BigFix Remote Control
Target User's Guide

Special notice

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

Edition notice

This edition applies to version 10.0 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview of the Remote Controlsystem

The Remote Control system includes the following main components:

Remote Control Target

The target is installed on every computer that you want to control remotely with Remote Control. It listens for connection requests that come from the controller. You can also start a remote control session over the internet with a target, by using a broker.

Targets that are outside of your intranet can be configured to register their details with the server. Sessions with these targets are managed by server policies. The targets must be deployed with the **Managed** property set to Yes. The **ServerURL** and **BrokerList** properties must also be configured. Targets can also be configured so that they do not send their details to the server. These targets are classed as unregistered targets. You can install the target software and set the **Managed** property to No. The **BrokerList** property must also be set. You can also use the on-demand target features to start a remote control session with a computer that does not have any target software preinstalled. Server policies are used to manage the on-demand sessions. The target software is deleted at the end of the session.

Remote Control Controller

The controller can be installed by using the Fixlet, or by using the installer that is provided for use in peer-to-peer sessions. It can also be launched in context from the remote control server or the Remote Control console. In all instances, the controller can be used to allow the user to control a remote computer on which the remote control target is installed. The controller delivers an interface to several actions, available to the controller user, like remote control, guidance, chat, file transfer, collaboration, and many more.

Remote Control Server

A web application that manages all the deployed targets that are configured for managed mode and to point to the Remote Control Server 's URL. You can deploy it on an existing WebSphere® server, or install it by using the installer package along with an embedded version of WebSphere®. The server listens for HTTP or HTTPS connections by default. When it is installed with the embedded WebSphere® option, WebSphere® it listens on ports 80 and 443. When it is deployed on top of an existing WebSphere® server, the Remote Control server listens on ports 9080 and 9443. The server requires a database server: embedded Derby, only for proof of concept deployments; DB2®, SQL Server, and Oracle are the supported options. Additionally, it can also be configured to synchronize and authenticate user and group data from an LDAPv3 server, such as Active Directory or Tivoli Directory Server. This deployment scenario has the same networking characteristics as peer-to-peer. Therefore, direct TCP connectivity is required between all the controllers and all the targets. However, the Remote Control server provides a method of centralized, and finer, policy control, where targets can have different policies that are determined by the user who is trying to start the remote control session. The Server also provides for centralized audit and storage of full session automatic recordings. In this scenario, the controller is not a stand-alone application, but is started as a Java™ Web Start application from the Remote Control server's web interface to start the remote control session.

Note: Peer-to-peer and managed are not exclusive modes. You can configure the Remote Control target in the following ways:

- To be strictly managed.
- To fail back to peer-to-peer mode when the server is not reachable.
- To accept both peer-to-peer and managed remote control sessions.

The following components can be used only in managed mode:

Remote Control CLI tools

CLI tools are always installed as part of the target component but you can also install them separately. The CLI provides command-line tools for the following tasks:

- Script or integrate the launch of managed remote control sessions.
- Run remote commands on computers with the managed target installed.

Remote Control Gateway

A service that is installed in computers in secure network boundaries, where there is strict control of traffic flows between the secure networks. For example, the firewall at the boundary allows only traffic between a pair of specific IP address and ports. In these scenarios, a network of gateways can be deployed. The gateway routes and tunnels the remote control traffic from the controller, which is located in a particular network zone, to the target that is in a different network zone. The gateway is a native service that can be installed on a computer that has a Windows™ or Linux™ operating system installed. It does not have a default port for listening, although 8881 is a usual choice, and can be configured for multiple incoming listening ports and outgoing connections.

Remote Control Broker

A service that is installed in computers typically in a DMZ so that computers outside the enterprise network, in an Internet cafe or at home, can reach it. The Remote Control broker receives inbound connections from the controller and the target and tunnels the remote control session data between the two components. The broker is a native service that can be installed on a Windows™ or a Linux™ computer. It does not have a default port for listening, but 443 is a recommended option because usually this port is open for outbound connections and has fewer issues with content filtering than, for example, 80 would have.

