

## **Remote Control Controller 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

<b>Chapter 1. Overview of the Remote Control system.....</b>	<b>8</b>
<b>Chapter 2. The BigFix Remote Control server interface.....</b>	<b>10</b>
Accessing the server interface.....	10
Logging on to the server.....	10
Logging off.....	11
Targets menu options.....	11
Starting a broker session.....	11
Joining a broker session.....	11
Browsing for targets.....	12
Viewing all targets.....	12
Searching for targets.....	12
Creating a favorite targets list.....	13
Viewing the favorite targets list.....	13
Removing targets from favourites.....	14
Viewing recently accessed targets.....	14
Viewing the session history for a target.....	14
Viewing target status details.....	15
Viewing the session policies that are in effect between a user and a target.....	15
Starting a remote control session .....	16
Requesting temporary access to targets.....	17
Options that are available in the <b>Users</b> menu.....	20
Viewing your user details.....	20
Changing your password.....	21
Viewing the list of user groups that you belong to.....	21
Sessions menu options .....	21
Viewing your session history.....	21
Searching for specific sessions.....	22
Viewing session details .....	22
Reports menu options.....	23
Running standard reports.....	23

Running custom reports.....	24
Options menu.....	24
Setting your homepage .....	24
Resetting your homepage.....	25
Refreshing the data that is displayed on screen.....	25
Setting page display options .....	26
Exporting data in various formats .....	26
Tools menu options.....	27
Downloading tools from the BigFix® Remote Control Server .....	27
Getting help.....	32
<b>Chapter 3. Remote control sessions.....</b>	<b>33</b>
Types of remote control sessions that can be established.....	34
Taking full control of a target system.....	34
Chatting to the target user.....	35
Transferring files and directories.....	36
Providing guidance to the target user.....	39
Rebooting a target machine.....	43
Command Session Mode.....	43
Starting a remote control session from the server.....	45
Starting a peer to peer session.....	46
Starting a remote control session using a broker .....	48
Connecting to a target that is already in a session.....	50
Joining or Disconnecting a session.....	50
<b>Chapter 4. Using the controller interface as a controller user.....</b>	<b>52</b>
Overview of the controller interface .....	52
Changing the session type during a remote control session.....	55
Changing to Active Mode during a remote control session.....	55
Changing to chat only mode during a remote control session.....	56
Changing to monitor mode during a remote control session .....	56
Changing to guidance mode during a remote control session.....	56
Changing to command mode during a remote control session.....	57
Enabling and Disabling Local Input.....	57

Setting the state of the target numlock led during a remote control session in Remote Control.....	57
Actions that you can perform on the target.....	57
Retrieving Target System Information.....	61
Chatting to the target user during a remote control session.....	61
Inviting multiple participants into a remote control session.....	62
Collaboration sessions using the server UI.....	62
Peer to Peer collaboration sessions.....	66
Collaboration during sessions connected through a broker.....	70
Controlling collaboration session activity.....	74
Ending a collaboration session.....	76
Ending a collaboration session when you disconnect.....	76
Collaboration and handover audit events.....	77
Controller tools.....	77
Capturing the screen during a remote control session.....	78
Enabling quick input of text to the target screen.....	78
Viewing session information.....	79
Recording a remote control session.....	80
Exporting and downloading a recording from the server.....	80
Making a local recording .....	82
Playing a local recording .....	82
Transfer of files during an active session.....	83
Sending files to the target.....	84
Receiving files from the target.....	84
Opening the file transfer folder.....	85
Opening the target's file transfer folder.....	85
Viewing the list of transferred files.....	85
Copying clipboard information between the controller and target.....	86
Sending clipboard text to the target.....	87
Receiving clipboard text from the target.....	87
Connecting to a smart card reader during a session.....	87
Network response indication.....	88
Viewing multiple target screens.....	88

Scrolling the target screen during a session.....	89
Viewing the full target screen in a session window.....	89
Change the color quality of the session window to improve session performance .....	89
Chang the color depth of the session window.....	91
Creating a local configuration for the controller.....	91
Enabling debug in the local controller configuration.....	95
Obtaining help .....	95
Ending a Session.....	96
<b>Chapter 5. Use remote control commands from the command line.....</b>	<b>97</b>
Starting a remote control session from the command line.....	98
Examples of usage.....	100
Running commands on the target from the command line.....	100
Examples of usage.....	101
Error messages for the wrc and wrcmdpcr commands .....	102
<b>Chapter 6. Configuring global controller properties.....</b>	<b>107</b>
Run tools on the target during a peer to peer session.....	108
Sending key sequences to the target.....	111
Retaining logon credentials for P2P session.....	113
Hiding the master controller acceptance window.....	115
Enabling and Disabling the execution of tools on the target during a remote session.....	116
<b>Chapter 7. Auditing.....</b>	<b>117</b>
User acceptance audit events.....	117
Authentication audit events .....	118
Smart card audit events.....	119
<b>Chapter 8. Ensuring that current data is reported.....</b>	<b>122</b>
<b>Appendix A. Error messages .....</b>	<b>123</b>
<b>Appendix B. Session resilience for sessions that are connected by using a broker.....</b>	<b>126</b>
<b>Appendix C. Smart card status messages.....</b>	<b>128</b>
<b>Appendix D. Keyboard shortcuts for the BigFix® Remote Control Target for macOS.....</b>	<b>129</b>
<b>Appendix E. Support.....</b>	<b>130</b>
Notices.....	cxxxi
Index.....	a

# Chapter 1. Overview of the Remote Control system

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, command, 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 Microsoft® Entra ID or 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. The BigFix Remote Control server interface

The Remote Control server UI provides various functions that include creating and managing users and targets, starting remote control sessions, running reports, importing data, and recording session activity.

The functions described in this section can be performed by users, super users, and administrators. For information about the additional functions that can be performed by an administrator, see the BigFix® Remote Control Administrator's Guide.

### Accessing the Remote Control server interface

After you have installed the Remote Control server software, you can log on to the user interface. For more information about installing and configuring the server, see the BigFix® Remote Control Installation Guide.

### Logging on to the Remote Control server

To use the BigFix® Remote Control Server, log on to the server user interface.

1. In a web browser type

`http://SERVERNAME/trc.`

**SERVERNAME:** The name of your BigFix® Remote Control Server. If you do not have the name, contact your Remote Control system administrator.

2. Enter a valid ID and password.

Invalid or missing IDs and passwords generate an error message.

If you are an Administrator, and it is your first logon, the default Admin ID is `admin`, and password is `password`. After you log on for the first time, you must change your password.

Password rules are set in the `trc.properties` file in the set of variables that start with **password..** For more information about password rules, see the *BigFix® Remote Control Administrator's Guide*.

3. Click **Logon**.

The BigFix® Remote Control Server UI is displayed.

### Getting a temporary logon password

If you forget your password, you can use the forgotten password option on the server logon screen.

The temporary password is sent to you in an email. This function is available when email is set up and enabled in the system. You can enable email functions at installation or by editing the `trc.properties` file. For more information, see the *BigFix® Remote Control Installation Guide* and the *BigFix® Remote Control Administrator's Guide*.



**Note:** If email and LDAP are enabled, the forgotten password option is not displayed.

To obtain a temporary password, complete the following steps on the **logon** window:

1. Enter your ID.
2. Click **Forgotten password**.
3. Click **Logon**.

A message is displayed: If the user ID matches an existing user, a new password will be sent to the user's registered email address

4. Log on with your ID and temporary password.

The **Edit details** screen is displayed where you can change your password.

5. Type and confirm your new password.
6. Click **Submit**.

Your new password is saved. When email is enabled, you can contact the system administrator by using the link on the **logon** window.

## Logging off from the Remote Control server

To log off from the Remote Control server UI, select **Sign Out**. The **welcome screen** is displayed.

## Targets menu options

In the Remote Control system, targets are endpoints that you install the target software on. When a target is first installed, it contacts the server and sends its details that include serial number, model, manufacturer, and logged on user. This information is stored in the database and made available through the server UI. Targets periodically contact the BigFix® Remote Control Server to report their status or a change in state. For example, when a user logs on, when a remote control session is taking place, or when the system powers on or shuts down. Use the **Targets** menu to work with the target information. For example, search for specific targets, create a list of favorite targets, or start a remote control session.

### Starting a broker session

Use the **Start Broker session** option in the **Targets** menu to start a remote control session through the internet, with a target that you do not have direct access to. Start a broker session to use a broker to make the required connection between the controller and target. For details about starting a broker session see, [Starting a remote control session using a broker \(on page 48\)](#).

### Joining a broker session

For a remote control session that was started using a broker, in which collaboration has been started, use the **Join Broker session** option in the **Targets** menu to join the session. For details about joining a broker collaboration session using this option, see [Joining a collaboration session by using a connection code \(on page 72\)](#).

## Browsing for targets

Use the **Browse targets** action to browse through the defined target groups for a specific target. When you select **Browse targets**, an expandable list of target groups is displayed. Select a target group to see a list of the target members. If you do not have permission to access the targets in the selected target group, no targets are displayed. The permission to access targets is derived from permissions links made between any groups that a user and target belong to. For details, see the BigFix® Remote Control Administrator's Guide.

To browse for targets, complete the following steps:

1. Click **Targets > Browse**.
2. Click the selector button to display the list of target groups.
3. Select the required target group.  
If you have permissions to access the target members in the selected group, the list of available targets is displayed on the right. If you do not have permissions, no targets are displayed.
4. Select the required target and click the selector button.
5. Click **Submit**.

The target details are displayed and if the target is selected, a list of available actions is displayed. These actions are explained in other sections of this document.

Click **Cancel** to return to the previously displayed screen.

## Viewing all targets

When targets have registered with the BigFix® Remote Control Server, use the **All Targets** action to display a list of these targets.

To view the list of targets, click **Targets > All targets**.

The **All targets** screen is displayed showing details of all targets defined in the system.

## Searching for targets

To access specific targets or find a target using non-specific information, use the search utility. To search for a target, complete the following steps:

1. Click **Targets > Search**  
The search screen is displayed.
2. Enter target information to be used in the search.  
This can be all or part of the manufacturer, model, serial number, computername, logged on user name, or IP address. For example, 2327, te, or se\*.



**Note:** The number of characters or wildcard characters allowed in the input field is determined by the **target.search.minimum.nonwildcards** and **target.search.maximum.wildcards** properties in the **trc.properties** file. For more information, see the BigFix® Remote Control Administrator's Guide.

For the quickest search, type unique target information into the Search Target field. For example, serial number or computer name.

3. Click **Submit**.

To clear or restore previous values on the input screen, click **Reset**.

To return to the previously displayed screen, click **Cancel**.

To display the list of all targets by leaving the input field blank, click **Submit**.

Any targets matching the search criteria are displayed. The information entered is not case sensitive. For example, Test will also match with test. If no matching targets are found, a message is displayed and the target list is blank.

## Creating a favorite targets list

If you access or connect to the same targets regularly, you can create a list of favorite targets. Use the **Add to Favourites** action to add one or more targets to the list.

To create a favorites list, complete the following steps:

1. Choose the appropriate method to select the required targets:
  - To select the required targets by searching, follow the steps in [Searching for targets \(on page 12\)](#), then go to step 2 [\(on page 13\)](#).
  - To select from the All targets list,
    - Click **Targets > All Targets**.
    - Select the required targets.
2. Choose the appropriate method to add the target to Favourites.
  - Select **Targets > Add to favourites**.
  - Select **Add to favourites** from the Action list on the left
3. The Favourites screen is displayed listing all targets that have been added to the favorites list.

## Viewing the favorite targets list

After you have created a favorite targets list, use the **Favourites** option in the targets menu to view this list.

To view the Favourites list, click **Targets > Favourites**.

The Favourites list is displayed.

## Removing targets from favourites

To remove targets from the favourites list, complete the following steps:

1. Click **Targets > Favourites**.  
The **Favourites** list is displayed.
2. Select the required targets.
3. Choose the appropriate method to select Remove from favourites.
  - Select **Targets > Remove from favourites**.
  - Select **Remove from favourites** from the Action list on the left.

The targets are removed from the list.



**Note:** To show the updated list, click the **Refresh** link on the upper right.

## Viewing recently accessed targets

Use the **Recently accessed** action to view a list of targets that you have had a remote control session with. The maximum number of items in this list is determined by the variable **limit.recently.accessed** which is set in the **common.properties** file. For more information about this file, see the BigFix® Remote Control Administrator's Guide.

To view a list of recently accessed targets, click **Targets > Recently accessed**.

The **Recent targets** screen is displayed. Targets might be displayed on more than one page depending on how many there are.

## Viewing the session history for a target

Use the **Session History** action to view the list of previous sessions for a target.

To view the session history for a specific target, complete the following steps:

1. Choose the appropriate method to select the required target:
  - To select the required target by searching, follow the steps in [Searching for targets \(on page 12\)](#) then go to step [2 \(on page 14\)](#).
  - To select from the All targets list:
    - Click **Targets > All Targets**.
    - Select the required target.
2. Choose the appropriate method for selecting Session History.
  - Select **Targets > Session History**
  - Select **Session History** from the action list on the left.

The Session History screen is displayed, listing all the previous sessions for a target.

## Viewing target status details

To view information for a specific target, use the Target status action. For example, the installed operating system, the version of Remote Control target software that is installed, the target IP address, or target hostname.

To view target status details, complete the following steps:

1. Choose the appropriate method to select the required target:
  - To select the required target by searching, follow the steps in [Searching for targets \(on page 12\)](#) then go to step 2 ([on page 15](#)).
  - To select from the All targets list:
    - Click **Targets > All Targets**
    - Select the required target.
2. Choose the appropriate method for selecting Target status:
  - Select **Targets > Target status**.
  - Select **Target status** from the action list on the left.

The **Target Status** screen is displayed showing details of the target.

To return to the previously displayed screen, click **Cancel**.

## Viewing the session policies that are in effect between a user and a target

Use the **View effective policies** action to view the policies and permissions that will be in effect, in a remote control session, between a selected user and target. The policies are displayed in the following forms.

### Considered Policies

Displays any permissions links defined for the user and target groups that the selected user and target belong to. The policies and permissions that have been derived from each of these links are also listed. These policies are used to determine the final set of policies and permissions that are granted for the session. For details about how policies are derived for a session, policy definitions, and permissions definitions, see the BigFix® Remote Control Administrator's Guide.

### Resolved Policies

Shows the final set of policies and permissions, that have been resolved from the considered policies. These policies are assigned when a remote control session is established between the selected user and target.

To view the effective policies, complete the following steps:

1. Choose the appropriate method to select the required target:
  - To select the required target by searching, follow the steps in [Searching for targets \(on page 12\)](#) then go to step 2 ([on page 16](#)).
  - To select from the All targets list:

- Click **Targets > All Targets**.
  - Select the required target.
2. Choose the appropriate method to view effective policies:
    - Select **Targets > View effective policies**.
    - Select **View effective policies** from the action list on the left.

The Show Effective Policies screen is displayed with the selected target shown.
  3. To select a user, click the selector button next to User.
  4. Select a user group.
  5. Select a user.
  6. Click the - **Select a User** - selector button.

The expanded Show Effective Policies screen is displayed showing Considered Policies and Resolved Policies. The resolved policies are in effect during a remote control session between this user and target. Click **Cancel** to return to the previously displayed screen.

## Starting a remote control session

Use the **Start Session** action to connect to and control a remote target. For details about the types of remote control sessions that can be established, see [Types of remote control sessions that can be established \(on page 34\)](#).

You can start remote control sessions from the server between users and targets who are members of groups that have permissions links defined. For details about creating and assigning members to user and target groups, for creating permissions links, and for how the policies and permissions are resolved for a remote control session, see the BigFix® Remote Control Administrator's Guide.

The Start session action is available when you select a target from any report that displays one or more targets. Some examples of these reports are

### All Targets

See [Viewing all targets \(on page 12\)](#).



**Note:** This report also displays the user ID of the user who is logged on to the target.

### Recently Accessed

See [Viewing recently accessed targets \(on page 14\)](#).

### Favourites

See [Viewing the favorite targets list \(on page 13\)](#).

### Search Targets

See [Searching for targets \(on page 12\)](#).

For the steps required to start session from the server, see [Starting a remote control session from the server \(on page 45\)](#).



## Requesting temporary access to targets

You can use Remote Control to access and establish a remote control session with the targets you have permission to access. The type of access is determined by your group membership, and the relationships that have been set up between these groups and target groups. However, you can also request temporary access to one or more targets that you do not have access to using the **Request access** function. Use this function to select the required targets, define the types of remote control sessions that you want to establish, and define a time period for the temporary access. When the request is submitted, notification is sent to an administrator. When the request is answered, an email is sent to you detailing the outcome of the request.



**Note:** The email functionality must be enabled on the BigFix® Remote Control Server so that the notification process can take place. For details about enabling email, see the BigFix® Remote Control Administrator's Guide.

You can request temporary access to targets for the following reasons:

- You have been notified of a problem on a target or targets that are not members of any of the target groups you have permission to access and you need to establish a connection to be able to solve the problem.
- The permissions that you have for accessing these targets have expired or do not allow you to do what is required for the session.
- You are not a registered user in the BigFix® Remote Control Server.

The following info must be provided for an access request.

### Session Types

Enter the session types that you want to establish with the chosen targets.

### Justification

Enter the reason for requesting access to the selected targets.



**Note:** You must add any policies that you want to be valid for the session. Particularly where you have existing permissions to access the target, but need these modified for the temporary session, otherwise your existing policies are in effect for the session.

For example: You are not allowed to access or view the registry keys of the target but need to for the temporary session. You must enter in the justification that you need to access the registry keys so that the administrator can enable the registry keys policy for the temporary session.

### Start date

Enter the date, in the format **yyyy-mm-dd**, or select from the calendar. This is the date you want the access to start.

### Start time

Enter a time, in the format **hh:mm:ss**. This is the time that you want the access to start.

#### End date

Enter the date, in the format **yyyy-mm-dd**, or select from the calendar. This is the date that you want the access to end.

