send commands to the target system via **wrcmdpcr** command line interface is conditioned to the setting of the “command” session policy. The existing policies will have to be updated to allow the command session mode. This will enable both the command session mode from the controller and the use of the **wrcmdpcr** command line.
- To ensure no environment disruption the following upgrade sequence should be followed. First upgrade the targets, then the controllers, and finally the server. Once the server is upgraded, update the existing session policies to allow the command session mode when required.

Unattended Target Initial Session Selection

Starting with this release, it is possible to start a session with an unattended target in any session mode. In previous releases, it was only possible to start the session in Active mode. Once the session is established it is possible to change the session mode.

When operating from the Controller Target List it is possible to define a preferred initial session mode when the session is established. You can define the list of preferred initial session mode setting to *true* for any of following properties in the `trc.properties` file.

- **rc.target.list.preferred.session.active**
- **rc.target.list.preferred.session.command**
- **rc.target.list.preferred.session.filetransfer**
- **rc.target.list.preferred.session.chat**
- **rc.target.list.preferred.session.monitor**
- **rc.target.list.preferred.session.guidance**

Note that when operating from the controller target list, the actual policies are defined at session time once the target is selected. Hence, it is not possible to know before starting the session what session modes are enabled at the policy level. If you select a preferred session mode that is not available in the actual policies, the session will start in some other session mode that is available.

When operating from the server interface the selectable initial session mode accurate as it is computed from the policy in effect for the target.

Multiple Controller Instances on MacOS

Starting from this release it is possible to start multiple controller instances on MacOS targets as in the other platforms.

Auto delete of Controller trcjws file

This product release introduces the possibility to delete the trcjws file once the controller is closed. To enable the auto delete set the value of **trcjws.delete.after.use** to *true* in the `common.prorperties` file.

Update of WAS Liberty and Java and OpenSSL

This product release adopts the following:

- IBM WAS Liberty version is 24.0.0.4
- IBM Java SDK version 8.0-SR8-FP25
- IBM Semeru JRE version 8u402
- OpenSSL version 3.1.5

What's new in 10.1.0 GA

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.1.0.

TLSv1.3 Support

This release includes support for Transport Layer Security (TLS) version 1.3. By default, Remote Control components at 10.1 GA version operate in a backward compatibility mode. In this mode of operation, when the connection is between components at version 10.1, the TLSv1.3 protocol is used. Otherwise, the TLSv1.2 protocol is used.

Components at earlier versions are able to remain operative with no disruption. Also, newly deployed 10.1 components are able to operate within existing pre-10.1 environments. When planning for an upgrade to version 10.1, consider that there are no requirements on the components' upgrade order.

Once all product components are updated to version 10.1 or in case you are deploying a brand new Remote Control environment from scratch, it is possible to configure the product to operate in TLSv1.3 only mode. In this mode of operation, the only possible connection is between components that are at version 10.1.

Cipher suites Hardening

This release of the product adopts a set of cipher suites that are at the time of release rated more secure.

Subject Alternate Name Support

This release includes support for Subject Alternate Names (SAN) in certificate validation.

In past releases, Remote Control components were validating the server identity by means of the certificate Common Name (CN).

Starting from this release, the certificate SAN is also used when validating the server identity. This can be useful, for example, while dealing with Broker certificates when the internal broker name is different than the external broker name. Both DNS and IP Subject Alternate Names are supported.

Serviceability Enhancements

This release includes 4 new Fixlets in the maintenance category to collect log files and configuration for the different components.

- 408 - Collect Logs and Confs on BigFix Remote Control Target
- 409 - Collect Logs and Confs on BigFix Remote Control Gateway
- 410 - Collect Logs and Confs on BigFix Remote Control Broker
- 411 - Collect Logs and Confs on BigFix Remote Control Server

Refer to the fixlet description for usage notes.

Extended Group search for Users and for Target

In case of a complex user group or target group tree structure with many intersecting branches, it is possible that the default group search fails to detect the complete groups membership for a given user or target. These situations are very rare and can be linked to a complex user group structure

when importing users from LDAP or when using a complex target group structure to reflect corporate structure.

This product release introduces the possibility to perform a full group search when resolving session policies. This possibility is controlled by the following properties in the *common.prorperties* file.

To enable full user group search, change the value of *user.group.search.full.tree* to *true*.