Chapter 2. Remote control target overview

The BigFix® Remote Control Target software provides the interface that the target user can use to communicate with the controller user during a remote control session.

When the target software is installed and the BigFix® Remote Control Target service is running, the target icon  is visible in the taskbar of the target system. You can use this icon to open the target interface to communicate with the controller user during a remote control session and also to obtain connection and system information.

Chapter 3. Tasks you can do from the target icon

When the Remote Control target software is installed, the target icon is visible in the taskbar.

Rolling the mouse over the icon

You can roll the mouse pointer over the icon to display the computer name, IP address, and FIPS status of the target.

Right-clicking the icon

You have the following options when you right-click the icon:

Open Remote Control - Target

Use this option to display the target interface. For more information about the interface, see The target interface *(on page 7)*.

About

Use this option to display the version number of the currently installed target software.

Note: The version number is useful for reporting connectivity issues to HCL software support.

Online help

Use this option to access the Remote Control online documentation.

Connection info

Use this option to display the target computer name and IP address.

Report status to server

Use this option to force the target to contact the server and report its status to it.

Who is connected?

Use this option to display the user ID of the controller user and the IP address and MAC address of the controller system that established the remote control session.

Note: This option is available only during a remote control session.

Disconnect

Use this option to disconnect the target from any remote control session.

System Information

Use this option to generate a `sysinfo.txt` file, which contains information about the target such as computer name, vendor, model, IP address, and running processes. The file is displayed in a text file.

Transfer folder

Use this option to open the folder that is used for transferring files to and from the server.

Enter connection code

Use this option to enter the connection code that is required to start a session through a broker. For more information, see Starting a remote control session that uses a broker *(on page 16)*.

Double-clicking the icon

Double-click the icon to open the target interface. For more information, see The target interface *(on page 7)*.

Chapter 4. The target interface

You can use the target interface to participate in a remote control session and communicate with a controller user during the session. When you double-click the target icon in the taskbar, the target interface opens.

The interface has the following capabilities:

- **Connection status**. See Viewing the session connection status *(on page 7)*.
- **Session types pulldown**. See Selecting a session type from the target interface *(on page 7)*.
- **Show / Hide Chat Area**. See Viewing or hiding the chat area *(on page 8)*.
- **Show / Hide Transfer Area**. See Viewing or hiding the file transfer area *(on page 8)*
- **Actions Menu**. See Actions that can be made from the target interface *(on page 8)*
- **View System Information**. See Viewing system information *(on page 10)*
- **Help Menu**. See Getting help *(on page 10)*

Viewing the session connection status

Check the remote control session status by clicking the connection icon  . This icon is visible and connected when a session is established and is disabled when there is no session in progress.

Selecting a session type from the target interface

The session list on the target interface displays the session types that you can select during a remote control session. The controller user selects the session type when they start a session. When the session starts, you can change the session type by selecting one from the list. The session type options available are determined by what is set in the permissions

for the session. For more information about session types, see the BigFix® Remote Control Controller User's Guide.

Viewing or hiding the chat area

You can click the **Show/Hide Chat Area** icon  to open a chat window for real-time communication with the controller. Click the icon again to hide the chat window.

When the chat window opens, you can type into the window and press enter. The text is displayed in the chat window and the controller user can respond. The chat history can be removed from the window by selecting **Clear chat history** from the **Actions** menu.

Note: Depending on the policies that are set for the remote control session, if chat is not enabled, the chat icon is disabled.

Viewing or hiding the file transfer area

You can click the **Show/Hide Transfer area**  icon to open a window that shows the transferred files between the controller and target. The icon on the left shows the direction of the transfer. The color of the progress bar denotes which type of transfer took place.

When the transfer is from the target to the controller, a left arrow is displayed. The status bar turns green when the transfer is complete.

When the transfer is from the controller to the target, a right arrow is displayed. The status bar turns blue when the transfer is complete.

Actions that can be made from the target interface

You can use the **Actions** menu  for the following actions:

Connection info

This action displays the computer name, IP address list, and FIPS status of the target system. Click **OK** to continue.