#### End time

Enter a time, in the format **hh:mm:ss**. This is the time that you want the access to end.

#### email address

Required. Enter your email address. This address is used by an administrator when responding to the request.

## Making a request, as a registered user

If you are a user who is already registered with the BigFix® Remote Control Server, you can request temporary access to targets in the following ways.

- Use the **Request access** option in the **Targets** menu.
- Click the **Request access** button when starting a session.

Your request is sent to an administrator who decides whether to allow you temporary access to the selected targets. An email is returned notifying you of the outcome of the request. If your request has been granted, you can access the selected targets within the specified dates and times. If your request has been denied you are **NOT** allowed to access to the selected targets.

## Using the request access option

To request temporary access to one or more targets, complete the following steps:

1. Click **Targets >All targets**.
2. Select one or more **targets**.
3. Choose the appropriate method for selecting **Request Access**:
  - Select **Targets > Request Access**.
  - Select **Request Access** from the Actions list on the left.

The **Request Access to target** screen is displayed.
4. Enter the required information for the access request.
 

For more details, see [Requesting temporary access to targets \(on page 17\)](#).
5. Click **Submit**.

Your request is sent to an administrator who decides whether to allow you temporary access to the selected targets. An email is returned notifying you of the outcome of the request. If your request is granted you can access the selected targets within the specified dates and times. If your request is denied you **cannot** access to the selected targets.

## Requesting temporary access at session start

To start a remote control session with a target that you do not have permission to access, use the request access option on the create new session screen. This option is available only if the **trc.ticket.allow.access** property is enabled. This property is set in the **trc.properties** file by an administrator. For details about editing the properties files, see the BigFix® Remote Control Administrator's Guide.



**Note:** If the property is not enabled, the request access option is not displayed.

To request temporary access to a target from the **Create new session** screen complete the following steps:

1. Select the target.
2. Click **Start session**.
3. Click **Request Access** on the **Create new session** screen.
4. Enter the required information for the access request.  
For more details, see [Requesting temporary access to targets \(on page 17\)](#).
5. Click **Submit**.

Your request is sent to an administrator who decides whether to allow you temporary access to the selected targets. An email is returned notifying you of the outcome of the request. If your request is granted you can access the selected targets within the specified dates and times. If your request is denied you **cannot** access to the selected targets.

## Requesting access to targets as a non registered user in the BigFix® Remote Control Server.

If you are not a registered user in the BigFix® Remote Control Server, you can request temporary access to targets. Use this procedure if you do not use the BigFix® Remote Control Server application but need access to update software on certain targets, or need to debug a problem on a target. The availability of this option is determined by the property **trc.ticket.allow.allaccess**, set in the **trc.properties** file. For details about editing the properties files, see the BigFix® Remote Control Administrator's Guide.

To request temporary access to one or more targets, complete the following steps:

1. Type the following URL into your browser

```
http://servername/trc/requestAccessAnon.do
```

where *servername* is the address of your BigFix® Remote Control Server

2. Enter the required information for the access request.  
For more details, see [Requesting temporary access to targets \(on page 17\)](#).
3. Click **Submit**.



**Note:** You must give details of the targets required in the Admin Notes® field so that the administrator who accesses the request can determine which targets to select.

When you click **Submit** an email containing the request is sent to the administrator. An email is returned detailing the outcome of the request. If the request is granted click the link in the email to go to the **Create new session** screen from where you can start a session with the selected targets within the specified date and times. If your request is denied you are **NOT** allowed access to the selected targets.

## Viewing your requests for temporary access

After you have submitted requests for temporary access to targets, you can view a list of these requests using the **My Requests** option.

To view your submitted requests, click **Reports > My Access Requests**.

The **My Requests** list is displayed showing all access requests that you have submitted.

## Options that are available in the **Users** menu

The BigFix® Remote Control Server program accommodates the following types of user authorities: user, super user, and administrator. Various BigFix® Remote Control Server functions can be performed by each user account, with the Administrator having the most comprehensive privileges. Some of the options in the **Users** menu are only available to a user with administrator authority. For more information about the user options that only an administrator can carry out, see the *BigFix® Remote Control Administrator's Guide*.

## Viewing your user details

Use the **My Details** option to view and update your own user details.

To view your user details, complete the following steps:

1. Click **Users > My Details**.

The **Change Details** screen is displayed.



**Note:** A warning message is displayed when Microsoft Entra ID or LDAP synchronization is enabled to indicate that any changes or additions might be lost at the next synchronization.

2. Change or update the relevant details.

The following items must be noted.

- a. The **user ID** field cannot be changed.
- b. If you are an admin user, you also see the list of User groups that are defined. You can select or clear selected groups that you are a member of.
- c. The **Change My Password** option is not available when LDAP authentication is enabled.

To change your password, click **Change My Password**. For more information, see [Changing your password \(on page 21\)](#).

3. Click **Submit**.

Your amended user details are saved.

## Changing your password

You can change your password by logging on to the Remote Control server UI.

To change your password, you must enter your current password too. To change your password, complete the following steps.



**Note:** The **Change My Password** option is not available when LDAP authentication is enabled.

1. Click **Users > Change My Password**.
2. Type your current password, new password, and retype your new password.
3. Click **Submit**.

Your new password is saved if the current password that you enter matches the password that is saved in the database. If it does not match, an error is displayed and you must retype your current password. The new password must conform to the password rules that are defined for your environment. If it does not, an error is displayed.

## Viewing the list of user groups that you belong to

To view a list of User Groups that you are a member of, use the **My Groups** option.

To view the list of groups, click **Users > My Groups**.

The **Selected User Groups** screen is displayed listing the user groups.

## Sessions menu options

### Viewing your session history

Use the **My Session History** option to view a list of all previous sessions that you have established with a target.

To view your session history list, click **Sessions > My Session History**.

The **My Session History** screen is displayed.

## Searching for specific sessions

Using the search utility for sessions, you can search for a specific previously established session or find a session by using a specific or nonspecific search criteria.

To search for a session, complete the following steps:

1. Click **Sessions > Search**.

The Search Session screen is displayed.

2. Type in your session search information.

Enter information about the target that was connected to the session.

- To search for sessions, use all or part of any of the following target information:
  - manufacturer
  - model
  - serial number
  - computername



**Note:** The information entered is not case sensitive.

3. Click **Submit**.

- If any matching targets are found within the session information, the session details for these are displayed.
- If no matching targets are found, a message is displayed and the sessions list is blank.

## Viewing session details

The **Session Details** action is available when a target is selected from either the **My Session History** report or the **Search Sessions** report. Details of the controller system, the policies and values set for the session, and any audit log entries for both the controller and target are displayed.

To view session details for a specific session, complete the following steps:

1. Click **Sessions**.
2. Select either **My Session History**, **All Session History**, or **Search**. Follow steps in [search sessions \(on page 22\)](#) to generate the report when selecting search.
3. Select a target from the list.
4. Choose the appropriate method to select Session details.
  - Select **Sessions > Session details**
  - Select **Session details** from the action list on the left.

The remote control session information screen is displayed showing details of the controller system and the policies and permissions that were applied to the session. If the Force Session Audit policy was set to Yes for the session, any audit entries that were saved for the controller and target are also shown. If the Force Session Recording policy

was set to Yes there is also a link to play back the recording of the session. For details about setting policies and permissions, see the BigFix® Remote Control Administrator's Guide.

## Playing a recording from the Session details page

When you are viewing the session details page for a specific remote control session use the **Play the recording of this session** link to view a recording of the session.



**Note:** The link is available only if the **Force Session Recording** policy was set to Yes for the session.

To Playback a recording complete the following steps:

On the Session Details screen, click **Play the recording of this session**.

The Session Recording Player window opens and the recording begins to play.

The following buttons and functions are available during the playback

### **Pause**

To pause the recording while playing.

### **Stop**

To stop the recording and clear the playback window.

### **Enable Auto Scrolling View**

To scroll up, down, right or left by moving the mouse over each edge of the playback window.

### **Enable Scaled View**

To scale down the display of the recording to show the full recorded window inside the playback window.

## Reports menu options

Use the **Reports Menu** to create or run reports. The menu items displayed are determined by the authority of the user who is logged on. This section describes the options available to a user with user authority. A Super User or Admin authority have more options available and these are explained in the BigFix® Remote Control Administrator's Guide.

The Reports menu for a user shows all Standard and Custom Reports that the user has access to run.



**Note:** If you do not have access to any Custom Reports, the Reports menu does not contain any items.

## Running standard reports

There are a number of standard reports that are provided in the BigFix® Remote Control Server which provide information about users, targets, and groups.

To run a standard report, complete the following steps:

1. Click **Reports > Standard Reports**.
2. Click the required standard report name.

The output of the standard report is displayed on the screen.

## Running custom reports

Custom reports are created by Super Users or Administrators. When saving the custom query, they can select a group or groups that have permission to run the report. The reports menu, for all members of the selected groups, is populated with a custom reports item. Select this item to see a list of available custom report menus and their corresponding reports. For more information about creating custom reports, see the BigFix® Remote Control Administrator's Guide.

To run a custom report, complete the following steps:

1. Click **Reports > Custom reports**.
2. Click the menu item that the custom report belongs to.
3. Click the required custom report name.

The output of the custom report is displayed on the screen.

## Options menu

Use the **Options** menu to perform actions on reports. For additional options that are available only to Super Users and Admin Users, see the BigFix® Remote Control Administrator's Guide. Use the Options menu to set your homepage, choose page display options, or format the data for output to other applications.



**Note:** On screens that are not in a report format, for example search screens or input screens, the Options menu is not visible in the menu bar.

To work with the Options menu click **Options** and select from the following choices.

- Set Current Report as Homepage
- Reset to Default Homepage Report
- Refresh Results
- Page Options
- Output

## Setting your homepage

Use this option to make the currently displayed report your homepage. This is the initial screen that appears when you logon to the BigFix® Remote Control Server user interface.



To set a default homepage, complete the following steps:

1. Generate the required report by running a standard report from any of the BigFix® Remote Control Server menus or run a custom report that you have access to from the Custom reports menu.
2. Click **Options > Set Current Report as Homepage**.

For example, to make the Favourites report your homepage:

- a. Click **Targets > Favourites**.
- b. Click **Options > Set Current Report as Homepage**.

The next time you log on to BigFix® Remote Control Server the **Favourites** report is displayed as the initial screen.

## Resetting your homepage

The default homepage for the BigFix® Remote Control Server is defined by the property **default.query** in the `trc.properties` file. This property is used to determine the initial page that is displayed when a user logs on to the application if **no other** default homepages have been set. For details about editing the properties files, see the BigFix® Remote Control Administrator's Guide. If you have previously set your homepage to a different page, by selecting the **Set Current Report as Homepage** option, change it back to the default homepage by selecting **Reset to Default Homepage Report**.



**Note:** Next time you log on, the page that is initially displayed is determined by either the value set in **default.query** or by any default homepages that have been set for the groups you are a member of. For details about how homepages are determined, see the BigFix® Remote Control Administrator's Guide.

To reset to the default homepage, click **Options > Reset to Default Homepage Report**.

**Example 1:** The All targets report is defined as the default homepage and you had selected the Favourites report as your homepage. If there are no default homepages set for any of the groups that you belong to and you select **Reset to Default Homepage Report**, if you logoff and logon the All targets report is the first page you see.

**Example 2:** You are a member of user group `testtargets` and a default homepage of *targets manufactured by companyX* has been set for the group. If you select **Reset to Default Homepage Report**, logoff and logon again, the *targets manufactured by companyX* is the first page that is displayed.

## Refreshing the data that is displayed on screen

Whenever a report is generated in BigFix® Remote Control Server a query is run against the database to retrieve the required data and display it on the screen. This data is held in a temporary location for the next time the same report is run so that the data is displayed more quickly on the screen. To ensure that the latest data is reported to the screen, including any updates that have taken place since the last time the report data was displayed, click **Options > Refresh Results**. The report is updated with any changes or updates that have been made.



**Note:** Use the **Refresh** link on the upper right for the same purpose.

## Setting page display options

Use this option to select the number of rows of output to be displayed on the screen particularly if the report to be displayed is large. Select the number of rows per page to display, from the list.

## Exporting data in various formats

Use the options in the **Output** menu to export report data into various formats. You can save, email, or print the data.

To export the report data, complete the following steps:

Click **Options > Output** and select one of the following options:

### CSV File(UTF-8)

Generates a comma-separated values file, that uses **UTF-8** encoding, containing the data from the currently displayed report.

On the file download window select one of the following options:

- Click **Open**, to open the report in csv format.
- Click **Save** to save the report data as a **.csv** file.

### CSV File(UTF-16LE)

Generates a csv file, that uses **UTF-16LE** encoding, containing the data from the currently displayed report.

Follow the instructions in CSV File(UTF-8), to create and save the file

### TSV File(UTF-8)

Generates a tab-separated values file, that uses **UTF-8** encoding, containing the data from the currently displayed report.

On the file download window select one of the following options:

- Click **Open**, to open the report in tsv format.
- Click **Save** to save file as a **.tsv** file.

### TSV File(UTF-16LE)

Generates a tsv file, that uses **UTF-16LE** encoding, containing the data from the currently displayed report.

Follow the instructions in TSV File(UTF-8), to create and save the file

### Email Report

Sends the currently displayed report as a csv file, in an email.

- a. Generate the required report.
- b. Click **Options > Output > Email Report**. The **Email Report** screen is displayed.
- c. **E-Mail To**: type the Email address of the recipient.
- d. **Email Contents**: type the content for your email.
- e. Click **Send**.

The current report is attached to the email as a csv file and is sent to the recipient's email address.



**Note:** Email must be enabled for this option to work. If email is not enabled, a message is displayed.

### Printable Report

Displays the current report in a new browser window with no menus, for easier printing.

- a. Generate the required report.
- b. Click **Options > Output > Printable Report**. A new window opens with the report displayed.
- c. To print the report, select print from the **File** menu in the action bar.

## Tools menu options

The Tools menu provides a set of utilities that can be downloaded and installed. These include the target, controller, and command line interface components and the utility used for playing back a recording of a session. For additional options also available to an administrator, see the BigFix® Remote Control Administrator's Guide.

### Downloading tools from the BigFix® Remote Control Server

Use the **Downloads** option to obtain the files required for installing various Remote Control components. You can download or run the player used to playback session recordings and download the installation files for the target, controller, and command line interface components.

### Starting the Remote Control Session Player

Use the Remote Control session player to play recordings of sessions that have been made and saved locally to your system.

Start the Session Player using Java™ Web Start by performing the following steps:

1. Click **Tools > Downloads**.  
The **Downloads** page is displayed, showing the available items for download.
2. Click **Launch Remote Control Player**.
3. On the file download window select **Run** or **Save**  
for the **TRCPlayer.jnlp** file. For more details about playing a local recording, see [Recording section \(on page 82\)](#).

## Downloading the Session Player

Use the Session Player to play back recordings of sessions that have been saved locally on your system. For more details on Session Recording, see [Local Recording of a session \(on page 82\)](#). To download the session player, complete the following steps:

1. Click **Tools > Downloads**.
2. Click **Download Remote Control Player**.
3. Save the file to the required location.



**Note:** Some browsers will save the file as a `.zip` file. Rename the file `TRCPlayer.zip` to `TRCPlayer.jar`.

---

### Related information

[Playing a local recording \(on page 82\)](#)

## Downloading the component software from the server

Use the **Agent Downloads** function to download files for installing the target, controller, or command-line software. When you select this function, the agent downloads window is displayed listing the available items that can be downloaded.

### Downloading the Windows™ target software

Use the Agent Downloads option to run or save the file that is required for installing the Windows™ target software.

1. Click **Tools > Downloads**.
2. Click **Agent Downloads**.
3. Select **trc\_setup\_target.exe**.
4. On the file download window, select **Run** or **Save**.

If the target software is already installed, an upgrade prompt is displayed. Click **Yes** to continue the installation. For more information about installing the target software, see the *BigFix® Remote Control Installation Guide*

### Downloading the Linux™ target software

Use the Agent Downloads to run or save the file that is required for installing the Linux™ target software.

1. Click **Tools > Downloads**.
2. Click **Agent Downloads**.
3. Select **trc-target-10.x.x.<arch>.rpm**.

Where *10.x.x* is the version that you want to install.

4. Click **Save**.

For more information about installing the Linux™ target software, see the *BigFix® Remote Control Installation Guide*.

## Downloading the Windows™ controller software

Use Agent Downloads option to run or save the file that is required for installing the Windows™ controller software.

1. Click **Tools > Downloads**.
2. Click **Agent Downloads**.
3. Select **trc\_controller\_setup.exe**.
4. Select **Run** or **Save**.

### Run

To begin installing the controller software.

- a. Click **Next** at the welcome panel.
- b. Accept the license agreement, click **Next**.
- c. Accept or change the location for the installation files, click **Next**.
- d. Click **Install**.
- e. Click **Finish**.



**Note:** If the controller software is already installed, repair or remove options are available.

### Save

To save the **trc\_controller\_setup.exe** file to a selected location.



**Note:** Run the executable file to install the controller software.

## Downloading the Linux™ controller software

Use the Agent Downloads option to run or save the file that is required for installing the Linux™ controller software.

1. Click **Tools > Downloads**.
2. Click **Agent Downloads**.
3. Select **trc-controller-10.x.x.noarch.rpm**.  
Where 10.x.x is the version that you want to install.
4. Select **Save** to save the rpm file.
5. Use the following command to install the controller software.  
Where 10.x.x is the version that you want to install.

```
$ rpm -ivh /PATH/trc-controller-10.x.x.noarch.rpm
```

Where PATH is the path to the location that you saved the rpm file to.

## Downloading the Windows™ command-line files

Use the Agent Downloads option to run or save the file that is required for installing the Windows™ command-line software.

1. Click **Tools > Downloads**.
2. Click **Agent Downloads**.
3. Select **trc\_cli\_setup.exe**.
4. Select **Run** or **Save**.