To enable full user group search, change the value of *target.group.search.full.tree* to *true*

Note: Pay attention when enabling the extended group search in an existing deployment as it may result in changes in session policies that are computed at session time.

Update of WAS Liberty and Java

This product release adopts the following:

- IBM WAS Liberty version is 23.0.0.8
- IBM Java SDK version 8.0-SR8-FP10
- IBM Semeru JRE version 8u382

Starting from this release, the Linux server installer adopts a 64-bit JRE.

Adoption of OpenSSL3

This product release adopts OpenSSL version 3.1.3 with the FIPS module version 3.0.9.

This product release also includes a complimentary copy of the openssl executable in the broker and target packages to aid in problem determination and/or certificate operations. The executable is available in the installation path.

What's new in 10.0.0 Fix Pack 8

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.0.0 Fix Pack 8.

Digital signature of Linux RPM packages

Starting from this release the product RPM packages are digitally signed. In the remote control site "Fixlets and Tasks" under the Maintenance category, you can find Fixlet 408 `Install RPM signing certificate for BigFix Remote Control for Linux`. It is suggested to deploy this Fixlet before you install the desired component RPM package. When installing on a Linux configured in FIPS mode, the Fixlet 408 may be a prerequisite depending on how the FIPS is configured.

Adoption of IBMJCEPlusFIPS cryptographic provider

Starting from this release when the server is configured in FIPS mode the IBMJCEPlusFIPS cryptographic provider is used in place of it's predecessor IBMJCEFIPS. The new provider has similar functionality to the older equivalentbut offers support for newer algorithms, additional hardware-accelerated cryptographic capabilities (where supported), and performance enhancements.

Withdrawal of Firefox plugin

The installation of the Firefox plug-in does not complete successfully on Firefox Version 57 or higher as Mozilla dropped support for legacy add-ons. The support for this installation method was deprecated in Remote Control starting from Version 9.1.4 IF0003 (Build Number 0309) and it was permanently removed starting from Version 10.0.0.0818.

Deprecation of ActiveX, Java Applet and Java Web Start plugins

The support for those installation methods is deprecated in Remote Control starting from Version 10.0.0.0818. Those installation methods are either lacking browser support (ActiveX) or may not be supported in more recent browsers. Relay on the executable file installation method.

Java Web Start Controller Start Method Deprecation

The Java Web Start memthod of the controller was deprecated in Remote Control since version 9.1.2. The deprecation is renewed at this time. A future Remote Control upate will withdraw the Java Web Start as a controller invocation method.

What's new in 10.0.0 Fix Pack 7

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.

Cipher suites Hardening

This release of the product adopts a set of cipher suites that are at the time of release rated more secure.

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's new in 10.0.0 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 10.0.0 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 10.0.0 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 10.0.0 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 adoped 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 10.0.0 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 Form Home scenario. Fore 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 10.0.0 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

BigFix Remote Control Version 10.1.0 Fix Pack 5 contains the following fixes:

- KB0129071: Entra ID configuration utility allows to connect with plaintext secret and the Secret Encrypted flag enabled
- KB0128078: Entra ID users membership sync is not working
- KB0129807: Unable to export the recording from the Server

- KB0127880: DOC - Remote Control AV Exclusion for Linux / Mac
- KB0127810: DOC - Remote Control SSL not working
- KB0127558: DOC - Add that File Transfer doesn't keep file metadata

Fixes included in previous Fix Packs

Fixes included in Fix Pack 4

BigFix Remote Control Version 10.1.0 Fix Pack 4 contains the following fixes:

- KB0123164: Update GetSystemInfo function for detecting the correct OS version (Windows 11 Support)
- KB0120692: File transfer is slow during high latency
- KB0121369: Lagging during BigFix Remote control session
- KB0122737: Quick Input Field – Clipboard Visibility Concern
- KB0123068: HKLMProxyOverride Implementation on Target Component (Target and Target ODT)
- KB0123677: Fixing empty Unattended target list
- KB0123866: Question on version of Installer used for Remote Control Target: install is failing
- KB0124320: Screen capture fails on some macOS computers if "Release" version of the Target app is used
- KB0124071: "rc.dashboard.broker.mapping" parameter documentation review
- KB0124152: Broker session keep disconnecting when the link between Controller and Broker is slow and the Broker is heavy loaded
- KB0124154: File transfer pull is always canceled when the link between Controller and Broker is slow and the Broker is heavy loaded
- KB0124200: Slow loading of Deployment Status Dashboard
- KB0124446: Command Mode: wrong output for Reg Query command
- KB0124744: Cannot see offline Unattended Targets into the Deployment Status Dashboard
- KB0124642: Truncated output into the Controller for the Command Mode
- KB0124855: Broker session never reconnect after temporary disconnection
- KB0125010: Information Discrepancy about Support for RC Target running on Linux distributions
- KB0125032: Alt+F4 injection from controller closes OSSN banner
- KB0125095: Exception on the Deployment Status Dashboard if a managed target does not have a group
- KB0125131: Remote Control collaboration issues cumulative fix
- KB0127050: With collaboration enabled the controller of the participant connects to Target hostname
- KB0124592: Unable to contact the broker and unable to start a session with InboundHTTPS
- KB0127028: DOC Unable to open ODT session
- KB0125273: DOC Internet Explorer removal from supported browser (planned for next DOC refresh)
- KB0124749: DOC Improve the documentation related to the RC Broker renewal certificate
- KB0122864: Strip the "centos" OS check from all Linux Fixlet and Tasks
- To improve the security, the following response headers have been added:
    - Cross-Origin-Embedder-Policy
    - Cross-Origin-Opener-Policy
    - Cross-Origin-Resource-Policy

Fixes included in Fix Pack 3

BigFix Remote Control Version 10.1.0 contains the following fixes:

- KB0119265: Remote control access shows a gray screen when connecting
- KB0119643: Broker crash issue
- KB0121115: Self-signed error for Root certificate with Reverse Proxy enabled on the Broker
- KB0120278: Login disclaimer of the RC Server allows bypassing
- KB0122763: Increased CPU usage of the RC Server with duplicated GUIDs of Unattended Targets
- Hardening of the Content-Security-Policy response header

Fixes included in Fix Pack 2

Fix Pack 2 of BigFix Remote Control Version 10.1.0 contains the following fixes:

- KB0118075: Deployment Status Dashboard takes time to load.
- KB0098754: Full recording not uploaded on the server if the session switches to reboot mode.
- KB0117146: BigFix Remote Control does not work with Yubikey 5 NFC smartcards.
- KB0115376: P2P sessions fail if properties are Managed="yes" and AllowP2P="yes".
- KB0116148: Incorrect prerequisite information in the "Linux broker support" documentation page.
- KB0119117: Command Session Mode - "Abort" command should match the "End Process Tree".
- The Content-Security-Policy and X-Frame-Options response headers have been added for GET requests to the fully qualified domain name of the Remote Control Server.
- An exception is thrown by the Remote Control Server while viewing an audit of a session where the command mode has been used and the browser language is not english.
- FIPS mode cannot be enabled on macOS Target.
- File transfer error for files larger than 2 GB.

Fixes included in Fix Pack 1

Fix Pack 1 of BigFix Remote Control Version 10.1.0 contains the following fixes:

- KB0113091: Error message processing long IP address list during target call home.
- KB0110496: LDAP Connection error using hostname with underscore.
- KB0111703: Error ORA-00922 when creating table USER_TOKENS.
- KB0110677: Remote Control 10.1 GA SSO logon fails with Azure Identity Provider.
- KB0110935: On Demand Target doesn't work on Windows if FIPS is enabled.
- KB0111197: On Demand Target crashes on macOS if HTTPStrictValidation is enabled.
- KB0109753: Error in relevance and action script of Fixlet 108.
- KB0113415: Broker connection hangs indefinitely when a remote endpoint loses connection just before the TLS handshake.

- Broker session connections are not cleaned properly if one of the participants loses the connection and it doesn't reconnect within the timeout time.
- The controller connection is not cleaned properly when the controller moves to another broker while reconciling with a target.