Report status to server

This action causes the target to contact the server to report its status. This action is not available when the **Managed** target property is set to No.

Who is connected?

Displays the user ID of the controller user and the IP address and MAC address of the controller system that started the remote control session. Click **OK** to continue.

Note: This option is available only during a remote control session.

Transfer folder

View the contents of the file transfer directory. All transferred files from the controller to the target are shown in the directory.

Send file to controller

Select a file on the target system and transfer it to the controller system. For more information about transferring files, see the *BigFix® Remote Control Controller User's Guide*.

Clear chat history

Clears the chat history area of the target interface.

Hidden Windows™

Displays any running applications on the target that were hidden before the session was established. For more information about hiding running applications, see Hiding applications *(on page 14)*.

Enter connection code

Enter the connection code that is required to start a session through a broker. For more information, see Starting a remote control session that uses a broker *(on page 16)*.

Viewing system information

To view a target's system information, click the **Get system info** icon  . This action generates a file called `sysinfo.txt`, which contains information about the target such as computer name, vendor, model, IP address and running processes. The file is displayed in a text file and can be sent to the controller in an email to assist in troubleshooting.

Getting help

To get help, click the **Help** menu  and select one of the following options.

About

Use this option to display the version number of the currently installed target software.

Note: The version number is useful for reporting connectivity issues.

Online help

Use this option to go to the HCL Knowledge Center where you can view the Remote Control documentation.

Chapter 5. Accepting remote control session actions

When a remote control session is requested or certain actions are carried out by the controller user, you can be asked to confirm acceptance of these actions. Your acceptance is requested if user acceptance session policies are enabled and set to yes for the session. Target user acceptance can be requested when the following actions are carried out by the controller user:

- Starting a remote control session
- Changing the session type during a remote control session
- Requesting target system information
- Transferring files to and from the target
- Making a local recording of a remote control session
- Requesting to allow multiple participants in a session

The following options can be available in the acceptance window when confirmation is required, depending on the action that is being accepted.

Accept

To accept the request and allow the controller user to complete the action, click **Accept**.

Refuse

To refuse the request and not allow the controller user to complete the action, click **Refuse**.

Session type

When user acceptance is enabled for starting a session, if you do not want the controller user to have Active control of your system, select a different session type.

Guidance

The controller user can view your system in guidance mode, but cannot control the remote mouse or keyboard. For more information about this session type, see the *BigFix® Remote Control Controller User's Guide*.

Monitor

The controller user can view your system in monitor mode, but cannot control the remote mouse or keyboard. For more information about this session type, see the *BigFix® Remote Control Controller User's Guide*.

Chat

You can chat with the controller user without allowing them to view your system.

Hide applications

To hide any running applications on the target that you do not want the controller user to see, click **Hide applications**. For more information about hiding applications, see Hiding applications *(on page 14)*.

Note: When you receive an acceptance request, you have a predefined number of seconds to accept or refuse it. If you do not accept in time, the outcome of the request is determined by the values that are set for the following properties.

Acceptance timeout action

If the session was initiated from the BigFix® Remote Control Server.

AcceptanceProceed

If the session was initiated directly between the controller and the target.

If both properties are set to proceed, the requested action is completed without user acceptance. If they are set to *Abort*, the requested action is not completed and a message is displayed on the controller system. For more information about how

policies are derived for a remote control session, see the *BigFix® Remote Control Administrator's Guide*.

Chapter 6. Hiding applications

Before accepting a remote control session, you can hide any applications on your system that you do not want the controller user to see.

Hiding running applications from view during a remote control session

When a remote control session is requested, you can hide any running applications on the target that you do not want the controller user to see. This option is available on the acceptance window when the **Enable user acceptance for incoming connections** and **Hide Windows** server policies are enabled (managed session) or the **ConfirmTakeOver** and **HideWindows** target properties are set to yes (peer-to-peer session). It is shown on the user acceptance window when the session is requested.