### Run

Select **Run** to begin installing the command-line software.

- a. Click **Next** at the welcome pane.
- b. Accept the license agreement, click **Next**.
- c. Accept or change the location for the installation files, click **Next**.
- d. On the server address pane, enter the relevant information and click **Next**.

#### Server host name

Enter the IP address or server name of the BigFix® Remote Control Server.

#### Server port

Enter the port number that the server is listening on.

#### Use secure connections(https)

Select https to use secure connections to contact the server.

#### Server context

Enter a value for the server context. For example, `trc`.

#### Use a FIPS certified cryptographic provider

Select to install FIPS-compliant tools.

#### Enable NIST SP800-131A compliance (Enables FIPS)

Select to install NIST SP800-131A compliant tools.

#### Advanced settings

Click to set the context and server port.

- e. Enter the relevant information on the **Proxy settings** pane.
  - If you are not using a proxy server or remote control gateway, click **Next**.
  - If you are using a proxy, select **Use a proxy server or a Remote Control Gateway**.  
Type in the relevant information.

- Type in the host name or IP address for the proxy server.
  - Type in the port that proxy server is listening on.
  - Select **Use an HTTP proxy** or **Use a Remote Control Gateway**.
  - Select **Proxy requires authentication** and enter the User id and password for authenticating to the proxy server.
  - Click **Next**.
- f. Accept the default port or type in a relevant value, click **Next**.
- g. Click **Install**.
- h. Click **Finish**.

### Save

Select **Save** to save the `trc_cli_setup.exe` file to a specific location.



**Note:** Run the executable file to install the command-line software.

The following executable files are in the selected directory.

- `wrc.exe`
- `wrcmdpcr.exe`

For more information about using the tools, see [Use remote control commands from the command line \(on page 97\)](#).

## Downloading the Linux™ command line files

Use the Agent Downloads option to run or save the file that is required for installing the Linux™ command-line software.

1. Click **Tools > Downloads**.
2. Click **Agent Downloads**.
3. Select **trc-cli-10.x.x.<arch>.rpm**.  
Where *10.x.x* is the version that you want to install.
4. Select **Save** to save the rpm file to the required location.
5. To install the package, follow the instructions from the Installing the CLI tools in Linux topic.
6. When the installation is complete edit the `/etc/trc_target.properties` file and set your configuration.
  - Set the value of **ServerURL** to the host name or IP address of your BigFix® Remote Control Server
  - For FIPS compliance set the value of **FIPSCompliance** to Yes.
  - For NIST SP800-131a compliance, set the value of *SP800131ACompliance* to yes.
7. Save the file.



**Note:** If you install the CLI tools on a computer that does not have the target software installed, you must uninstall the CLI tools before you install the target software. Use the following command to remove the CLI tools.



```
$ rpm -e trc-cli
```

## Getting help

Use the **Help** menu to see the version of the BigFix® Remote Control Server that is installed and to access the online documentation.

### **Online Documentation**

Remote Control information center where you can view the latest documentation.

### **About Remote Control**

Displays the version number of the currently installed server software.



# Chapter 3. Remote control sessions

Use remote control sessions to establish a connection to a computer in your environment to observe or actively control the computer remotely. In the session the controller user's keyboard and mouse become the primary keyboard and mouse for the remote system. Functions such as chat, guidance, reboot, and file transfer are some of the options available for use in a remote control session.

There are seven remote control session modes

- Active
- Chat only
- Guidance
- Monitor
- File Transfer
- Reboot
- Command

For more details of the session types, see [Types of remote control sessions that can be established \(on page 34\)](#).

There are four ways that a remote control session can be established

## **From the Remote Control server**

A remote control session in which the controller user starts the session from the Remote Control server. The controller component starts and contacts the target to send the session request. The target contacts the server to authenticate the request and obtain the policies and permissions for the session. For more information on policies and permissions for a managed remote control session, see the *BigFix® Remote Control Administrator's Guide*. If the target cannot reach the server the session is refused.

## **In peer to peer mode**

A remote control session that is established directly between the controller and the target. The controller user starts the controller component locally and specifies the target that they want to takeover remotely. The local properties that have been set on the target are used for the session. For more details of target properties, see the *BigFix® Remote Control Administrator's Guide*.

## **Using the broker component**

A remote control session that is established with targets outside the managed enterprise network. This type of session requires the targets to be managed by an Remote Control server. The broker component is used for making the connection between the controller and target machines. For details on installing and configuring the broker component, see the *BigFix® Remote Control Installation Guide*.

## **From the Remote Control Console**

A remote control session in which the controller user initiates the session from the Remote Control site within the Remote Control console. For more details, see the *BigFix® Remote Control Console User's Guide*.

## Types of remote control sessions that can be established

When establishing a remote control session with a target you can choose the type of session to take part in. The session types available are defined by the policies that have been set for the session.

### Active Mode

Connect to a target and obtain full remote control of the target. You can view the target's screen and control the remote mouse and keyboard. For more details, see [Taking full control of a target system \(on page 34\)](#).

### Chat Only

Use Chat only mode to chat to the target user. You are not able to view the target's screen. See also [Chatting to the target user during a remote control session \(on page 61\)](#).

### Monitor Mode

Connect to a target to view the target's screen to monitor activity. You have no control over the remote mouse or keyboard.

### Guidance [\(on page 39\)](#)

Connect to a target to view the target's screen and add guidance icons to it. You have no control over the remote mouse or keyboard. For more details, see [Providing guidance to the target user \(on page 39\)](#).



**Note:** Maximising a window on the target or performing something which requires a repaint of the target screen may remove them.

### File Transfer [\(on page 36\)](#)

Connect to a target to view the target's file system and transfer files and directories from your system to the target and vice versa. For more details, see [Transferring files and directories \(on page 36\)](#).

### Reboot [\(on page 43\)](#)

Use the Reboot session type to connect to a target and restart it.

### Command Session Mode [\(on page 43\)](#)

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.

## Taking full control of a target system

You can connect to a target and obtain full remote control of the target system by establishing an **Active** session. When you connect in active mode you can view the target's screen and have full remote input control by controlling the remote mouse and keyboard. This mode is useful when there are no privacy issues and the target user consents

to giving you full access to their machine. Active mode incorporates all the functions of the other remote control session types.




**Note:** The functions available in the session will be determined by the session policies that have been set. For details of how policies are derived for a session, see the BigFix® Remote Control Administrator's Guide.

## Chatting to the target user

You can participate in an online conversation with the target user by starting a **Chat** session. During this type of session the target screen is not visible to you.

After you have established a **Chat** session, type your message in the lower window and click **Send**.

The message is sent to the target and the target user sees the message on their screen. The message is also displayed in the view area in your chat window. Click **Clear** to remove any message from your view only. The chat history is still be visible on the target screen.

**Copy Selected text** and **Paste**  are functions also available during a chat session.

### Copy selected text

Use to copy text from the chat area to another location.

1. Select the required text within the chat window.
2. Click **Copy selected text**. This text can be pasted into another location on your system. For example, to be added to an email.

### Paste

Use to paste text into the chat area.

1. Select and copy text that is not in the chat window. You can use CTRL+C to copy. For example, from a open document.
2. In the controller window click **Paste**. The text is pasted into the input field of the chat window.
3. Click **Send** to forward the text to the target user.



**Note:** You can also chat to a target user during other types of remote control session. For more details, see [Chatting to the target user during a remote control session \(on page 61\)](#). Depending on the policies set for the session, this option might not be available.

## Transferring files and directories

File Transfer Mode is a connection mode that you can use to remotely connect to a target. When connected in File Transfer Mode you can view the target's file system and transfer files and directories from the controller machine to the target and vice versa. There is also an option to delete files and directories and create a directory.

When the connection is established the controller window displays two panes. The pane on left shows the controller's file system, the pane on the right shows the target's file system.

The behavior of file transfer sessions in peer to peer mode has changed with Version 9.1.4 FP1. Up to Release 9.1.4 GA, when a file transfer session was established in peer-to-peer mode, the permissions used to access the target file system were set to System access on Windows and root access on Linux. With this Fix Pack, the permissions used on the target file system are those of the logged on user. A new target configuration option, **EnableFileTransferSystemAccess** is used to implement the new behavior.

### Transferring files and directories from controller to target

When you are connected to a target in a File Transfer Mode session you can transfer one or more files or directories from the controller machine to the target machine.

To copy one or more files or directories from the controller to the target complete the following steps:

1. Select the right pane and navigate to the location that the files or directories should be copied to on the target.
2. Select the left pane and navigate to the location of the files or directories to be copied.
3. Select the required files or directories. Hold the CTRL key while holding the left mouse button to select multiple items.
4. Choose the appropriate method to complete the file transfer by doing **one** of the following actions
  - Drag the file or directory to the right pane. You can only do this when copying 1 item.
  - Click **Copy**.

The selected files or directories appear in the target file system.

### Transferring files and directories from target to controller

When you are connected to a target in File Transfer Mode session you can transfer one or more files or directories from the target machine to the controller machine.

To copy one or more files or directories from the target to the controller complete the following steps :

1. Select the left pane and navigate to the location that the files or directories should be copied to on the controller.
2. Select the right pane and navigate to the location of the files or directories to be copied.
3. Select the required files or directories. Hold the CTRL key while holding the left mouse button to select multiple items.
4. Choose the appropriate method to complete the file transfer by doing **one** of the following actions

- Drag the files or directories to the left pane. You can only do this when copying 1 item.
- Click **Copy**.

The selected files or directories appear in the controller file system.

## Displaying and hiding file information

Select the file and directory information that you want to display in a file transfer session. The columns that are displayed in the left and right panes of the session window can be displayed or hidden.

You can display the following file and directory information.

- Size. For files only.
- Date created. Displayed in Coordinated Universal Time.
- Date modified. Displayed in Coordinated Universal Time.
- Attributes. The following file attributes can be listed.

**Table 1. File attributes**

Attribute	Description	Controller file system	Target file system
A	Archive	*	*
R	Read-only	*	*
D	Directory	*	*
H	Hidden	*	*
S	System	*	*
C	Compressed		*
E	Encrypted		*
I	Indexed		*

When you hover the mouse over an entry in the table, a tooltip displays the same information. The operating system that you are running determines which columns you can hide or display. The **Date created** and **Attributes** columns are not available when you are running a Linux operating system. Use the following options to configure the session view.

In the pane that you want to configure, right-click the column heading row and complete the steps for the relevant option.

- Display a column

Select the column name that you want to display.

- Hide a column

Clear the selected column name that you want to hide.

- Synchronize the panes

Select **Synchronize Table Panes** to display the same column headings in the left and right panes. This option is selected as default, the first time you start a file transfer session. However, note that the pane that you select **Synchronize Table Panes** in determines what is displayed in both panes. If **Synchronize Table Panes** is not selected and you select it in the left pane, the column headings in the right pane are overwritten with the column headings in the left pane.

At the end of the session, the column selection is saved and is displayed the next time that you start a file transfer session.

## Deleting files or directories during a file transfer session

When you are connected to a target in a File Transfer Mode session you can delete files and directories from the controller machine and the target machine.

To delete one or more files or directories complete the following steps:

1. Select the left pane to delete from the controller OR select the right pane to delete from the target
2. Navigate to and select the required files or directories.  
Hold the CTRL key while holding the left mouse button to select multiple items.
3. Click **Delete**.
4. Click **Yes** to delete.

The selected files or directories are removed from the controller or target file system.



**Note:** Click **Refresh** to refresh the contents of the panes if the files or directories do not immediately disappear.

## Creating directories during a file transfer session

When you are connected to a target in a File Transfer Mode session you can create directories on the controller and target machines.

To create a directory complete the following steps:

1. Select the left pane for the controller file system OR select the right pane for the target file system.
2. Navigate to the required the location for the new directory.
3. Click **New Directory**.
4. Type in a name for the directory and click **OK**.

The new directory is created on the controller or target system.



**Note:** Click **Refresh** to refresh the contents of the selected pane and clear any selections.

## Viewing the list of transferred files

When you are connected to a target in a File Transfer Mode session you can display the list of items that have been transferred during the session. After you have displayed the file list you can select to hide the list from view.

To display the list of transferred items, click **Show Transfers** in the file transfer session window.

A **File Transfers** window opens, displaying the list of transferred items. You can select an item and click the red 'X' to delete the item from the list. You can click **Open transfer folder** to show the contents of the file transfer folder on the controller.



**Note:** When you click **Show Transfers** it changes to **Hide Transfers**. Click **Hide Transfers** to close the **File Transfers** window.

## Providing guidance to the target user

You can remotely connect to a target system to provide guidance to the target user to help solve a problem. When connected in guidance mode you can view the target's screen, but have no input control. You cannot control the remote mouse or keyboard. However through a series of graphically implicit icons you can guide the target user to perform necessary tasks on the target machine. This type of session mode is often used in training situations, and in workplaces of very high sensitivity. For example, financial institutions.



**Note:** Maximizing a window on the target or performing something which requires a repaint of the target screen may remove them.

Use the on-screen guidance symbols and the chat function to guide the target user through any task they have to perform on the target machine.

## Tools for providing instructions to a target user

During a guidance session with a target, you can use various tools to provide instructions for the target user. You can show them where to click their screen or to highlight a particular part of the screen. The tools are available in the **Perform action in target** menu in the controller window.



**Note:** Apart from the **Guidance Tool** and the **Mouse Tool**, the tools are also available during an active session.

### Guidance Tool

Use this tool to direct the target user, by placing symbols on the screen to show them what and where to click. For more information, see [Using the guidance tool \(on page 40\)](#).

### Drawing Tool

Use this tool to draw simple colored lines on the target screen. For example, to circle something for the target user to note.

### **Highlight Tool**

Use this tool to highlight parts of the target screen.

### **Mouse Tool**

Use this tool to display your mouse cursor in the target system so that the target user can see your mouse as it moves around their desktop.

### **Clear Instructions**

Use this tool to clear all guidance instructions from the targets screen.

## Using the guidance tool

Use the guidance tool to place symbols on the target screen to show the target user what to click on their screen or where to click.

To use the guidance tool complete the following steps :

1. Click **Perform action in target > Guidance Tool**.
2. Move your mouse to where you want the target user to place their mouse and click the mouse button you want them to click.  
For example, the left mouse button. A list of actions appears.
3. Select the action you want the target user to perform.  
For example, **Single Click**.

The guidance symbol for the selected action is displayed on the screen indicating to the target user which button on the mouse to click and which action to perform on that button.

Use [Removing guidance instructions from the screen \(on page 43\)](#) to remove all symbols placed on the remote screen.

## Guidance Tool Symbols

Use the guidance tool to display action symbols on the target screen to indicate to the target user which mouse button that they should press and what action should be taken. The following actions are available.

### **Cancel**

to cancel the mouse action you just performed. A guidance symbol is not placed on the target screen.

### **Move**

to move the target mouse to this particular point on the screen.

### **Single click**

to click the target mouse button once.

### **Double click**

to click the target mouse button twice.



**Drag Start**

to click and hold the target mouse button and start to drag the mouse.

**Drag Stop**

to continue to drag the mouse then release the mouse button at this point.




The following table shows the relevant actions and their symbols.

**Table 2. Mouse Action Symbols**

Single Click Left button	Single Click Right button	Double Click Left button.	Double Click Right button.	Drag Start	Drag Stop
					

The mouse button that you click determines which mouse button on the guidance symbol is shaded. This will indicate to the target user which button to press. The following table gives examples of the symbols showing how each mouse button action will look.

**Table 3. Mouse action symbols**

Left button	Middle button	Right button
		

## Using the drawing tool

Use the **Drawing Tool** to draw basic colored lines on the target screen to mark the parts of the screen you want the target user to take note of.

To use the drawing tool complete the following steps :

1. Click **Perform action in target > Drawing Tool**.



The cursor changes to the drawing tool cursor within the session window.

2. To draw a line move the mouse while holding down the left or the right mouse button.



**Note:** Using the left button produces blue lines, the right button green lines and the centre button, or right and left together, produces red lines.

Use [Removing guidance instructions from the screen \(on page 43\)](#) to remove all lines drawn on the remote screen.

## Using the highlight tool

Use the **Highlight Tool** to highlight an area on the target screen.

To use the highlight tool complete the following steps :

1. Click **Perform action in target > Highlight Tool**



The cursor changes to the highlight tool cursor within the session window.

2. To highlight text on the target machine screen move the mouse while holding down the left or the right mouse button. Release the mouse button when you have highlighted the required area.

Use [Removing guidance instructions from the screen \(on page 43\)](#) to remove all highlights.

## Displaying the controller mouse cursor on the target system

Use the **Mouse Tool** option to display the controller user's mouse cursor on the target system during a guidance session. The target user can see the position of your mouse cursor as it moves around the target desktop.

The **Mouse Tool** option is available only in guidance mode. When you enable the tool, it remains enabled until you select a different guidance tool, or you select a different session type. When you clear the **Mouse Tool** option, the mouse cursor icon is displayed in the last position before you cleared the option.

To enable the **Mouse Tool**, click **Perform action in target > Mouse Tool**. Your mouse cursor is displayed on the target



system with a remote control icon next to it.

To remove the cursor icon from the target desktop after you disable the **Mouse Tool**, select **Perform action in target > Clear Instructions**.



**Note:**



The **Mouse Tool** is disabled when you are in a session with a Linux™ target or an BigFix® Remote Control Target for macOS. It is also disabled if the target component that is installed is earlier than V9.1.4.

## Removing guidance instructions from the screen

Use the clear instructions function to remove any guidance symbols, drawn lines, or highlighted areas you have placed on the remote control session screen.

To clear instructions, click **Perform action in target > Clear Instructions**

All guidance symbols are removed from the screen.



**Note:** Maximising a window on the target or performing something that requires a repaint of the target screen may remove them.

## Rebooting a target machine

Reboot mode is a connection mode you can use to remotely reboot the target machine.

To reboot, select **Reboot** from the session type list. A reboot message is displayed. There is an option to reconnect in a different session mode if required. The target machine shuts down and restarts.