Fixes included in 10.1.0 GA

BigFix Remote Control Version 10.1.0 contains the following fixes:

- KB0105778: Full User Group/Target Group search for policy determination
- KB0105721: Cannot use the remote CLI commands to run DOS commands on the target
- KB0107056: LDAP Failures during synchronization can cause undesired user deletion
- KB0107954: DB2 Selection in Server Wizard results in Derby Install Instead
- KB0107980: Tasks created with the RC Target Wizard are not visible on the load panel
- KB0108711: Targets with large MAC Address list cannot register to the RC Server
- KB0108239: (Doc) P2P issues with Num-lock and "Send CTRL + ALT + DEL"
- KB0108320: (Doc) Auditing - Accessing Event Viewer
- KB0106436: (Doc) Use of CA certificate for RC single sign-on configuration
- KB0107951: (Doc) Missing information for Apple Silicon architecture support

Fixes included in Fix Pack 8

Fix Pack 8 of BigFix Remote Control Version 10.0.0 contains the following fixes:

- KB0104815: Failed to automatically re-establish a session with the Target after a reboot if session user acceptance is enabled
- KB0104506: Relevance of "Remote Control Controller Logs" analysis causing performance issues
- KB0104496: Target crash upon P2P session closure
- KB0103715: View of server log from admin menu no longer works after server upgrade
- KB0103712: Acceptance Dialog Customization not working on MacOS.
- KB0103711: MacOS pull file dialog not properly refreshing
- KB0103501: Installer log does not properly trace properties manipulation
- KB0103500: Target unable to contact Broker after Certificate Update
- KB0103374: Computers cannot start Remote Controls Target service when IP list is very long
- KB0103341: User Acceptance error on Remote Control version 10.0.0-0736.- LogRollover
- KB0103338: Broker Service is unstable with FP7 installed (Broker Crash: NullPointer)
- KB0102880: Remote Control Broker cannot receive any connection when HTTPSStrictValidation is set to "yes"
- KB0099025: Remote Control Broker is randomly down (FP7) / Memory Leak
- KB0103834: Remote Control Web URL configuration steps optimization
- KB0104582: Remote Control truncates IP address on SQL insert and update
- KB0104536: Dashboard on RC server stretches when the Application Error table has a long message
- KB0102450: Problem with display resolution with Remote control Target on Mac with Hi res screen

Fixes included in Fix Pack 7

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 Fix Pack 6

Fix Pack 6 of BigFix Remote Control Version 10.0.0 contains the following fixes:

- 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 .trcjws 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 V10.1.0	Known problems and limitations
Fix Pack 5	• **Web Based Controller** Usage Notes and Limitations: ◦ Brokers and Targets must be updated at version 10.1 Fix Pack 5 ◦ Only Monitor and Active Session modes are available. ◦ Only Broker Session types with Connection Codes are supported (Managed and Unattend Session types are not available).

Fix Pack version of BigFix Remote Control V10.1.0	Known problems and limitations
	◦ Supported browsers: Edge and Chrome. ◦ Session reconnection in case of an unexpected connection drop is not currently supported. ◦ Only High Quality sessions are supported so the High Quality color Session Policy must be enabled. ◦ File Transfer and Chat are not currently supported. ◦ Quick Text Input is not currently supported. ◦ Privacy Mode is not currently supported. ◦ Joining sessions or collaborations is not currently supported. ◦ Multi screen selection is not currently supported. ◦ Smart Card selection is not currently supported. ◦ Enable scaled view is not currently supported. ◦ Full Screen support is not currently supported. ◦ Enable/Disable input is not currently supported. ◦ Controller tools: Quick Text Input is not currently supported. ◦ Configure controller: General is not currently supported. ◦ Configure controller: Run Tools is not currently supported. ◦ Configure controller: Key Sequence is not currently supported. ◦ Enable/Disable NumLock in Target is not currently supported. ◦ Network Response Time is not currently available. ◦ Enable auto scrolling view is not currently supported. ◦ Session Recording (local to Controller) is not currently supported. ◦ Controller tools: Show Session info is not currently available. ◦ Get System info is not currently supported. ◦ Quality selector is not currently supported. • **New Application Server and Java runtime** Usage Notes and Limitations: ◦ The RC Server now only supports 64-bit architectures; 32-bit support has been discontinued. ◦ The iKeyman tool used to handle keystores has been replaced by the Java Semeru v25 keytool utility. ◦ JKS Keystores are not supported if FIPS is enabled. ◦ Lack of connection with Oracle if FIPS is enabled. ◦ JDBC drivers must be updated to support Java 25. ◦ With Windows Server 2025 the following steps can be used if the installer exists immediately with the “This Application has Unexpectedly Quit” message:

Fix Pack version of BigFix Remote Control V10.1.0	Known problems and limitations
	▪ Open a CMD. ▪ Run set JAVA_TOOL_OPTIONS="-Dos.name=Windows Server 2016". ▪ Start the .exe server installation file from the same cmd. • **New Java runtime and FIPS 140-3 support for the Controller** Usage Notes and Limitations: ◦ The RC Controller now only supports 64-bit architectures; 32-bit support has been discontinued.
Fix Pack 4	• **Compatibility mode for Server Installer on Windows Server 2025** To manually install the Server on Windows Server 2025 it is required to run the installer in Windows 8 compatibility mode. • **Hanging install or uninstall of the Server** This issue is related to the `InstallAnywhere` registry file (standard path: `C:\Program Files (x86)\BigFix\TRC\server\.com.zerog.registry.xml`) and occurs when the file size exceeds approximately 200MB. When this happens, the installer and uninstaller cannot parse the file, causing the task to fail or hang. To resolve this issue, rename the file; a new, smaller `.com.zerog.registry.xml` file will be created upon the next installation. • **Automatic re-establish of session only available for Windows Targets and not with ODT** It is not possible to re-establish a session after a reboot that was initiated from a Target which has Linux or macOS as Operating System. The feature is not available with the On Demand Target. • **Elevated privileges to run command tools only available for Windows Targets and not with ODT** It is not possible to use the elevated privileges to run command tools from a Target which has Linux or macOS as the operating system. This feature is not available with On Demand Target.

Fix Pack version of BigFix Remote Control V10.1.0	Known problems and limitations
Fix Pack 2	• **LDAP and Microsoft Entra ID synchronization tasks** Only one synchronization task can be enabled at the same time. If the **sync.entra-ID** property in the `common.properties` file is enabled together with the LDAP synchronization (**sync.LDAP**), then only the LDAP synchronization task will be executed. • **MacOS On Demand Targets do not support reboot** The reboot is not supported with macOS On Demand Targets even if it appears listed in the available session modes. • **Command session mode and Reboot session mode not supported in Peer to Peer**
Fix Pack 1	• **In Command Session mode, garbage in command output.** There may be commands that produce a formatted output. Such formatting characteristics are platform dependent and may not be rendered correctly on the controller where they appear as symbols intermixed with characters. For example, this is the case with "man" command on MacOS. • **In Command Session mode, some commands may provide output only when a terminal is detected.** There may be commands that produce output only if a terminal is detected. The effect of this command on the controller is that of a hang command while there should be a visible prompt for input. For example, take the case of "read -p “Please Enter..” var". The read command will only produce "Please Enter.." if it detects a tty. • **In Command Session mode, some commands may spawn a sub process/shell.** There may be commands that produce a new execution context. The interaction of such commands from the controller appears as if the command is still in execution. For example, take the case of "su - user" command. After this command you have no prompt for input at the controller while the target process is waiting for input. You can interact with the remote system in these circumstances by sending input and receiving output. You can normally close the remote process by sending an exit command. • **In Command Session mode, Controller Collaboration not supported.**

Fix Pack version of BigFix Remote Control V10.1.0	Known problems and limitations
	It is not possible to initiate a controller collaboration while in command mode. Hence, the collaboration button is disabled when in command mode. Similarly, switching to command session mode while a controller collaboration is in progress is not supported. • **Possible malfunctions in Export Recording feature (Windows Only)** The export recording function from the remote control server session history pages may not work at all (in version 10.1 GA) or may not work when exporting in compressed form (in version 10.1 FP1 build 10.1.0122 or higher). To resolve this problem, perform the following steps: 1. Install a Remote Control Controller. 2. Copy the `C:\Program Files (x86)\BigFix\Remote Control\Controller\jre` folder to `C:\Program Files (x86)\BigFix\TRC\server` and rename it to something like *jreEXP*. 3. Edit the `encode.cmd` file located in `..\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear`. 4. Update Line 8 and Line 9 to reference the new jre folder - `"%servhome%jreEXP\bin\java"`. **Note:** The default recording folder (`rc_recording`) where session recordings and now command histories are located is placed by default under the `wlp tree`. This tree is however removed at upgrade time. As indicated in the upgrade section make a copy of the `rc_recording` folder. It is suggested to place the `rc_recording` outside to the `wlp tree` and update the **rc.recording.directory** in `trc.properties` like for example: `C:\Program Files (x86)\BigFix\TRC\server\rc_recordings`
10.1.0 GA	• **10.1 Broker in FIPS mode no longer supports .p12 keystore type** The following error appears in the Broker log file when the Broker is configured to operate in FIPS mode and a .p12 keystore is used to contain the broker keys.