Hide applications by completing the following steps

1. In the user acceptance window, click **Hide Applications** and **Accept**.
   The **Show / Hide** window opens, listing all the running applications on the target.
2. Select the applications that you do not want the controller user to see.
3. Click **OK**.

When the session is established, the selected applications are no longer visible in the target and controller windows.

Note:

- The procedure can be carried out only by the target user in the session.
- If you click **Cancel** in the **Show / Hide** window, the selected applications are not hidden when the session is established.

Restoring hidden applications to view during a remote control session

If, during a remote control session, any running applications that were hidden are now required to be seen by the controller user, the target user can make them visible again.

Make hidden applications visible again by completing the following steps:

1. Double-click the Remote Control target icon to bring the target window toolbar into view.
2. From the **Actions** menu, select **Hidden Windows**.
3. Click **Accept** on the acceptance window.
4. On the Show/Hide applications window, select the applications that you want to bring back into view.
5. Click **OK**.

The previously hidden applications, are now visible in the controller window.

Chapter 7. Starting a remote control session that uses a broker

When your system is on the internet, a controller user can start a remote control session that uses a broker to make the connection to your system. To connect to the session, you must enter a connection code.

To start a remote control session that uses a broker, obtain a session connection code from the controller user who is starting the remote control session.

When a controller user starts the remote control session, they use the Remote Control server UI. A broker is used to make the required connection. To connect to this remote control session, you need a connection code, which is obtained from the controller user. To use the connection code to connect to a remote control session, complete the following procedure.

Enter the connection code on the target computer by following the steps relevant to the target operating system.

Note: If the target is newly installed, the Enter Connection Code option is unavailable until the target contacts the server for the first time or you manually populate the ServerURL and BrokerList properties on the target.

Windows target

Choose the appropriate method to enter the connection code:

- Right-click the target notification icon and select `Enter Connection Code`.
- Open the target UI and select **Actions menu > Enter Connection Code**.

Type the connection code and click **Connect**.

Linux target

- Open the target UI and select **Actions menu > Enter Connection Code**.
- Type the connection code and click **OK**.

Alternatively, you can also use the GUI command-line for this. For details, see Using the command-line to send actions to the target GUI.

If a successful connection is made to a broker, the connection code is verified, and the session is authenticated by the server, the remote control session begins automatically. If the **Enable user acceptance for incoming connections** policy is enabled in the session policies, the target user can accept or reject the session request. After the session starts, the features and functions that are available depend on the server policies and permissions that are set for the session.

Use the **Try Again** option if the broker connection cannot be made, the connection code cannot be verified, or the target is not authenticated by the server. When you click **Try Again**, the **Connection Code** window is displayed and you can reenter a connection code. If you click **Cancel**, the remote control session is not established.

Chapter 8. Disconnecting from a remote control session

When a remote control session is started, you can disconnect in the following ways:

- Press **PAUSE/BREAK** on your keyboard.
- Click the **Connection** icon 

The controller is disconnected and a cancel message is displayed.

Chapter 9. Auditing

Remote control session events are saved for auditing purposes if the **AuditToSystem** policy is enabled for the session.

On a Linux target computer, you can use the `messages` log file and the Application Event Log on a Windows target.

To access the Application Event Viewer in Windows, click **Start > Control Panel > Administrative Tools > Event Viewer > Application**. A list is displayed. Select **Remote Control - Target**. Right-click and select **Properties**. The **Information Properties** window opens.

Select **Remote Control - Target**.

The following information is displayed.

- Date of Takeover
- Time of Takeover
- Computer being taken over
- IP address initiating takeover
- MAC Address
- A Description section

If you are using the on-demand target, the audit log is written to a text file on the target. A `trcaudit_`*`date_time`*`.log` file is created, where date_time is the date and time that the session took place. For example, `trcaudit_20130805_132527.log`. The file is created in the currently logged on user's home directory.

Chapter 10. BigFix Remote Control Target for macOS V10 Update 6

Remote Control V9.1.4 introduces support for target users who are using macOS devices.

After you install the BigFix® Remote Control Target for macOS and start the application, the target status icon is displayed in the menu bar and the Remote Control target icon is displayed in the Dock.