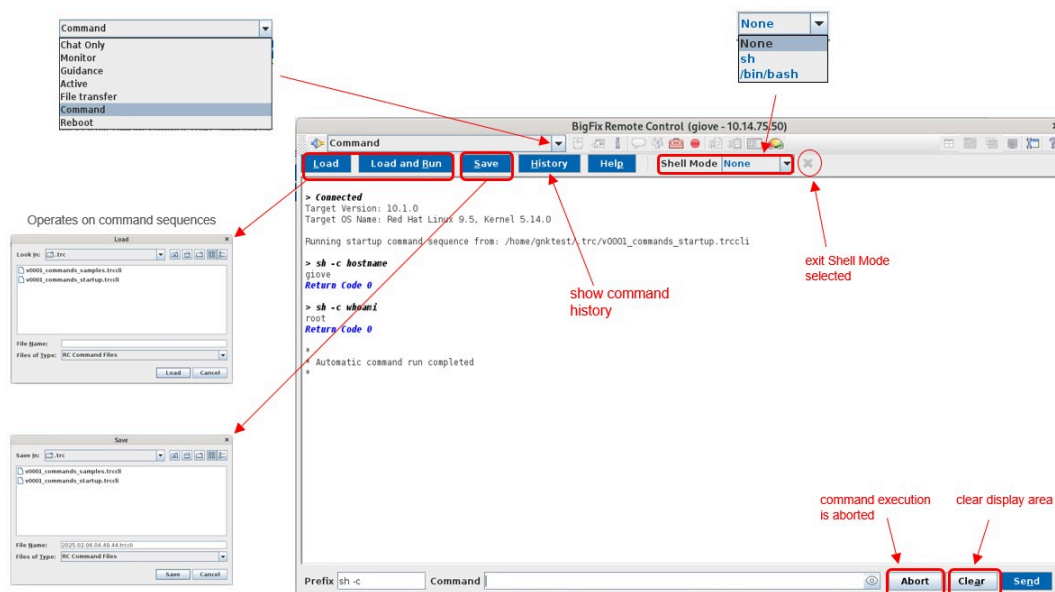
## Command Session Mode

The command is executed as a standalone invocation without a command shell on the target side that inherits state between commands. In other words, there is no way to interact with the invoked command.

- **Shell mode set to None** - Each command is executed on the target in its own process that terminates at the end of the process.
- **Shell Mode not set to None** - A shell process is started on the target and piped via the forth protocol with the controller. The shell is active and persistent until exited.

The interaction possible with the remote shell are those via the command line. That is, it's not possible to start an editor (such as "notepad" or "vi") or other similar processes that rely on the existence of a terminal (tty) as there is no terminal concept in current implementation.

Figure 1. Command Session Mode



- **Abort:** This button will instantly kill the shell process and its children, thus the processes started through a command.
- **Load:** This button will allow the system to read a selected **.trccli** file and display its contents in the command window without executing them. The user can execute a command loaded by pressing the **ESC** key and its relative command index.
- **Load and Run:** This button loads a **.trccli** file and immediately starts executing the command sequence defined in the file. Execution follows the order specified in the **<history>** section, using the **<autorun>** settings to determine behavior such as stopping on failure or applying a delay.
  - A **.trccli** file consists of two main sections: **<autorun>** and **<history>**. The **<autorun>** section defines execution settings, while the **<history>** section contains command sequences.
    - The **<autorun>** section includes the following elements: **<enable>** set to true or false, **enable or disable automatic execution**, **<stopOnFailure>** set to true or false to define whether execution stops on failure, **<delay>** set to the number of seconds before execution begins.
    - The **<history>** section contains multiple commands, each defined by three elements: **<platform>** specifies the operating system (windows, linux, macos), **<prefix>** defines the command interpreter (cmd /c, powershell, sh -c, bash -c, etc.), and **<command>** that contains the actual command to execute. Each command must be on a separate line and begin with **<platform>** at column 0. Commands for different platforms should be grouped accordingly. To reference paths or arguments with spaces, use single double quotes or the @ symbol when in command mode. Avoid using double double-quotes.

Example command sequences:

```
For Windows :
<platform>windows</platform>
```

```
<prefix>cmd /c</prefix>
<command>net start | findstr BigF</command>
```

For Linux:

```
<platform>linux</platform>
<prefix>sh -c</prefix>
<command>grep -E '^(VERSION|NAME)= ' /etc/os-release</command>
```

For macOS:

```
<platform>macos</platform>
<prefix>sh -c</prefix>
<command>sw_vers</command>
```

- **Save:** This button will create a `.trccli` file containing all the commands run during the command session. A user can use the generated file to load the command.
- **History:** This button will print all the commands run during the command session.



**Note:** This program is run in 32-bit mode when executed on Windows. As a result, the command line, PowerShell, and any other sub-processes launched by the application will also operate in 32-bit mode, along with the usual limitations and compatibility considerations of a 32-bit application.

## Starting a remote control session from the server

You can start a remote control session from the BigFix® Remote Control Server when you select a target from any report displaying one or more targets. Some examples of these reports are

### All Targets

to create this report, see [Viewing all targets \(on page 12\)](#).



**Note:** This report also displays the userid of the user who is logged on to the target.

### Recently Accessed

to create this report, see [Viewing recently accessed targets \(on page 14\)](#).

### Favourites

to create this report, see [Viewing the favorite targets list \(on page 13\)](#).

### Search Targets

to create this report, see [Searching for targets \(on page 12\)](#).

The following steps detail how to start a session from the All targets report, for the others, see the relevant sections for displaying these reports then follow from step 2 ([on page 46](#)) below

To start a session, complete the following steps:

1. Click **Targets > All Targets**.
2. Select the target.
3. Click **Start session**

The start session screen is displayed. This screen gives the details for the selected target including the version of target software installed and the policies and permissions that will be assigned for the session.

4. Click the session mode button corresponding to the session type you want to start.
5. When the Open or Save window is displayed, select **open**.

The controller starts to run and the session is either accepted or refused.

If the session is accepted, the connection is established and the controller window is displayed, showing the target screen. The IP address of the target is displayed in the heading of the controller window. This is helpful for keeping track of who you are connected to if you have multiple sessions running at the one time.

If the session is refused a message is displayed .

Session refusal can occur for a number of reasons,

- The target user has clicked refuse on the acceptance window, if user acceptance was required for the session.
- The target user has not accepted the session within the given time. This is determined by the acceptance grace time policy and if the acceptance timeout policy was set to abort.
- The target is already in a remote control session, in which case a message is displayed showing who is connected to the target.

For details of policies, see the BigFix® Remote Control Administrator's Guide.



**Note:**

1. If the session mode buttons are not displayed on the **Start Session** screen and an error message is displayed the following cases can be the reason for this.
  - The user or target are not a member of any groups.
  - No permissions links are defined for any of the groups that the user and target belong to.
  - The target is offline.
  - None of the session mode policies have been set to Yes.

For details of groups, policies, and permissions, see the BigFix® Remote Control Administrator's Guide.

## Starting a peer to peer session

When a remote control session request is initiated from the server, the controller is launched and it contacts the target to send the session request. The target contacts the server to authenticate the request and obtain the policies and permissions for the session. Peer to peer remote control sessions are remote takeover sessions not initiated

from the server, they are established directly between the controller and the target. When peer to peer mode is enabled on the target and the server is down or cannot be reached by the target, the session is established directly between the target and the controller. The local policies that have been set on the target are used for the session. You can set the peer to peer policies during installation of the target or after installation by configuring the target properties.

You can start a peer to peer session with a target that has been enabled for peer to peer connections by running the controller locally on your system. If you have an Remote Control server installed you can download and install the controller from there. For details, see [Downloading the component software from the server \(on page 28\)](#). For details of installing the controller component, if you do not have a server installed, see the *BigFix® Remote Control Installation Guide*.

After installing the controller you can start a peer to peer session by completing the following steps :

1. Start the controller.

#### **Windows® systems**

- a. Click **Start > All Programs**
- b. Click **Remote Control > Controller**

#### **Linux® or UNIX® systems**

To start the controller locate the Remote Control controller application from the operating system application interface or issue the following command

```
/opt/bigfix/trc/controller/trc_controller.sh
```

The Controller application can be also started using the following menu entries **Applications > Internet > BigFix Remote Control - Controller**

#### **macOS systems**

- a. Open Finder (Applications folder) or Launchpad.
- b. Locate the **Remote Control Controller** application and open it.

2. In the **Open Connection** window:

- a. Enter the IP address of the target you want to start a session with
- b. Enter the port used by the target for listening the incoming connections (unless changed the default port is 888 or 8787 depending on the OS)
- c. Select **Use proxy** to use a proxy
- d. Select the required protocol and provide the required information.

#### **Server**

Enter the host name or IP address of the proxy server.

#### **Port**

Enter the port required for the proxy server.

#### **Proxy requires authentication**

Select this option if you require to authenticate with the proxy server. Provide the username and password that is required for authentication.

3. Click the required session type.



**Note:** If the target has a Windows® operating system installed, and the **CheckUserLogin** policy is set to Yes, a login window opens. Enter a valid Windows™ ID and password to continue. If the target is already in a remote control session you might have the option to join or disconnect the session, depending on other target properties that have been set. For more details see, [Connecting to a target that is already in a session \(on page 50\)](#).

Successful connection to the target is established when any of the following conditions are met.

- No user acceptance policies have been enabled for accepting the session.
- User acceptance policies for accepting the session have been enabled and the target user has accepted the request. For more details on consenting to a remote control session, see the *BigFix® Remote Control Target User's Guide*.

After the session is accepted and established, the policies set locally on the target determine the actions that can be carried out during the session.

## Starting a remote control session using a broker

To start a remote control session through the internet with a target, you do not have direct access to, you can initiate a remote control session from the Remote Control server UI and use a broker to make the required connection.

To start a remote control session by using a broker to make the connection, you do not select a target. Instead, select to start a broker session from within the BigFix® Remote Control Server UI. A request for a connection code is made. The code is generated by the remote control server, passed to the broker and is displayed on the controller computer. When the target user enters this connection code, it is passed to the remote control server along with the target data for authentication. When the session is authorized, the applicable policies and session information are passed back to the target and the session proceeds. This procedure describes how to initiate a remote control session from the BigFix® Remote Control Server, by using a broker to make the connection to the target and the steps that are required for the controller and target users.

1. Click **Targets > Start Broker session** in the server UI on the controller computer.

If a successful connection is made to a broker, the Connection code window is displayed. The connection code to be used for the remote control session, field is displayed. A **URL** field might also be displayed. The connection timer begins to count down from 15 minutes, in seconds. Status shows waiting for target.

While the **Connection Code** window is displayed the following options are available.



- Click **Request New** for a new connection code.



**Note:** The time resets to 15 minutes and begin to count down in seconds.

- Click **Extend Timeout** to increase the time that is allowed for the session connection to take place.



**Note:** The time resets to 15 minutes and begin to count down in seconds.

- Click **Cancel** to remove the connection code window. The connection to the broker does not take place.

2. Pass the connection code to the user on the target computer you want to start a remote control session with. For example, this can be done by email or phone.
3. 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.



**Note:** If there are multiple brokers in the brokerlist and the controller computer is not connected to the same broker as the target, the controller connects to the same broker. The following message is displayed on the controller computer before the remote control session begins. `Connecting to:hostname:port` where `hostname:port` is the host name and port of the broker that the target computer is connected to.

If the broker connection cannot be made, the connection code cannot be verified or the target is not authenticated by the server, the target user is given the option to try the connection option again. When they click **Try Again**, the Connection Code window is displayed and they can enter a connection code. If they click **Cancel**, the connection attempt to the broker ends and the remote control session is not established.



**Note:** An Active session is started unless one of the following conditions are met.

- The policies that are set for the session do not have Active enabled. In this case the next enabled session mode is used in the following order of precedence.
  - Guidance mode
  - Monitor mode
  - Chat mode
  - File transfer
- User acceptance is enabled and the target user selects another session type on the acceptance window.

## Connecting to a target that is already in a session

When you attempt to start a peer to peer remote control session with a target that is already in a session there are two features you can use to connect to this target. If a collaboration session has been started with the target you can request to join the session, or use the disconnect feature to end the session and connect to the target instead. The disconnect feature is useful in situations where a controller user is no longer using their machine and has not disconnected from a session. Both of these features are available only during peer to peer remote control sessions when the target properties, **Managed= No** and **CheckUserLogin=Yes**. If collaboration has been started you can use the join function. If the **AllowForceDisconnect** target property is set to **Yes**, you can use the disconnect function.

## Joining or Disconnecting a session

When you attempt to connect to a target in peer to peer mode and the target is already in a remote control session you can join or disconnect the session, depending on the target properties that are set.

When the target properties Managed = No and CheckUserLogin = Yes, and either AllowForceDisconnect = Yes or collaboration has been started you can perform the steps in this task. Join or disconnect the session by completing the following steps:

1. Start a peer to peer session with the target and enter the target IP address and port in the connection window.
2. Logon with your operating system ID and password.  
When you have successfully authenticated, a message window with action buttons is displayed if the target is already in a remote control session.
3. Click the required action button in the message window

**Cancel**

Click **Cancel** to remove the message window and end the session attempt.

### Join

Click to join the current collaboration session. If user acceptance is enabled, your acceptance into the session is determined by the controller and target users. If they accept, you are joined to the session. If they refuse, you are not joined to the session.

### Disconnect session

Click to disconnect the session. When you click **Disconnect session**, a message window is displayed informing you that the current controller has been informed of your request and how long they have to respond before they are automatically disconnected. If you click **Cancel** the current controller receives the message, `The request to disconnect was cancelled. Your attempt to connect to the target ends.`

A message window is also displayed on the current controller's screen with a timer showing the number of seconds they have to react to the request and the option to accept or refuse your disconnection request. They can select from the following options:

#### Accept

If they click Accept, your connection to the target is finally determined by the target user if target user acceptance is enabled. You are connected to the target if the target user accepts the request, or they do not respond in the given time and the **AcceptanceProceed** property is set to PROCEED. You are not connected to the target if the target user refuses the request, or they do not respond in the given time and the **AcceptanceProceed** property is set to ABORT. If target user acceptance is not enabled, the current session is disconnected and you are connected to the target.

#### Refuse

If the current controller user clicks refuse, a message is displayed on your system and the current controller is not disconnected from the session.

#### No response

If the current controller user does not respond within the given time you are connected to the target if the **AcceptanceProceed** property is set to PROCEED. You are not connected if **AcceptanceProceed** is set to ABORT.

## Chapter 4. Using the controller interface as a controller user

The Remote Control controller window is the interface used by the controller user to communicate with the target. You can use the interface to connect to a machine with the target software installed and perform certain functions as if at the local machine.

## Overview of the controller interface

Use the menus and menu items available in the controller interface, during a remote control session to communicate with the target user and perform actions on the target computer.



The menu items are:

### Connection icon



When a remote control session is established, the connection icon is displayed. Click this icon to disconnect from the session.

### Session Drop-down list

Displays the types of sessions that are available during the current remote control session. Depending on the policies that are set for the session, can be any or all of the following types:

- Chat only
- Monitor
- Guidance
- Active
- Reboot
- File Transfer
- Command



**Note:** Only Active and Monitor session modes are available on the BigFix® Remote Control Target for macOS.

For more information about the session types, see [Types of remote control sessions that can be established \(on page 34\)](#).

### Enable or Disable input



To forward local mouse movements and keyboard strokes to the remote computer within an Active session. When local input is disabled, you cannot use the mouse or keyboard to interact with the target. For more information, see [Enabling and Disabling Local Input \(on page 57\)](#).

### Target Num Lock state



Click to set the state of the target **Num Lock** led. When the icon is displayed as **Num**, the target **Num Lock** led is off. When it is displayed as **Num on**, the target **Num Lock** led is on. For more information, see [Setting the state of the target keyboard numlock led \(on page 57\)](#).

### Perform action in target



Contains a dynamic menu. The session mode determines what items are displayed in the menu. For more information about the menu options that can be available, see [Actions that you can perform on the target. \(on page 57\)](#).

### Get System Info



Use this option to gather and display information about the target system. For more information, see [Retrieving Target System Information \(on page 61\)](#).

### Open Chat Window



Use this option to open the **Chat** window and chat to the target user during a remote control session. For more information, see [Chatting to the target user during a remote control session \(on page 61\)](#).

### Collaboration



Use this option to invite multiple participants into a remote control session. For more information, see [Inviting multiple participants into a remote control session. \(on page 62\)](#).

### Controller Tools



Contains a menu of tools you can use for text input or capturing the screen of the target computer. For more information, see [Tools available in the controller tools menu \(on page 77\)](#).

### Record Session



Use this option to make a recording of the remote control session. For more information, see [Recording a remote control session \(on page 80\)](#).

### File transfer menu



Use this option to transfer files between the controller and target and vice versa. For more information, see [Transfer of files during an active session \(on page 83\)](#).

### Clipboard transfer menu



Use this option to transfer the contents of the clipboard to or from the target. For more information, see [Copying clipboard information between the controller and target \(on page 86\)](#).

### Smart card selection menu



To enable smart card support and allow the use of Common Access Card (CAC) or Personal Identity Verification (PIV) smart cards during an Active mode session. Select a local smart card reader to create and attach to a virtual smart card reader on the target. For more information, see [Connecting to a smart card reader during a session \(on page 87\)](#).

The **Smartcard selection** option is available only when the following operating systems are running on the controller and target; Windows 7 or later, or Windows Server 2008 R2 or later. The smart card reader driver must also be installed on the target. For more information about installing the smart card reader driver on the target, see the *BigFix® Remote Control Installation Guide*.

### Network Response Indicator



Provides an indication of the network response time during a session. For more information, see [Network response indication \(on page 88\)](#).

### Select Screens



When a target is configured with multiple displays, you can toggle between each screen or view all screens at the same time. For more information, see [Viewing multiple target screens \(on page 88\)](#).