Fix Pack version of BigFix Remote Control V10.1.0	Known problems and limitations
	PKCS12_parse: 14460000:error:0308010C:digital envelope routines: inner_evp_generic_fetch:unsupported:crypto\evp\evp_fetch.c:341:Global default library context, Algorithm (PKCS12KDF : 187), Properties (<null>) This is caused by OpenSSL3 that no longer allows PKCS12KDF algorithm when in FIPS mode. The work around for this issue is to convert the .p12 keystore in a .pem keystore. You can use the complimentary openssl executable included along with the broker binaries. The PEM file needs to contain the following items, in the order listed below: ◦ Broker's certificate ◦ Any intermediate certificates, if required ◦ Root certificate ◦ Broker's private key Use the following openssl commands to convert the .p12 in .pem where keystore is your keystore file. Use your existing keystore passwords when prompted. ◦ openssl pkcs12 -nokeys -in keystore.p12 > keystore.pem ◦ openssl pkcs12 -nocerts -in keystore.p12 >> keystore.pem If your keystore.p12 already contains a CA signed certificate the intermediate and root certificate the keystore.pem should contain them, otherwise add them manually to the .pem file. Update the *trc_broker.properties* to reference keystore.pem in place of the keystore.p12. You may need to add the path where openssl is to the PATH and to the LD_LIBRARY_PATH environment variables before you can run the complementary openssl depending on the platform. • **Review Existing Broker Configuration after the upgrade to 10.1** A Broker upgrade may overwrite the existing *trc_broker.properties* file. Make a backup copy of the *trc_broker.properties* before proceeding with the upgrade. After the upgrade review your current broker configuration and remove any existing *DefaultTLSCipherList*, *DefaultHTTPSCipherList*, *ServerTLS**, and *UseTLS** properties to ensure that the Broker operates with version 10.1.0 hardened configuration. • **A 10.1 Environment in FIPS mode cannot enable TLSv1.3 Only mode of operation.**

Fix Pack version of BigFix Remote Control V10.1.0	Known problems and limitations
	The IBM Java JCE FIPS 140-2 Cryptographic Module included in the Remote Control Server does not support the TLSv1.3 protocols. This implies that in a Managed Mode environment configured in FIPS mode it is not possible to operate the product in a TLSv1.3 only mode. In a Remote Control version 10.1.0 environment configured in FIPS the connections between Components will always occur using FIPS certified providers. When the connection occurs between Target, Controller, and Brokers the connection uses the TLSv1.3 protocol. When the connection occurs between the components and the Remote Control Server the connection uses the TLSv1.2 protocol. A future release of Remote Control will include a FIPS Certified Java Cryptographic Module capable of TLSv1.3 as soon as IBM provides one. • **Pre 10.1 Managed Targets may establish a session with a pre 10.1 controller even if TLSv1.3 only mode has been activated** A Managed Target of version pre 10.1 that is configured AllowP2P=yes AllowP2P-failover=yes may be able to accept and establish a session from a Controller of version pre 10.1 configured even if the environment is set to operate in TLSv1.3 Only. This is an extremely rare condition that is triggered by an improper activation of the TLSv1.3 only mode and by the managed target call home history at the time of the session establishment. Ensure that all your components are at 10.1 version before activating the TLSv1.3 Only mode.
10.1.0	Make sure that the services window is closed during the installation or upgrade of the BigFix Remote Control Server. On certain windows platforms, an open services window can result in the installation process hanging or to the absence of the BigFix Remote Control Server service.

For other known issues and limitations, see the Release Notes in the BigFix Remote Control Knowledge Center: https://help.hcl-software.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 10.1.0.

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.hcl-software.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.hcl-software.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.hcl-software.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.hcl-software.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.hcl-software.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.hcl-software.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.hcl-software.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.hcl-software.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.hcl-software.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.