Currently, the BigFix® Remote Control Target for macOS can participate in sessions that are not managed by the Remote Control server.

When a controller is connected to your computer in a remote control session, the status icon is displayed in full contrast. The icon is displayed in low contrast when you are not in a remote control session.

Starting the BigFix® Remote Control Target for macOS

After you install the BigFix® Remote Control Target for macOS, start the `Remote Control Target` application.

To start the application, complete the following steps:

1. Click **Go > Applications**.
2. Double-click the `Remote Control Target` icon.

The target status icon is displayed in the top menu bar and the Remote Control target icon is displayed in the Dock.

BigFix® Remote Control Target for macOS menu bar

When you click the Remote Control target icon in the Dock, the menu bar displays the following menu options.

Note: Some of the options are also available when you click the status icon, which is on the right of the menu bar. They are also available when you right-click the Remote Control target icon in the Dock.

Table 1. Options that are available in the BigFix® Remote Control Target for macOS menu bar.

Menu	Menu option	Description
Remote Control Target	About Remote Control target	Select this option to display the version number of the currently installed target software. **Note:** The version number is useful for reporting connectivity issues to HCL software support.
	Quit Remote Control Target	Select this option to stop the Remote Control Target application.
Session	Active mode	Select this option to change the session to Active mode. The controller user has full remote control of your system. They can view your screen and control your remote mouse and keyboard.
	Monitor mode	Select this option to change the session to Monitor mode. The controller user can view your screen to monitor activity. The controller user has no control over your mouse or keyboard.
	Disconnect	Select this option to disconnect the target from any remote control session.
Actions	Connection info	Select this option to display the target computer name and IP address.

Table 1. Options that are available in the BigFix® Remote Control Target for macOS menu bar. (continued)

Menu	Menu option	Description
	Who is connected?	Select this option to display the user ID of the controller user and the IP address and MAC address of the controller system that established the remote control session.
	Transfer folder	Select this option to open the folder that contains the files that are transferred from the controller during a remote control session. The folder is opened in the **Finder** window.
	Send file to controller	Select a file on the target system and transfer it to the controller system.
	Enter connection code	Enter a connection code to connect to a broker session.
Help	Online Help	Select this option to go to the HCL Knowledge Center where you can view the Remote Control documentation.

BigFix® Remote Control Target for macOS toolbar

A floating toolbar is available for the BigFix® Remote Control Target for macOS. Various options are available in the toolbar. For example, to disconnect from a session, switch session mode, and send files to the controller.

During a remote control session, the toolbar opens and is displayed in front of other application windows. You can close or minimize the toolbar. When the session ends, the toolbar closes unless it was open before the session started. When you are not in a remote control session, you can open the toolbar by using the **Open Remote Control Target** option in the status menu or dock icon menu.

The toolbar contains the following options.

Disconnect

Click this option to disconnect from the session.

Session mode

Click and select a new session mode. The session mode list is blank when you are not in a remote control session.

Actions

The **Actions** menu contains the following options. For more information about the options, see BigFix Remote Control Target for macOS menu bar *(on page 20)*.

- **Connection info**
- **Who is connected?**
- **Transfer folder**
- **Send file to controller**
- **Enter connection code**.

Help

The **Help** menu contains the following options. For more information about the options, see BigFix Remote Control Target for macOS menu bar *(on page 20)*.

- **About**
- **Online help**

Entering a connection code to connect to a broker session

The BigFix® Remote Control Target for macOS can participate in remote control sessions that use a broker to make the connection. Use the following method to enter the connection code to connect to the session.

Obtain a session connection code from the controller user who is starting the remote control session. For more information about sessions that are connected by using a broker, see Starting a remote control session that uses a broker (on page 16).

You can enter a connection code on the BigFix® Remote Control Target for macOS in multiple ways. To enter a connection code, complete the following steps:

1. Choose the method to enter the connection code.
    - Click the status icon, in the right of the menu bar. Select **Enter connection code**.
    - Right-click the application icon in the Dock. Select **Enter connection code**.
    - If the Remote Control Target menu is visible, select **Actions > Enter connection code**.
    - If the floating toolbar is visible, select **Actions > Enter connection code**.
2. Type the connection code and click **Connect**.