#### Enable or Disable autoscrolling view



Use this option to scroll the view of the targets desktop without having to use the scroll bars. For more information, see [Scrolling the target screen during a session \(on page 89\)](#).

#### Enable or Disable scaled view



Use this option to resize the view of the remote desktop to fit within the controller window. For more information, see [Viewing the full target screen in a session window \(on page 89\)](#).

#### Performance settings



Use this option to adjust the image quality of the target desktop and improve the session performance, if your network is slow. For more information, see [Change the color quality of the session window to improve session performance \(on page 89\)](#).

#### Configure controller



Use this option to create a local controller configuration. Local configuration properties override global configuration properties. For more information, see [Creating a local configuration for the controller \(on page 91\)](#).

#### Help



Use this option to access the online Remote Control documents or view details of the product version. For more information, see [Obtaining help \(on page 95\)](#).

## Changing the session type during a remote control session

During a remote control session you can change from your current session mode to a different session mode using the Session type list in the controller window.

### Changing to Active Mode during a remote control session

If the current session is not an active session you can change to an active session by selecting **Active** from the session type list on the controller window.

The remote control session continues in active mode and you can control the remote mouse and keyboard.



**Note:** Depending on the policies set for the session, the target user might be asked to accept or refuse the session mode change. If they refuse, the session does not change to active mode.

## Changing to chat only mode during a remote control session

If the current session is not a chat only session you can change to this type of session by selecting **Chat only** from the session type list in the controller window.

The remote control session continues in chat mode. You can no longer view the target screen.



**Note:** Depending on the policies set for the session, the target user might be asked to accept or refuse the session mode change. If they refuse, the session does not change to chat mode.

## Changing to monitor mode during a remote control session

If the current session is not a monitor session you can change to this type of session by selecting **Monitor** from the session type list in the controller window.

The remote control session continues in monitor mode. You can still view the target screen but you have no control over the remote keyboard or mouse.



**Note:**

1. Depending on the policies set for the session, the target user might be asked to accept or refuse the session mode change. If they refuse, the session does not change to monitor mode.
2. The **Disable Input**, **Perform Action in target**, and **Clipboard Transfer** menu on the toolbar become inactive when a monitor session is established.

## Changing to guidance mode during a remote control session

If the current session is not a guidance session you can change to this type of session by selecting **Guidance** from the session type list in the controller window.

The remote control session continues in guidance mode. You can still view the target screen although you have no control over the remote keyboard or mouse. You can provide guidance instructions on screen using drawing and highlighting tools. For more details, see [Tools for providing instructions to a target user \(on page 39\)](#).



**Note:** Depending on the policies set for the session, the target user might be asked to accept or refuse the session mode change. If they refuse, the session does not change to guidance mode.



## Changing to command mode during a remote control session

If the current session is not a command session you can change to this type of session by selecting **Command** from the session type list in the controller window.


The remote control session continues in command mode. You can no longer view the target screen.



**Note:** Depending on the policies set for the session, the target user might be asked to accept or refuse the session mode change. If they refuse, the session does not change to command mode.

## Enabling and Disabling Local Input

Use **Disable input** to disable the mouse and keyboard on the controller machine during the session.

Local Input is available only during an **Active** session. The **Disable input** icon  is available when the use of the local keyboard and mouse is enabled. Click the icon to disable local input. Click the icon again to enable local input.



**Note:** On opening the controller, local input is set dependant on the type of session. During a remote control session, to use your mouse and keyboard to access the target desktop, local input must be enabled. However if the target user moves the mouse when local input is enabled, you are temporarily blocked from sending any input events to the target until the target user stops moving the mouse. The icon changes to a blocked mouse image. When switching from an Active session to another session local input is disabled.

## Setting the state of the target keyboard numlock led

You can use the **Target numlock state** icon in the controller window to see and set the state of the target keyboard numlock led. You can toggle the state of the target numlock led by clicking on the icon. Both the controller and target keyboard leds should be set to the same state if there is a requirement to use the numeric keypad during the remote control session. When the icon is displayed as **Num** the target numlock led is off. When it is displayed as **Num on** the target numlock led is on.

## Actions that you can perform on the target.

Use the **Perform action in target** menu to perform various actions on the target system during an active or guidance remote control session. The following actions are available depending on the type of remote control session that is running. The full list is available during an active session and a limited number of actions are available during a guidance session. Depending on controller properties that are set, you might also see menu items for running tools or injecting key sequences on the target. For more information about controller properties, see [Configuring global controller properties \(on page 107\)](#). For information about the keyboard shortcuts that are available for the BigFix® Remote Control Target for macOS, see [Keyboard shortcuts for the BigFix Remote Control Target for macOS \(on page 129\)](#).

**Inject Ctrl + Alt + Del**

Injects Control, Alt, and Delete keys. The resulting action is system dependant.



**Note:** When you inject Ctrl +Alt +Del and you are using Windows™ 7 operating system or higher, complete the following steps:

The two scenarios that ensure that the logon window pops up are as follows.

- UAC on and Secure Attention Sequence set to Services
  - UAC off and Secure Attention Sequence set to Services
1. To start Microsoft™ Management Console, click **Start > Run > mmc.exe** .
  2. To add Group Policy Object Editor Snap-in, select **File > Add/Remove Snap-in.. > Group Policy Object Editor > Add > Finish > OK**.
  3. Expand **Local Computer Policy**.
  4. Expand **Computer Configuration**.
  5. Expand **Administrative Templates**.
  6. Expand **Windows Components**.
  7. Select **Windows Logon Options**.
  8. Double-click **Disable or enable software Secure Attention Sequence**.
  9. Select **Enabled**.
  10. Select **Services**.
  11. If **Ease of Access applications** was already selected, choose **Services and Ease of Access applications**.
  12. Select **OK**.



**Note:** The **Inject Ctrl+Alt+Del** menu is disabled during a session with an on-demand target when you are using Windows™ XP or Windows™ Server 2003 operating systems.

**Inject Alt + F4**

To close the active window on the target computer.

**Inject Alt + Tab**

To switch between active windows on the target computer.

**Inject Alt + Enter**

To run a command-line window on the target in full screen mode. Select **Inject Alt + Enter** again to change the command-line window to normal mode.

**Inject Control + Esc**

To open and close the **Start** menu on the target computer.

### Drawing Tool

To draw basic colored lines on the target's screen. For example, to point to a particular area on the target screen by drawing a circle around the area. For more information about the drawing tool, see [Using the guidance tool \(on page 40\)](#).

### Highlight tool

To select and highlight a specific area on the target's screen. For more information about highlighting, see [Using the highlight tool \(on page 42\)](#).

### Mouse Tool

Use this tool to display your mouse cursor in the target system so that the target user can see your mouse as it moves around their desktop. For more information, see [Displaying the controller mouse cursor on the target system \(on page 42\)](#).

### Clear Instructions

To remove all guidance drawings or highlighted areas from the target screen.

### Lock Workstation

To lock the target workstation.

### Open URL

To type in a URL that is opened in the target computer's default web browser. Type in the URL and click **OK**. The target default browser opens at the specified URL.

### Enable Privacy

To hide the target screen from the target user. The target screen is blacked out with a message that the system is being serviced by Remote Control, is displayed. However, you can work with the target system on your screen. The local input and display are locked for the target user and they are not able to do anything on the target while privacy is enabled. Enable privacy is useful when you are working on systems with sensitive information.

### Lock target input

To lock the target user's mouse and keyboard during a remote control session. This menu item is available only when the **Allow input lock** policy is enabled for the session. The target screen is still visible to the target user.



**Note:** If the option to Enable Privacy is selected, the remote user input is automatically locked. It is not possible to enable privacy without also locking the input.

### Registry Keys

Available only if the **Allow registry key lookup** or **View registry key list** policies are enabled for the session. When you click **Registry Keys**, a list of registry keys might be displayed and an **Enter key** item,

depending on the policies that are set for the session. For more information about editing policies, see the *BigFix® Remote Control Administrator's Guide*.

**A list of defined registry keys is displayed.**

Click one of the listed keys to see the current value for it, on the target. The keys are defined in the `trc.properties` file and the names that are listed correspond to a specific registry key on the target. For more information about editing the properties files, see the *BigFix® Remote Control Administrator's Guide*.

For example,

when you click **Registry keys** you might see **Services** listed.

If you click **Services**, a new window opens that displays all of the services on the target.

**To enter a specific registry key.**

Use the Enter key item to enter a specific registry key you want to know the value for by completing the following steps:

- Type in a key value in the **Registry key** field. For example,

```
HKLM\SYSTEM\CurrentControlSet\Services\TRCTarget
```



**Note:** Make sure that you enter the exact path to the registry key.

- Click **View**.

A new window opens and displays the current values for the specified key, as defined on the target.

## Keep Session Log

The **Keep Session Log** option is available during an on-demand session. Determines whether you can save the session log to the target computer, when the session ends. Select **Keep Session Log** to save the log to the target computer in the user's working directory, at the end of the session. The log is saved in the following format:

`trc_odt_trace_yyyymmdd_hhmmss.log`.

For example, `trc_odt_trace_20130531_130300.log`.

If you do not select **Keep Session Log**, the log file is deleted at the end of the session. However, if the session is interrupted by a non-user event, for example, a network failure, the log file is also saved.



**Note:** The **Perform action in target** menu is a dynamic menu that changes depending on which operating system is being used and the session connection mode. The menu might also be disabled depending on the operating system and policies in the session.

## Retrieving Target System Information

Use **Get System Info** to retrieve and see information about the target, for example, the amount of memory or type of network connection.

Click **Get System Info**  in the taskbar.

A text file, `sysinfo.txt` is created on the target machine and is displayed on the controller.

On the controller system the file is saved within:

`$HOME` on a UNIX® system.

`%USERPROFILE%\TRC_FT` on a Windows® system.



**Note:** Depending on the policies set for the session, the target user might be asked to accept or refuse the system information request. If they refuse, the system information is not displayed.

## Chatting to the target user during a remote control session

Select the Open chat window option to chat to the target user during an active, guidance and monitor remote control session. The availability of this option depends on the policies set for the session having the chat function enabled.

To start a chat with the target user during a remote control session, complete the following steps :

1. Click **Open Chat Window**:



2. The Remote Control Chat Window opens on the controller system and the chat area is opened in the target window.
3. Type your text and click **Send** or press **Enter**.
4. Click **Clear** to remove any text which has been typed in the Chat Window.
5. To close the chat window click the **X** in the upper left of the window.



**Note:** Click **Clear** to remove the text from the chat window on the controller screen. The text remains in the chat window on the target screen.

## Inviting multiple participants into a remote control session.

During a remote control session use the collaboration function to invite other participants to join the session. This function is useful if you are connected to a target where the target user requires assistance and you need additional help to solve the problem. All controller users who join the session can see the target screen. The controller who initiates the collaboration session with the target is known as the master controller and it is this user who controls the activity in the session. For example, who is allowed to join, how many people are allowed to participate or who should have control of the session. All other controllers in the session are known as participants. When a new controller joins the session they can see the target screen in the session window but they do not have any control of the session and should request control when they need to work with the target. If user acceptance for collaboration is enabled, the target user will have the final decision on whether the new controllers can join the session. The value of the **Enable user acceptance for collaboration requests** server policy or the **ConfirmCollaboration** target property determines whether the target user should accept or refuse the request to join the session, depending on the type of collaboration session.

### Yes

the target user is asked to accept or refuse the request to join the session. If they accept the request, the new controller is connected to the session. If they refuse, or do not respond in a given time, a refusal message is displayed and the new controller is not joined to the session.



**Note:** If the target user does not respond in the given time and the **Acceptance timeout action** server policy or **AcceptanceProceed** target property is set to PROCEED, you are connected to the session.

### No

user acceptance is not required by the target user and the new controller is automatically connected to the session.

## Collaboration sessions using the server UI

To start a collaboration session when you are logged on to the server UI, start a session with the required target and start collaboration to allow other participants to join the session. The availability of this function is determined by the value set for the **Allow multiple controllers** server policy. The value that is set for the session is derived from the permissions links that are set up between the user groups and target groups that the controller user and target belong to. For more information on how policies and permissions are derived for a session, see the BigFix® Remote Control Administrator's Guide.

### Set to Yes

The **Open the collaboration panel for multiple controllers** icon is available in the controller session window. Use this to start collaboration sessions. This is the default value.

### Set to No

The **Open the collaboration panel for multiple controllers** icon is not available in the controller session window and therefore you cannot start collaboration sessions.

## Starting collaboration in a session started from the server

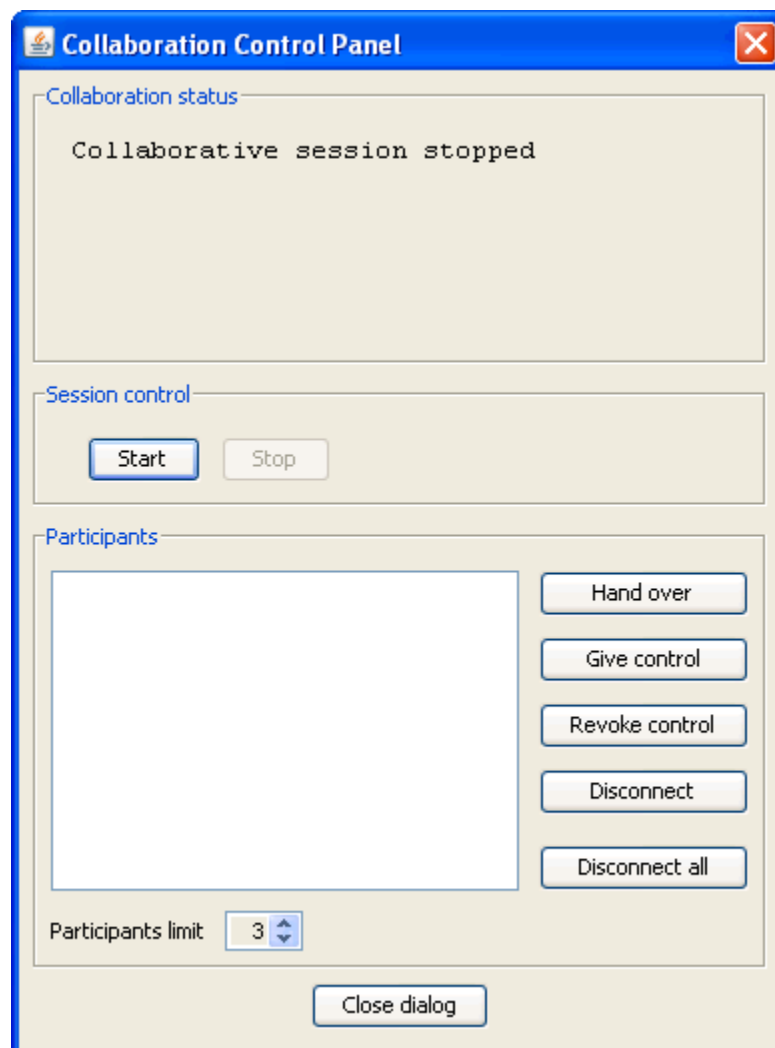
To start a collaboration session from the Remote Control server UI, and allow others to join the session, start a session with the required target and become the master controller by completing the following steps:

1. Generate a target report that contains the required target.  
For example All targets.
2. Select the required target.
3. Select **Start session**.
4. When the session starts, click **Open the collaboration panel for multiple controllers**.



The Collaboration Control Panel opens.

Figure 2. Collaboration Control Panel



5. Click **Start**.

You are now the master controller for the session and other participants can request to join the session. When other participants join the session, use the functions within the Collaboration Control Panel to control the activity within the session. For more details, see [Controlling session activity as the master controller \(on page 74\)](#). You can also accept or reject requests for control of the session from the other participants.

Click **Handover** to pass full control of the session over to another controller user. For more details of this feature, see [Handing over a collaboration session, started from the server \(on page 65\)](#).

## Joining a collaboration session from the Remote Control server

When a target is already in a remote control session you can attempt to join this session if collaboration has been started. When you select to join a collaboration session, if user acceptance is enabled, your acceptance into the



session, is determined firstly by the master controller and then by the target user. The value of the server policy **Enable user acceptance for collaboration requests** determines whether target user acceptance is required.

To join a collaboration session complete the following steps :

1. Generate a target report that contains the required target. For example `All targets`.
2. Select the required target.
3. Select **Start session**.

A message is displayed indicating that the target is already in a session but is accepting multiple participants.

4. Click **Join**.

As the remote control session starts, a message is sent to the master controller letting them know that you have requested to join the session. They can respond to the request by selecting Yes or No.

#### Yes

If the master controller clicks Yes, your final acceptance into the collaboration session is determined by the target user and whether user acceptance for collaboration is enabled. For more details see [Inviting multiple participants into a remote control session. \(on page 62\)](#).

#### No

If the master controller clicks No, you are not allowed to join the session and a refusal message is displayed. Click **OK**.

After you have joined the collaboration session the master controller can see you listed in the participants list in the Collaboration Control Panel. You have no mouse or keyboard control in the session but you can use the chat feature, if it has been enabled for the session. Use the collaboration icon to request control of the session. For more details of collaboration actions that can be used, see [Controlling session activity as a participant \(on page 75\)](#)

## Handing over a collaboration session, started from the server

If you are the master controller of a collaboration session, you can pass full control of the session to another participant by using the handover function.

During a collaboration session, use the **Handover** function to pass full control of the session to one of the other participants in the session. They become the master controller and you can leave the session without having to end it. The availability of this function is determined by the value of the server policy **Allow session handover**.

#### Set to Yes

The **Hand over** button is displayed in the collaboration control panel.

#### Set to No

The **Hand over** button is not displayed in the collaboration control panel.

To pass control of a collaboration session to a new master controller, complete the following steps:

1. Select the required controller in the participants list, in the collaboration control panel.
2. Click **Hand over**.

The outcome of the handover request is determined by the value that is set for the **Enable user acceptance for collaboration requests** server policy.

If this policy is set to Yes for the session, the target user is asked to accept or refuse your request to hand over control. If they accept the request, full session control is passed to the selected controller. If they refuse, or do not respond in time, a refusal message is displayed on your screen and on the selected controllers screen. You are still the master controller of the session. Click **OK**



**Note:** If the target user does not respond in time and the **Acceptance timeout action** server policy is set to PROCEED, control is passed to the new master controller.

If **Enable user acceptance for collaboration requests** is set to No, user acceptance is not required by the target user and full session control is passed to the new master controller.

When the session is handed over to the new master controller, the collaboration control panel opens on their system. The list of participants is displayed in the collaboration control panel. You lose input control for the session. The IP address of the new master controller is displayed in the window title of your session window.

The new master controller sees the IP address of the target in the window title of their session window.



**Note:** The policies for the session remain as they were when the session was started. The policies do not change even although the controller user changed. The initial policies that are set for the session are valid throughout the collaboration session regardless of who is the master controller.

## Peer to Peer collaboration sessions

During a peer to peer remote control session, the value of the target property **AllowCollaboration**, determines the availability of the collaboration feature.

### Set to Yes

The **Open the collaboration panel for multiple controllers** icon is available in the controller session window. Use this to start collaboration sessions. This is the default value.

### Set to No

The **Open the collaboration panel for multiple controllers** icon is not available in the controller session window and therefore you are not able to start collaboration sessions.

## Starting a peer to peer collaboration session

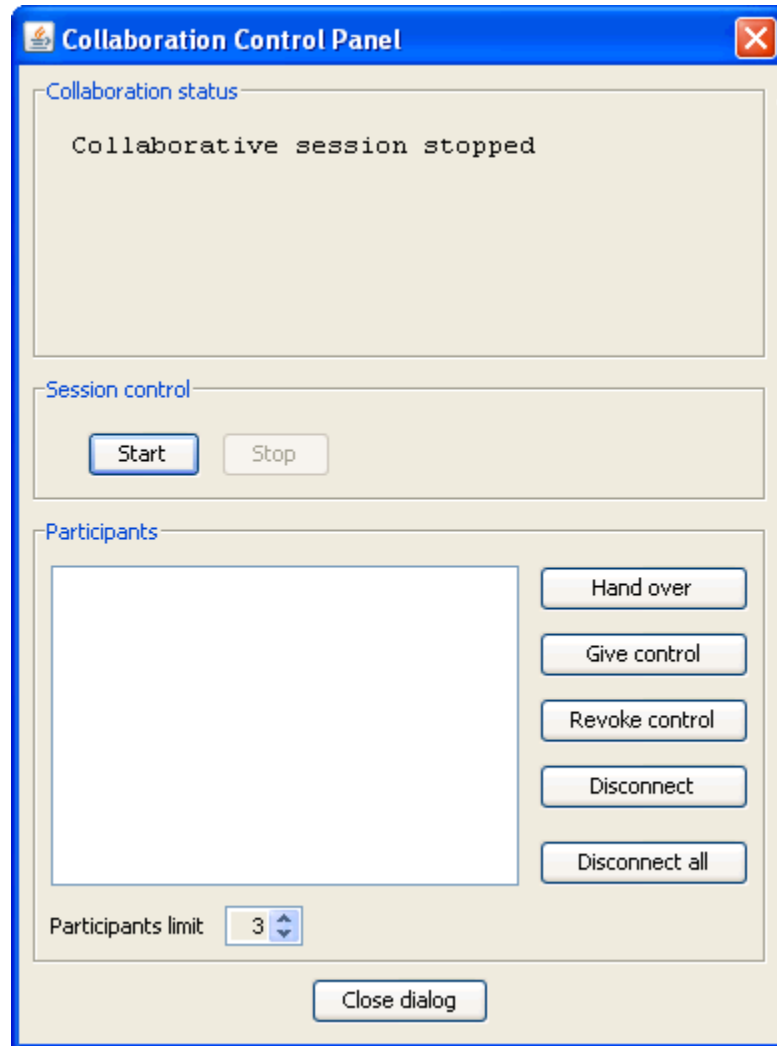
To start a collaboration session and allow others to join the session, start a peer to peer session with the required target and become the master controller by completing the following steps:

1. Start a peer to peer session with a target.  
For details on how to start a peer to peer session, see [Starting a peer to peer session \(on page 46\)](#).
2. Click **Open the collaboration panel for multiple controllers** in the controller window toolbar when the session starts.



The Collaboration Control Panel opens and you are now the master controller for the session.

Figure 3. Collaboration Control Panel



3. Click **Start**.

You can allow other participants to join this remote control session. When other participants join the session, use the functions within the Collaboration Control Panel to control the activity within the session. For more details, see [Controlling session activity as the master controller \(on page 74\)](#).

Click **Handover** to pass full control of the session over to another controller user. For more details of this feature, see [Handing over a peer to peer collaboration session \(on page 69\)](#).



**Note:** When each new controller requests to join the session you are asked to accept the request. You can configure the controller so that you are not asked to accept these requests. For more details see, [Hiding the master controller acceptance window \(on page 115\)](#).

## Joining a peer to peer collaboration session by connecting to the master controller

When a remote control session is started by connecting directly to the target in peer to peer mode you can attempt to join this session if collaboration has been started. Your acceptance into this session is determined by the master controller and the target user, depending on policy values that have been set. You can join a peer to peer remote control session by connecting to the master controller of the session.

To join a peer to peer collaboration session by connecting to the master controller, you must obtain the IP address and listening port for the master controller. These values are displayed in the collaboration control panel on the master controller's machine when they start collaboration.

When joining a collaboration session, your acceptance into the session is determined firstly by the master controller and then by the target user. The value set for the target property **ConfirmCollaboration** determines whether target user acceptance is required.

To join a collaboration session start a peer to peer session and enter the IP address and port for the master controller machine.



**Note:** In a collaboration session only the master controller connects to the target, while the other controllers connect to the master controller. The port to be used to connect to the master controller is reported in the Collaboration Control Panel after clicking the Start button.

For details of how to start a peer to peer session. see [Starting a peer to peer session \(on page 46\)](#)

As the remote control session starts, a message is sent to the master controller letting them know that you have requested to join the session. They can respond to the request by selecting Yes or No.

### Yes

If the master controller clicks Yes, your final acceptance into the collaboration session is determined by the target user and whether user acceptance for collaboration is enabled. For more details see [Inviting multiple participants into a remote control session. \(on page 62\)](#).

### No

If the master controller clicks No, you are not allowed to join the session and a refusal message is displayed. Click **OK**.

When you join a peer to peer collaboration session you can see the IP address of the master controller displayed in the title of the session window. The master controller can see you listed in the participants list in the Collaboration Control Panel. Use the collaboration icon to request control of the session. For more details of collaboration actions that can be used, see [Controlling session activity as a participant \(on page 75\)](#)

## Joining a peer to peer session by connecting to the target

When a target is already in a peer to peer remote control session you can attempt to join this session if collaboration has been started and the target properties **Managed = No** and **CheckUserLogin=Yes**. Your acceptance into this session is determined by the master controller and the target user, depending on the user acceptance property values that have been set.

To join a peer to peer collaboration session by connecting to the target, complete the following steps :

1. Start a peer to peer session and enter the IP address and port for the target machine.  
For details of how to start a peer to peer session. see [Starting a peer to peer session \(on page 46\)](#)
2. Click **Join**.

As the remote control session starts, a message is sent to the master controller letting them know that you have requested to join the session. They can respond to the request by selecting Yes or No.

### Yes

If the master controller clicks Yes, your final acceptance into the collaboration session is determined by the target user and whether user acceptance for collaboration is enabled. For more details see [Inviting multiple participants into a remote control session. \(on page 62\)](#).

### No

If the master controller clicks No, you are not allowed to join the session and a refusal message is displayed. Click **OK**.

When you join a peer to peer collaboration session you can see the IP address of the master controller displayed in the title of the session window. The master controller can see you listed in the participants list in the Collaboration Control Panel.

## Handing over a peer to peer collaboration session

During a peer to peer collaboration session use the **Handover** function to pass full control of the session to one of the other participants in the session. They become the master controller and you can leave the session without having to end it. The availability of this function during a peer to peer collaboration session is determined by the **AllowHandover** target property.

### Set to Yes

The **Hand over** button appears in the collaboration control panel.

### Set to No

The **Hand over** button does not appear in the collaboration control panel.

To pass control of a collaboration session to a new master controller complete the following steps :

1. Select the required controller in the participants list in the collaboration control panel.
2. Click **Hand over**.

The outcome of the handover request is determined by the value set for the **ConfirmCollaboration** target property.

If this property is set to Yes for the session, the target user is asked to accept or refuse your request to handover control. If they accept the request, full session control is passed to the selected controller. If they refuse, or do not respond in a given time, a refusal message is displayed on your screen and on the selected controllers screen, and you are still the master controller of the session. Click **OK**



**Note:** If the target user does not respond in the given time and the **AcceptProceed** target property is set to PROCEED, control will be passed to the new master controller.

If **ConfirmCollaboration** is set to No, user acceptance is not required by the target user and full session control is passed to the new master controller.

When the session is handed over to the new master controller, the collaboration control panel opens on their system. The list of participants is displayed in the collaboration control panel. You lose input control for the session. The IP address of the new master controller is displayed in the window title of your session window.

The new master controller sees the IP address of the target in the window title of their session window.

## Collaboration during sessions connected through a broker

During remote control sessions that are started by using a broker to make the connection, use the collaboration function to allow other participants to join the session.

The server policy **Allow multiple controllers** is used to determine the availability of the collaboration feature during a broker remote control session. The value that is set for the session is derived from the permissions links that are defined for the user groups and target groups that the controller user and target belong to. For more information on how policies and permissions are derived for a session, see the BigFix® Remote Control Administrator's Guide.

### Set to Yes

The **Open the collaboration panel for multiple controllers** icon is available in the controller session window. Use the icon to start collaboration sessions. Yes is the default value.

### Set to No

The **Open the collaboration panel for multiple controllers** icon is not available in the controller session window and therefore you cannot start collaboration sessions.

You can use the **Handover** function to pass full control of a collaboration session to a new master controller.

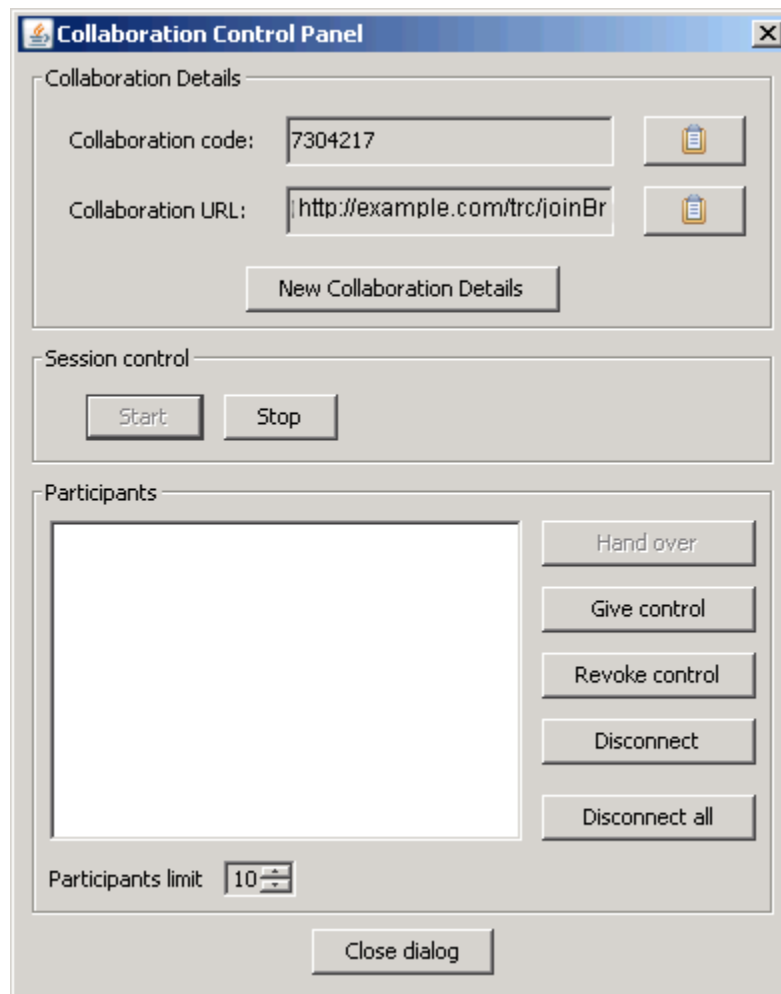
## Starting collaboration during a broker remote control session

To start a collaboration session and allow others to join the session, start a broker session with the required target and become the master controller by completing the following steps:

1. Start a broker remote control session.  
For the steps required to do this, see [Starting a remote control session using a broker \(on page 48\)](#).
2. When the session starts, click **Open the collaboration panel for multiple controllers**.

The Collaboration Control Panel opens.

Figure 4. Collaboration Control Panel for a collaboration session that connects through a broker



3. Click **Start**.

A collaboration code and URL are displayed in the **Collaboration Details** section of the **Collaboration Control Panel**. Pass these values to any new controllers who need to join the collaboration session.



**Note:** You can use the clipboard icon to copy the connection code and URL to the clipboard.

Click **New Collaboration Details** to obtain a new connection code and URL if required.

You are now the master controller for the session and other participants can request to join the session. For details of requirements for allowing others to join, see [Joining a broker collaboration session \(on page 72\)](#). When other participants join the session, use the functions within the Collaboration Control Panel to control the activity within the session. For more details, see [Controlling session activity as the master controller \(on page 74\)](#).

## Joining a broker collaboration session

For a remote control session that has been started using a broker to make the connection, if collaboration has been started, you can join this session by obtaining a connection code or URL from the master controller.



**Note:** If you select to start a remote control session with a target, using the start session option in the server UI, if the target is already in a session, connected using a broker, and collaboration has been started, you will be given the option to join the session. For more details of joining a collaboration in this way, see [Joining a collaboration session from the Remote Control server \(on page 64\)](#)

## Joining a collaboration session by using a connection code

During a broker remote control session, if collaboration is started, you can join this session from the Remote Control server UI by using a connection code.

To join the session, you must obtain a connection code from the master controller of the collaboration session.

If user acceptance is enabled when you select to join a broker collaboration session, the master controller and then the target user, determine whether you can join the session. The value of the server policy **Enable user acceptance for collaboration requests** determines whether target user acceptance is required.

To join a broker collaboration session, complete the following steps:

1. Click **Targets > Join broker session**.
2. Enter the connection code and click **Submit**.

The controller component starts.



**Note:** If the code is not valid, a message is displayed. Obtain and enter a valid code.

You can click **Cancel** on the **Join a session** window to return to the previously displayed window.

As the remote control session starts, a message is sent to the master controller letting them know that you have requested to join the session. They can respond to the request by selecting Yes or No.

**Yes**



If the master controller clicks Yes, your final acceptance into the collaboration session is determined by the target user and whether user acceptance for collaboration is enabled. For more details see [Inviting multiple participants into a remote control session. \(on page 62\)](#).

#### No

If the master controller clicks No, you are not allowed to join the session and a refusal message is displayed. Click **OK**.

## Joining a broker collaboration session by using the connection URL

During a broker remote control session, if collaboration is started, you can join this session by using a connection URL that is obtained from the master controller of the session.

To join the session, obtain the URL from the master controller of the collaboration session.

If user acceptance is enabled when you select to join a broker collaboration session, the master controller and then the target user, determine whether you can join the session. The value of the server policy **Enable user acceptance for collaboration requests** determines whether target user acceptance is required.

To join the session, type the connection URL into your browser address field and press enter.

If you are not already logged on to the Remote Control server UI, the logon window is displayed. Log on with a valid ID and password. The controller component starts.

As the remote control session starts, a message is sent to the master controller letting them know that you have requested to join the session. They can respond to the request by selecting Yes or No.

#### Yes

If the master controller clicks Yes, your final acceptance into the collaboration session is determined by the target user and whether user acceptance for collaboration is enabled. For more details see [Inviting multiple participants into a remote control session. \(on page 62\)](#).

#### No

If the master controller clicks No, you are not allowed to join the session and a refusal message is displayed. Click **OK**.

## Handing over a collaboration session that involves a broker

During a collaboration session that involves a broker, you can pass full control of a session to another participant.

During a collaboration session, use the **Handover** function to pass full control of the session to one of the other participants in the session. They become the master controller and you can leave the session without having to end it. The availability of this function is determined by the value of the server policy **Allow session handover**.

For information about the policy and the steps for using the **Handover** function in a session that involves a broker, see [Handing over a collaboration session, started from the server \(on page 65\)](#)

## Controlling collaboration session activity

When a collaboration session has been started and there are multiple participants, various actions can be carried out. The master controller can pass control of the session temporarily or fully over to another participants and can disconnect participants. Other participants can request control of the session.

### Controlling session activity as the master controller

After you have started a collaboration session and have become the master controller you can control the session activity using the following options on the Collaboration control panel :

#### HandOver

Use this option to pass full control of the session over to a new master controller.

1. Select a participant from the participants list.
2. Click **HandOver**.

The collaboration control panel opens on the new master controller's system, listing the participants and you lose input control for the session. The IP address of the new master controller is displayed in the window title of your session window. The availability of this option is determined by the value of server policies or target properties depending on which type of collaboration session has been started.



**Note:** This option is not available in collaboration sessions that are started using a broker to make the connection.

#### Give control

Use this option to select a participant and pass control of the session over to them. You are still the master controller of the session.

1. Select a participant from the participants list.
2. Click **Give control**.

The selected participant now has control of the session and the target and can use the tools and actions that are available in the controller window. They can also change the session type by selecting one from the session pull down.



**Note:** You no longer have control of the session and some of the actions in your controller window are now inactive.

#### Revoke control

Use this option to retake control of the session at any time by completing the following steps :

1. Select the participant from the list.
2. Click **Revoke control**.

You now have control of the session. The actions in your controller window are now active. The selected participant no longer has control.