Disconnecting from a session on a mac OS device

When a controller is connected to your computer in a remote control session, you can disconnect in the following ways.

- **Status icon**

  Click the **Target status** icon on the menu bar and select **Disconnect**.
- **Dock icon**

  Click the **Remote Control Target** icon in the Dock and select **Disconnect**.
- **Menu bar**
    1. Click the **Remote Control Target** icon in the Dock.
    2. Select **Session > Disconnect** in the menu bar.

Enable the required macOS permissions on Remote Control target version V10

When a session is established for the first time, to view the screen and control a macOS Target/On-demand Target, enable Accessibility and Screen Recording permissions.

After launching the Target or On-demand Target application on macOS for the first time, the operating system prompts to grant Accessibility permission first and then Screen Recording permission.

Note:

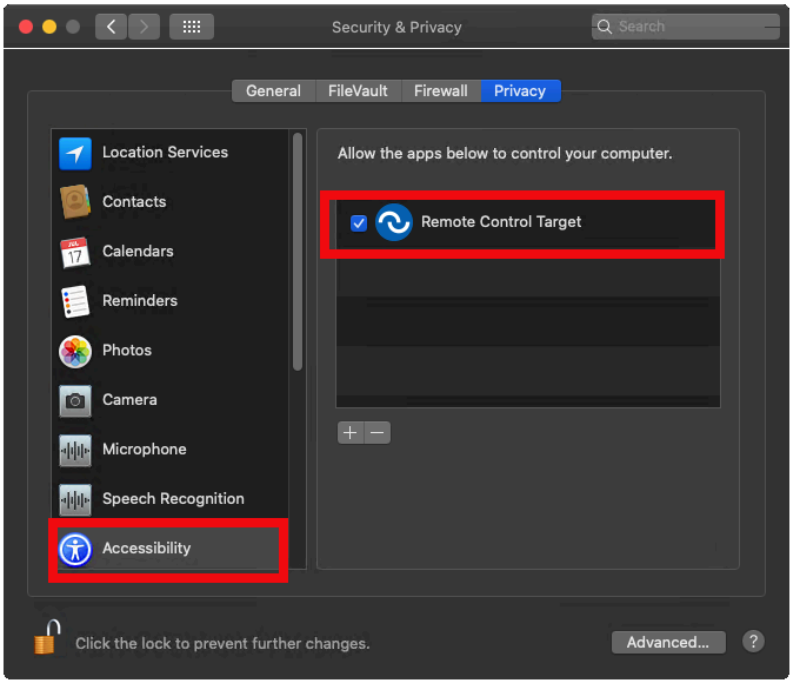
- If the Target computer is running macOS 10.14 Mojave, then only the Accessibility permission is requested.
- If you deny the needed permissions, the Controller screen does not show the remote Target screen and you cannot control the remote Target.

To grant the required permissions:

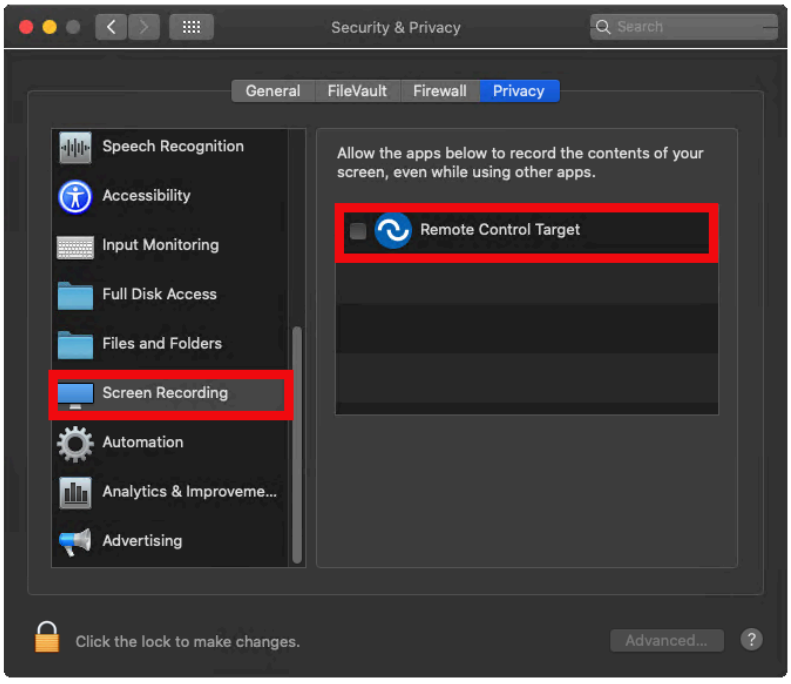
1. When prompted to grant accessibility access, click **Open System Preferences** or manually open **System Preferences** and navigate to **Security and Privacy** > **Privacy** tab > **Accessibility**.
2. Click on the lock icon and enter the credentials to allow changes on the settings.