### Disconnect

Use this option to disconnect one or more participants from the session at any time by completing the following steps :

1. Select the required one or more participants.
2. Click **Disconnect**.

The selected participants receive a message that the session has been cancelled. When they click **OK** their session ends.

### Disconnect all

Use this option to disconnect all participants from the session at any time. All participants receive a message that the session has been cancelled.

### Participants limit

Use this option to set the maximum number of participants that are allowed to join the session. The number is in the range of 1 to 10 and set to 3 as default whenever a collaboration session is established. You can change this value at any time during a session. When a controller tries to join a session, if the limit has already been reached they receive the following message when they click Join.

`Session rejected because the limit has been reached.`



**Note:** For a collaboration session started using a broker to make the connection, the maximum number of allowed participants is 20 and the default value is 10.

## Controlling session activity as a participant

As a participant in a collaboration session you can ask for control of the session and also return control back to the master controller. To request and return control of the session, complete the following steps:

1. In the controller window click **Open the collaboration panel for multiple controllers**.  
The Collaboration control panel opens.
2. Click the required option.

### Request control

Use this option to request control of the collaboration session. The master controller receives the following message with the option to accept or reject the request. Do you want to accept the

`request from user XXXXX at aaa.aaa.aaa to get control`

where XXXXX is the user id of the participant who is requesting control and aaa.aaa.aaa is the IP address of the participants machine.

If the master controller clicks Yes you now have control of the session.

If the master controller clicks No, you receive the following message and do not have control of the session. Request for session control has been denied. Click **OK** to continue.

### Return control

Use this option to return control of the session back to the master controller. You no longer have control of the session.



**Note:** If the collaboration control panel is not open, click the **Open the collaboration panel for multiple controllers** icon in the controller window toolbar.


## Ending a collaboration session

Click **Stop**, in the collaboration control panel, to end a collaboration session at any time. All participants in the session are automatically disconnected and receive a message that the session has been cancelled.

## Ending a collaboration session when you disconnect

When you end a session in which collaboration is started, you can choose to stay in the session or disconnect from the session.

You can end a remote control session in the following ways:

- Click the **Connection** icon in the taskbar. 
- Click the **X** in the upper right of the controller window.

If collaboration is started in the session and you are the master controller of the session, you are warned that collaboration is in progress. The following message is displayed. A Collaboration session is in progress. If you disconnect, the session will end. Keep the session open?

You can choose to disconnect and end the session or choose to remain in the session as the master controller.

### Cancel

When you click **Cancel**, the collaboration session continues and you are still the master controller.

### Disconnect session

When you click **Disconnect session**, the collaboration session ends and all participants are disconnected.

## Collaboration and handover audit events

The following audit events are reported for collaboration and handover sessions.

### From the controller

**Table 4. Events from the controller**

Event ID	Event Description
Audit.handover.request	Requested session handover to participant {0}
Audit.handover.request.granted	Session handover accepted
Audit.handover.request.rejected	Session handover rejected
Audit.handover.success	Handover was successful. Participant {0} is the new session owner
Audit.handover.reconnect	Participant {0} reconnected to the Remote Control session

### From the target

**Table 5. Events from the target**

Event ID	Event Description
ibm.trc.audit.0050	Collaboration request rejected. GUI is not running and proceed==FALSE.
ibm.trc.audit.0051	Collaboration request accepted. GUI is not running and proceed==TRUE.
ibm.trc.audit.0052	Collaboration request rejected by the user {0}
ibm.trc.audit.0053	Collaboration request accepted by the user {0}
ibm.trc.audit.0054	Collaboration Session Handover request rejected by settings
ibm.trc.audit.0055	Collaboration Session Handover request approved by settings
ibm.trc.audit.0056	Collaboration Session Handover request rejected by user {0}
ibm.trc.audit.0057	Collaboration Session Handover request approved by user {0}
ibm.trc.audit.0058	Collaboration Session Handover requested by remote user {0}
ibm.trc.audit.0059	Collaboration Session Handover completed. User {0} is now in control

## Tools available in the controller tools menu

The controller tools menu provides some functions that can be used during a remote control session . To access the

functions click **Controller tools**



The following options are available:

- **Quick text input box.**
- **Capture screen**
- **Show session information**

## Capturing the screen during a remote control session

Use the **Capture screen** function to take a snapshot image of the target screen as it appears in the session. The captured image is saved onto your system and can be useful when problem solving. For example, to attach to an email to send to another support agent.

To capture the target screen complete the following steps :-

1. Click **Controller tools**
2. Select **Capture screen**. The **Capture Screen to file** window opens.
3. Navigate to the location you want to save the image to by using **Save In**.
4. Type in a name for the file or accept the name that is given.
5. Click **Save**.



**Note:** If you click **Cancel** the captured screen image is not saved.

## Enabling quick input of text to the target screen

When you need to enter text onto the target screen, for example, to type in a path name or command, or to add some text to a file, use the **Quick text input box** to type in the full text required. Press Enter to send the text to the target system. This option is available only when local input is enabled. When you select **Quick text input box**, a text input box opens each time you press a key. You can use this function to compensate for differences in controller and target keyboard layouts. For example, the controller may have an English keyboard and the target may have a French keyboard. To use the **Quick text input box** function complete the following steps :

1. Click **Controller tools**.
2. Select **Quick text input box**.
3. Choose **Show Text** for content to be shown in clear mode or choose **Hide Text** for content to be shown in hidden mode.
4. In the session window, click where you want to enter the text and press the key of the first character that you want to enter.

The quick text input box appears. There are three ways that you can continue to input the required text

### Type text and enter

to type the required text and press **Enter**. The text is input into the target screen.

### Type text and assign it to favorites list

to keep a list of commonly used text strings as favorites. Each of these is stored in a slot assigned a number from 0 to 9. To assign a text string to the favorites list complete the following steps:

- Type the required text and press **CTRL+SHIFT+n**. Where *n* is a number from 0 to 9. For example CTRL+SHIFT+2.
- Press **ENTER**.

The text is assigned to the slot defined by the number entered.



**Note:** The favorites list is only maintained for the duration of the session.

### Retrieve previously entered text

to retrieve previously typed strings. The input box keeps a history of the recently typed text. You can do this in two ways.

#### Cycle through the text strings

to cycle through any previously typed text strings by clicking the UP or DOWN arrow keys.

#### Retrieve a string from the favorites

to retrieve a string from the favorites list by clicking **CTRL+n**, where *n* is the number of the slot that the string was assigned to when it was assigned to favorites. For example, clicking CTRL+2 will retrieve the string that was saved to slot 2. Press **ENTER** to send the text to the target.



**Note:**

1. Quick text input injects Unicode strings and is also intended to help when typing text when the connection is slow.
2. The text input box is invisible to the target.

## Viewing session information

Use the **Show session information** function to view the specific IP address of the target that you are connected to and the Encryption type being used during the session.

To view the session information complete the following steps :

1. Click **Controller tools**.
2. Select **Show session information**.

The Session information window opens displaying the IP address of the target and the encryption type being used during the session. Click **Close**.

## Recording a remote control session

You can use the recording function to record session activity during a remote control session. This can be useful for auditing and education purposes.

Two types of recording can be made.

### Automatic recording

is determined by the value of the **Force session recording** server policy which is set by an administrator.

If **Force session recording** is enabled for the current session, all session activity is recorded while the session is in progress and then saved to the server when the session ends. The session recording can be played back from the **Session details** screen. For details of playing back a session recording, see [Viewing session details \(on page 22\)](#). Server policies are used to determine whether the session is recorded by the controller or the target, and also the location that the recording is saved to. For more details of server policies, see the BigFix® Remote Control Administrator's Guide.

### Local recording

is determined by the value of the **Allow local recording** server policy which is set by an administrator.

If this policy is enabled for the current session, you can record and save the session activity to your system. For more details of server policies, see the BigFix® Remote Control Administrator's Guide

## Exporting and downloading a recording from the server

After a recording of a remote control session is saved to the server, use the **Export session recording** function to export and save the recording to your system.

This function can be useful in a number of ways

- If a local recording was not made during the session.
- If you want to use the recordings for education or training purposes.

To export one or more recordings complete the following steps:

1. Click **Sessions > My Session History**.



**Note:** If you are an administrator, you can also click **Sessions > All Session History**

2. Select one or more sessions.
3. Choose the appropriate method for selecting **Export session recording**.
  - Click **Export session recording** from the action list on the left
  - OR click **Sessions > Export session recording**

A list of saved recordings is displayed.



**Note:** If the recording export function is enabled on the server, the following message is displayed.





The recording export functionality is disabled. Please consult the documentation for details on how to enable it.

. For more information about enabling the export functions, see the *BigFix® Remote Control Administrator's Guide*

#### 4. Select the relevant file compression

##### Lossless

To compress the file without losing any detail. This option produces a larger file size. Choose this file type if you require a better image quality or if the recording might be used for editing to provide educational material. To play back this type of recording you must install a QuickTime codec.

##### Compressed

To compress the file and lose minor details. This option produces a smaller file size. Choose this file type if the recording is only for viewing. To play back this type of recording you must install an Xvid codec. The codec can be found on the [Xvid.org](http://Xvid.org):Home of the XVid Codec website.

Depending on which compression method you select, the **filename** field is populated with a file name and extension.

##### filename

Is in the format *SSS-nnnnnnnn*.

##### SSS

The session id.

##### nnnnnnnn

The computer name of the target.

For example, 152-mytarg

##### file extension

Is *.mov* or *.avi*.

##### .mov

Is applied when Lossless is chosen for the file compression.

##### .avi

Is applied when Compressed is chosen for the file compression.

#### 5. Click **Export recording**.

When the recording is exported, the status changes to Exported and a **Download** option is available.

#### 6. Click **Download**.

#### 7. Click **Save**.

- On the **Save As** window, browse to the relevant location for saving the recording file to. You can change or keep the name that is given and click **Save**.



**Note:** If you click **Cancel**, the file is not downloaded.

The recording is exported and downloaded from the BigFix® Remote Control Server and saved to your local system. To ensure that it can be played back correctly you must install the correct codec as indicated in step [4 \(on page 81\)](#).



**Note:** For Linux systems, you® must download and install MPlayer with support for the Xvid codec.

## Making a local recording

To record the session activity and save it to your local system complete the following steps :

- In the session window click **Record session** .  
The **Save session to file** window opens.
- Click **Save** to save the recording to the default location, or browse to the required directory and click **Save**.



**Note:** You can accept the file name and extension given for the recording file or you can change the name and extension to your own requirements.

The **Record session** icon changes to a square icon indicating that the recording is in progress. To stop the recording press the square icon .



**Note:** Local recording cannot be saved to the server.

## Playing a local recording

Use the Session Player to play a local recording of a remote control session in Remote Control.

To play back a local recording complete the following steps:

- Download the Session Player.  
For more information about downloading the player, see [Download session player \(on page 28\)](#).
- Start the Session player by using one of the following options.
  - Double-click **TRCPlayer.jar**.
  - Click **Start > Run** and browse to the **TRCPlayer.jar** file.
- In the Open file window, browse to the directory that the saved recording is stored in.
- Select the recording and click **Open**.

The recording starts to play.

The following buttons and functions are available in the Session Player. You can also use the slider to fast forward or rewind the recording to a specific time. For example, to fast forward the recording to a point 5 minutes into a 40-minute recording, move the slider to the right until the time is displayed as 05:00/40:00.

### Play

To play the selected recording. When the Play button is clicked it, changes to the **Pause button**.

### Pause

To pause the recording while it is playing. When the Pause button is clicked, it changes to the **Play button**.

### Stop

To stop the recording and clear the play back window.

### Open file

To open a recording file for playing.

- Browse to the required recording file.
- Select the required file and click **Open** for the recording to start playing.

### Enable Auto Scrolling View

To bring the non-visible parts of the recording into view. As the recording is playing, if the mouse pointer reaches the edge of the player window, the viewing area scrolls in the relevant direction. The function works in both the Vertical and Horizontal directions.

### Enable Scaled View

To scale down the display of the recording to fit fully inside the playback window.



**Note:** The top-level folder of the path where recordings are stored in the target by default, is a hidden folder. The hidden folder location applies for Windows™ Vista operating system and later. If a target user downloads the recording viewer and tries to open a stored recording, they must either change the windows folder settings to show hidden folders. They can also type `c:\ProgramData` in the **File open** window in the viewer and go to the folder where the recording is stored.

## Transfer of files during an active session

During an Remote Control remote control session, you can transfer files in two ways.

- In a File Transfer Mode Session
- Using the **File Transfer** menu

Use the **File transfer** menu options to transfer files during an **active** session. The options available in the **File transfer** menu are determined by the policies that are set for the active session and can include:

### Send file

To transfer a file from the controller to the target. For more information about this option, see [Sending files to the target \(on page 84\)](#).

#### **Pull file**

To transfer a file from the target to the controller. For more information about this option, see [Receiving files from the target \(on page 84\)](#).

#### **Open transfer folder**

To view the contents of your file transfer folder. For more information about this option, see [Opening the file transfer folder \(on page 85\)](#).

#### **Open remote transfer folder**

To view the contents of the target's file transfer folder. For more information about this option, see [Opening the target's file transfer folder \(on page 85\)](#).

#### **Toggle Show Transfers**

To view the list of files that are transferred during the session. For more information about this option, see [Viewing the list of transferred files \(on page 85\)](#).



#### **Note:**

1. The **Open transfer folder** option is also available in a Chat Only, Guidance, or Monitor session.
2. The target user might be asked to accept or refuse the file transfer request if the user acceptance policies are enabled for the session. If they refuse, the file is not transferred.

## **Sending files to the target**

Use the **Send file** option to transfer files from the controller system to the target system during an active session.

To send a file to the target complete the following steps :

1. Click **File transfer menu > Send file**.  
The **Send File to Client** window opens.
2. Select the required file and click **Send File**.

A progress bar is shown as the file is transferred to the file transfer directory on the **target**.

## **Receiving files from the target**

Use the **Pull file** option to transfer files from the target system to the controller system during an active remote control session.

To receive a file from the target complete the following steps :

1. Click **File transfer menu > Pull file**.

If the **Enable user acceptance for file transfers** policy is enabled for the session the target user must accept or refuse the request to transfer the file. If they accept the request, the **Choose file to send** window opens displaying the contents of the targets file transfer directory. If they refuse, or do not respond in a given time, a refusal message is displayed and the file transfer is not allowed.



**Note:** If the target user does not respond in the given time and the **Acceptance timeout action** server policy is set to PROCEED, the **Choose file to send** window opens.

If **Enable user acceptance for file transfers** is set to No, user acceptance is not required by the target user and you can continue with the file transfer.

2. Click the up arrow to change to a different location if required.
3. Select the required file and click **OK**.

The **Pull file to Destination** window opens displaying the contents of your file transfer directory. Select a different location if required.

4. Click **Save**.

The file is transferred to the file transfer directory or the selected destination folder on your system .

## Opening the file transfer folder

Use the **Open transfer folder** option in the controller window, to open the controller's file transfer directory and view the list of files that have been received from the target.

To open the file transfer folder click **File transfer menu > Open transfer folder**.

The content of the controller's file transfer directory is displayed. The target user does not see this folder.

## Opening the target's file transfer folder

Use the **Open remote transfer folder** option in the controller window, to open the target's file transfer directory and view the files that have been received from the controller.

To open the file transfer folder click **File Transfer Menu > Open remote transfer folder**.

The content of the target's file transfer directory is displayed in the session window. The controller user and target user can both view the contents.


## Viewing the list of transferred files

Use the **Toggle Show Transfers** option to view the list of files that have been transferred during the session. You can also open your file transfer directory. The list of files contains all files that have been transferred from the controller to the target and from the target to the controller during the current session.

To open the File Transfers window click **File Transfer Menu > Toggle Show Transfers**.

The File Transfers window opens and displays the list of files.



**Note:** Use the **Open transfer folder**  button to view the contents of your file transfer directory.

## Editing the file transfer directory location on the target

The directory defined as the file transfer directory, on the target, is determined by the **TransferDir** property. This property is defined in the target properties. You can modify this property and set a new file transfer directory location. Follow the steps relevant to the target operating system to change the directory.



**Note:** You require administrative authority to edit the target registry.

:-

### Windows® system

1. At a command prompt window run regedit.
2. Navigate to `HKEY_LOCAL_MACHINE/SOFTWARE/BigFix/Remote Control/Target`.
3. Right-click **TransferDir**.
4. Select Modify and type the required location into the Value data field.
5. Click **OK**.
6. Restart the target service.

### Linux® system

1. Edit the `trc_target.properties` file.
2. Change the value of **TransferDir** to the required location and save the file.
3. Restart the target service.

## Copying clipboard information between the controller and target

Use the **Clipboard transfer menu** to send clipboard information to and from the controller and target systems during a remote control session. You can use this function to copy text from your system into the clipboard then paste this into the target system or from the target system to your system.

The **Clipboard transfer menu** provides two options for transferring clipboard information.

### Send clipboard text

use this option to send text from the controller system to the target system.

### Pull clipboard text

use this option to transfer text from the target system to the controller system.

## Sending clipboard text to the target

You can send text to the target user during a remote control session by using the clipboard.

To send text to the target during a session, by using the clipboard, complete the following steps:

1. On your system, highlight the text that you want to send to the target.
2. Right-click and select **Copy** or click **Edit, > Copy**
3. Click **Clipboard transfer menu > Send clipboard text**.
4. On the target system, select **Edit > Paste** or click **CTRL+V**, in the location that you want to paste the text. For example, in a text file.

The text is pasted into the required location on the target system.

## Receiving clipboard text from the target

To receive text from the target during a session, by using the clipboard, complete the following steps:


1. In the session window, highlight the text on the target system that you want to copy.
2. Right-click and select **Copy** or click **Edit > Copy**.
3. Click **Clipboard transfer menu > Pull clipboard text**.
4. On your system, select **Edit > Paste** in the location that you want to paste the text. For example, in a text file.

The text is pasted into the required location on your system.