   Note: Administrator privileges are required for this permission.

3. Enable the checkbox in the **Accessibility** section.



4. When prompted to grant Screen Recording access, click **Open System Preferences** or manually open **System Preferences** and navigate to **Security and Privacy** > **Privacy** tab > **Screen Recording**.
5. Enable the checkbox in the **Screen Recording** section.



6. On the confirmation popup, click **Later**. You are now ready to use the application.

After the required permissions are granted, you can view the remote screen and control the target.

Note: If you are running the Target or On-demand Target 10.0.0.0029 or earlier, after every permission that you grant, you need to restart the application once.

For troubleshooting information, see Target screen not visible or input not working from the Controller on macOS.

Chapter 11. Privacy Mode and Input Lock

Enable **Privacy Mode** to hide the screen contents at the Remote Control Target.

During an Active remote session, Remote Control Controller user can enable **Privacy Mode** to hide the contents of the screen at the Remote Control Target. This allows the Controller user to control the remote Target without revealing the content of the screen to the Target user during the operations. When **Privacy Mode** is selected from the Controller action menu, the Target screen is covered with an image while the Controller keeps showing the remote Target screen.

Note: This feature is currently supported only on Targets and On-demand Targets running Windows.

The bitmap used to cover the screen can be customized by replacing the **privacy.bmp** image under the Target installation folder:

- For single-screen Targets, the privacy.bmp dimensions cannot exceed the resolution of the Target screen.
- For Targets with more than one screen:
  - Option 1: The privacy.bmp dimensions exceed the resolution of the Target screen with the lowest resolution. In this case, the image resolution must respect the following properties:
    - **Width** = The sum of all the screens Widths
    - **Height** = The greater Height among the screen heights

    For example: screen1(1920x1080), screen2(1920x1200), screen3(1280x1024). The provided image resolution must be exactly 5120x1200.

    Note: The screens are always assumed to be in a horizontal stacking (left to right), when the Privacy Mode is enabled.
  - Option 2: The privacy.bmp dimensions do not exceed the resolution of the Target screen with the lowest resolution. In this case, the screen which is

currently controlled will be covered with the privacy.bmp image while the others will be covered by a full-screen black image.

For example: screen1(1920x1080), screen2(1920x1200), screen3(1280x1024). The provided image resolution must be 1280x1024 or lower.

When **Privacy Mode** is enabled, **Lock target input** entry is automatically selected and enabled on the Controller. This prevents other users having access to the Target machine from controlling it.

On a P2P session, you can customize the behavior of the Privacy and Input Lock feature with the following properties:

During a session	When the session starts
AllowPrivacy	EnablePrivacy
AllowInputLock	EnableInputLock

Fore more information, see Properties that can be set in the target configuration

On a managed session, you can customize the behavior of the Privacy and Input Lock feature with the following policies on the server:

During a session	When the session starts
Allow input lock with visible screen	Set target locked
AllowInputLock	Display screen on locked target

Fore more information, see Server session policies

Appendix A. Support

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

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

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.

Index

V