## Connecting to a smart card reader during a session

To provide smart card support on the target during an Active mode session, select a local card reader to create and attach to a virtual card reader on the target. Your local card reader connects to the virtual card reader. During the session, you can use your local card, and reader as though they were on the remote target.

To connect to a smart card reader during a remote control session, complete the following steps:

1. Click **Smartcard selection** . A list of installed card readers is displayed.
2. Select a card reader.

The selected card reader is now ready for use and is connected to a virtual card reader on the target. To select a different card reader you must select the connected reader to disconnect it, then select a new reader. When you connect an additional physical card reader to your system, or remove a card reader, click **Refresh card list** to ensure that you display the most current list. During the session, you can use the credentials from your local card to perform an action on the target or to log on to the target.

For more information about the status messages that can be displayed during the session, see [Smart card status messages \(on page 128\)](#).

The **Smartcard selection** option is available only when the following operating systems are running on the controller and target; Windows 7 or later, or Windows Server 2008 R2 or later. The smart card reader driver must also be installed on the target. For more information about installing the smart card reader driver on the target, see the *BigFix® Remote Control Installation Guide*.

## Network response indication

The network response indicator provides an indication of the network round-trip time during a session. That is, the time it takes for network data to be sent from the controller to the target and the response returned to the controller.

At the start of the remote control session the network response indicator points to the green section. A ping is sent every 20 seconds and the network response indicator changes to indicate how responsive the network is.

After the first network response is returned, the indicator points to a colored section and continues to be updated after each ping is sent.

### Green



Indicates a good network response of 0 - 500 milliseconds.

### Yellow



Indicates a moderate response time of 500 - 1000 milliseconds.

### Red



Indicates a poor network response time of greater than 1 second.

## Viewing multiple target screens

During a session, with a target that is configured with multiple displays, you can toggle between each screen or view all screens at the same time.

Use the **Select Screens**  option in the controller window.




**Note:** When you use guidance or drawing tools on a target that has an 8-bit color depth screen, the drawing area hides the screen content. On other color depths, the drawing area is transparent and you can see the screen content.

- Click **Select Screens** to toggle between each screen on the target. The screen number is displayed as the screen changes.
- Right-click **Select Screens** to view the screens menu.  
You can select a screen or click **All Screens** to view all of the target screens.



## Scrolling the target screen during a session

Use the autoscroll function to view the target's screen, without having to use the scroll bars, when the target's screen is larger than the remote control session window. Use the **Enable autoscrolling view** option to enable this function.


To enable the scrolling function click **Enable autoscrolling view** . When the mouse pointer reaches the edge of the session window the non visible area of the target desktop scrolls into view. Click the icon again to disable the function and the screen no longer scrolls.



**Note:** This function works in both the horizontal and vertical directions. Autoscroll is off by default.

## Viewing the full target screen in a session window

To view the full target screen within the session window use **Enable scaled view** to reduce the size.

To enable the scaling function click **Enable/Disable Scaled View** . When the controller window is re-sized, the target view is re-sized to fit into the controller window. Click the icon again to disable the function and the target screen does not change in size.

Due to a slight increase in processing power it is only recommended that this function is used when remote or local resolutions prohibit viewing of the full screen. When switching this function off, the screen can be re-sized to the remote system by clicking on the @ in the lower right of the controller window. This "Match screen size" button changes the controller window size to match the remote system resolution: that is if the remote system is 800 pixels wide and 600 pixels high, the match screen size function will attempt to change the controller window size so that the remote view area of the UI is also 800 pixels wide and 600 pixels high.



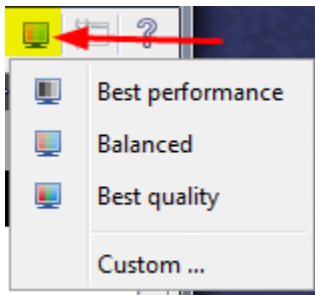
**Note:** When the controller window is first opened, scaled mode is set to disable. This option can be switched at any point during the session.

## Change the color quality of the session window to improve session performance

Use **Performance settings** during a session to adjust the image quality of the target desktop and improve the session performance, if your network is slow. You can also set custom values. The default performance setting at the start of the session is Balanced mode, which is 8-bit color with partial screen updates enabled. This option conserves bandwidth to reduce the amount of data that is passed across the connection during a session.

To select other color options, complete the following steps:

1. Click **Performance settings** and select the relevant session performance option.



#### **Best performance**

Choose this option to display the target desktop in grayscale with partial screen updates enabled. This option can be used when your network is slow. Use it when session performance is more important than the image quality of the target desktop in the session window.

#### **Balanced**

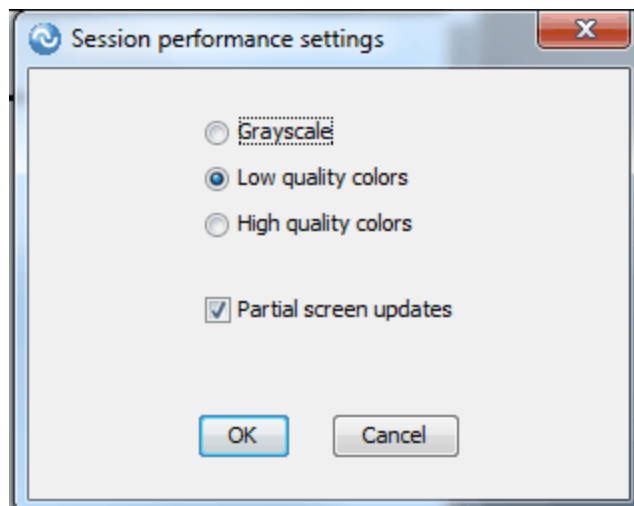
Choose this option to display the target desktop in 8-bit color mode with partial screen updates enabled. This option is the default value.

#### **Best quality**

Choose this option to display the target desktop in 24-bit color mode and partial screen updates disabled. This option can be used when the image quality of the target desktop in the session window is important. However, more bandwidth is used for the session and there is a slower response to actions during the session.

#### **Custom**


Use the custom option to set your own session performance options. You are not restricted to having partial screen updates only with certain color modes. For example, Best quality does not have partial screen updates enabled. You can use the custom option to select **High quality colors** (24-bit color mode) and enable partial screen updates.



- a. Select the relevant color mode.
- b. Select **Partial screen updates** to gradually display the image as it updates. If you clear this option and you have a slow network connection, there is a delay before the updated screen image is displayed.
- c. Click **OK**.

## Change the color depth of the session window

Use **Enable true colour** during a session, to switch between an 8-bit or 24-bit color view of the target desktop. The default view when you open the controller window at the start of the session is 8-bit. This feature conserves bandwidth by reducing the amount of data that is passed across the connection during a session, with 8-bit color.

To enable true color, click **Enable true colour** . The view in the session window changes to 24-bit color. Click the icon again to disable the true color view and revert to 8-bit color.



**Note:** At the start of a session, 24-bit color mode is disabled. Depending on the policies that are set for the session, the color mode can be switched at any point during the session. If the **Lock colour depth** policy is enabled, you cannot switch to a different color mode. For more information about policies and permissions, see the *BigFix® Remote Control Administrator's Guide*.

## Creating a local configuration for the controller

When you install the controller component, you can configure properties and the properties are saved to the `trc_controller.cfg` file in the controller installation directory. The properties in this file are used each time the controller starts and are the same for all users. However, you can also create a user-specific configuration after installation by using the **Configure controller** option in the controller UI.

The first time that you use the option, the configuration window displays the values that are set in the `trc_controller.cfg` file. When you save new values in the configuration window, the properties are saved to a `trc.properties` file. The file is in the `.trc` directory in your home directory. The property values in the `trc.properties` file override the property values in the `trc_controller.cfg` file.

You can set a mandatory property option in the global properties so that a user cannot edit the property in the **Configuration Window**. A mandatory property overrides a local property. This option applies to the properties in the **General Tab** only.

To set a property to mandatory, complete the following steps:

1. Edit the `trc_controller.cfg` file. You might need to change the permissions on the file to edit it.
2. For the property that you want to make mandatory, copy the property name and add `.mandatory = true` to the end.

For example, to make the **Enable Address History** property mandatory so that it cannot be edited in the **Configuration Window**:

```
enable.address.history=false
```

```
enable.address.history.mandatory=true
```

3. Save the file.
4. Stop and start the controller component.

To configure the controller properties in the controller UI, complete the following steps:

1. Click **Configure Controller > Configure**.
2. Configure options on the **General** tab.

Use the **General** tab to configure properties for peer to peer sessions only. Configure the following properties:

#### **Enable Address History, Enable User History, Enable Domain History**

Select the properties to store a history of the target IP addresses, user IDs, and domain names that are used to start a peer-to-peer session. The items are then available for selection in the **Open Connection** window when you start a peer to peer session. The history is stored in the `trc_history.properties` file in your home directory.

#### **Maximum Number of History Items**

Specify the maximum number of items you want to store in the history.

#### **RC Default Port**

Specify the port number that is displayed in the **Connection Window** when you start a session. If left blank, 888 is used by default.

#### **Collaboration Default Port**

Specify the port number that the controller listens on for collaborators who join a collaboration session. If left blank, 8787 is used by default.

#### **Enable Collaborator Join Prompt**

Select this option to display a prompt to indicate when a new controller requests to join a collaboration session.

#### **Forth v2 Security Level**

Allows compatibility with an earlier version of target. Default is 3. Select a lower level if the controller needs to connect to older targets.

#### **Hide Chat**

Select this option to hide the **Chat Only** button on the **Open Connection** window.



**Note:** Although the buttons can be displayed on the **Open Connection** window, this session type is not available on the BigFix® Remote Control Target for macOS target.

### Hide Guidance

Select this option to hide the **Guidance** button on the **Open Connection** window.



**Note:** Although the buttons can be displayed on the **Open Connection** window, this session type is not available on the BigFix® Remote Control Target for macOS target.

### 3. Configure options on the **Run Tools** tab.

Use the **Run Tools** tab to create a list of tools that you can run on the target during a remote control session. The tools are displayed as menu items in the **Perform Action in target** menu in the controller UI.



**Note:** If the **Edit** and **Remove** options are not available when you select the item, you cannot change or remove the item.

### To add a tool, complete the following steps:

- a. Click **Add**.
- b. Enter values for the tool.

#### Tool Name

Enter a name for the tool. The name is displayed as a menu item in the **Perform Action in target** menu. For example, **Control Panel**.

#### Tool Command

Enter the command to run the tool. For example, to run the **Control Panel** if you are using a Windows™ operating system, enter

```
[System Folder]\control.exe
```

If you are using a Linux™ operating system, enter

```
/usr/bin/gnome-control-center
```

#### Tool Parameters

Optional. Specify parameters for the command to run.

#### Tool User

Optional. Determines which privileges or credentials the command is run with. If left blank, run the tool as the logged on user.

- c. Click **OK**.

### To edit a tool entry, complete the following steps:

- a. Select a tool.
- b. Click **Edit**.
- c. Change the values for the tool.
- d. Click **OK**.

**To remove a tool entry, complete the following steps:**

- a. Select a tool.
- b. Click **Remove**.

4. Configure options on the **Key Sequences** tab.

Use the **Key Sequences** tab to create a list of special keys, or often repeated sequences of special keys, that can be sent to the target during a remote control session. The key sequences are displayed as menu items in the **Perform Action in target** menu in the controller UI.



**Note:** If the **Edit** and **Remove** options are not available when you select the item, you cannot change or remove the item.

**To add a Key Sequence, complete the following steps:**

- a. Click **Add**.
- b. Enter values for the key sequence.

**Key Sequence name**

Enter a name for the key sequence. The name is displayed as a menu item in the **Perform Action in target** menu. For example, `Inject F1`.

**Key Sequence Value**

Enter a sequence of keys. The sequence of keys is sent to the target computer. For example, to send the F1 key, enter `[F1]`.

- c. Click **OK**.

**To edit a key sequence entry, complete the following steps:**

- a. Select a key sequence.
- b. Click **Edit**.
- c. Change the values for the key sequence.
- d. Click **OK**.

**To remove a key sequence entry, complete the following steps:**

- a. Select an entry from the list.
- b. Click **Remove**.

5. Click **OK** on the configuration window to save the configuration to the `trc.properties` file.



**Note:** After you create your own configuration, you can reset the local values to the global values that are in the `trc_controller.cfg` file. Click **Revert** on the **Configuration Window** to display the global values. You must click **OK** on the **Configuration Window** to save the reverted values to the `trc.properties` file.

## Enabling debug in the local controller configuration

A property is now available to enable debug in the local configuration on the Remote Control controller.

Use the **debug.trace** property to enable debug on the controller. To enable debug, complete the following steps:

1. Edit the `trc.properties` file that is in your home directory.

The file is in the following directory.

### Windows systems

`USERHOMEDIR\.trc\trc.properties`, where `USERHOMEDIR` is the home directory of the logged on user.

### Linux or macOS systems

`USERHOMEDIR/.trc/trc.properties`, where `USERHOMEDIR` is the home directory of the logged on user.

2. Set `debug.trace=true`.
3. Save the file and restart the controller.

The next time that you start a session, the events that take place are logged in the `trctrace_XXXXX.log` file in your home directory. The file name contains the date and time stamp of when the file was created. For example, `trctrace_20170309_124230.log`

## Obtaining help

When using the controller interface you can access the online documentation or find out the version of Remote Control that you are running by using the **Shows Help** icon.

1. Click **Shows Help** in the toolbar



2. Select the required item

### Help

to access the online Remote Control documentation.

### About

to open a window displaying the product name and version number. Click the window or any key to return to the Remote Control controller window.

## Ending a Session

You can end a remote control session in the following ways:

- Click the **Connection** icon in the taskbar.



- Click the **X** in the upper right of the controller window.

Click **Yes** to quit the session.

The session ends and the target user regains sole control of their desktop. The target user can press **Pause** on their keyboard or click the connection icon to end the session. If the target user closes the session, it ends immediately. A message might be displayed when you disconnect.

If collaboration is started in the session and you are the master controller of the session, you are warned that collaboration is in progress. The following message is displayed. `A Collaboration session is in progress. If you disconnect, the session will end. Keep the session open?`

You can choose to disconnect and end the session or choose to remain in the session as the master controller.

### Cancel

When you click **Cancel**, the collaboration session continues and you are still the master controller.

### Disconnect session

When you click **Disconnect session**, the collaboration session ends and all participants are disconnected.



# Chapter 5. Use remote control commands from the command line

You can install tools that you can use to start a remote control session from the command line. You can also use the tools to run a command on a target and see the output of the command on your computer.

The cli tools can be useful if you want to connect to a target without using the BigFix® Remote Control Server interface. You can also use them as part of a script to run multiple commands. For more information about installing the cli tools, see the *BigFix® Remote Control Installation Guide*.

**COMMAND** session mode in server session policy must be enabled to use the CLI tools.

There are two command line tools available

- `wrc` - to start a remote control session.
- `wrcmdpcr` - to run a command on a target and see the output from the command on your computer.

Before you use the command line tools, the following configuration actions must be carried out.

- The server URL defined in the `trc.properties` file on the server must be the same as the URL that is defined in the **ServerURL** property in the target properties.
- The remote control port that is defined during the installation of the command line tools must be the same on both the computer that the commands are being run from and in the target settings.
- If FIPS compliance is required, you must enable FIPS on the computer that you use to run the command from and also on the target. For more information about enabling FIPS compliance, see the *BigFix® Remote Control Installation Guide*.



**Note:** The computer that is starting the controller software requires a **JavaHome** registry key entry. **JavaHome** must contain the path to the FIPS-compliant IBM® JRE that is installed with the controller software. If you are starting the controller on a remote computer, you must create a registry key entry on the remote computer too.

## Windows® systems

```
C:\Program Files\BigFix\Remote Control\Controller\jre
```

## Linux® systems

Edit the `trc_target.properties` file and update the value of the **JavaHome** property.

- An **INFO** level log, `cli_trace_[suffix].log` is created on the computer that you run the cli tools from. Where `[suffix]` is determined by the value of the LOGROTATION property. For example, `cli_trace_Mon.log`. To create a **DEBUG** level log, change the LOGLEVEL property value to 4.

## Windows system

1. Edit the target registry and go to `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`



**Note:** On a 64-bit system, all the 32-bit registry keys are under the WOW6432Node key. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`

2. Right-click **LogLevel** and select **Modify**
3. Set the value to 4 and click **OK**.

Edit the target registry

### Linux system

Edit the `/etc/trc_target.properties` file and set **LogLevel=4** and save the file.



**Note:** The `wrc` and `wrcmdpcr` commands do not work if you start the remote controller or the commands on computers where you need to establish the connection through Remote Control gateways.

## Starting a remote control session from the command line

You can start a session with a target by running the `wrc` command.

Use this command to specify the type of remote control session that you would like to start with the target.



**Note:** The target software must be installed on the target that you are starting a session with.

To start a remote control session, complete the following steps:

1. At a command prompt go to the directory where you installed the command-line tools.
2. Type in the `wrc` command to start a session

The command has the following syntax:- `wrcuser:passwordAction Rctarget[Rccontroller][options]`

### **user:password**

To provide a valid user ID and password to log on to the BigFix® Remote Control Server.

### **Action**

To define which type of remote control session you want to establish.

### **rc**

To start a remote control session whose type is determined by the value that is assigned to option `-S`. Used with option `-S`.

### **filexfer or filetransfer**

To start a file transfer session with the target.

**active**

To start an active session with the target.

**reboot**

To restart the target computer.

**guidance**

To start a guidance session with the target.

**monitor**

To start a monitor session with the target.

**chat**

To start a chat session with the target.

**Rctarget**

To specify the computer name or the IP address of the target to connect to. The parameter has the following syntax:

@Endpoint:<computername or ipaddress>

**Rcontroller**

To run the controller on a different computer, type the computer name or IP address of the other computer. If you do not specify a value for this parameter, the controller is started from the computer that the command is run from. The parameter has the following syntax:

@Endpoint:<computername or ipaddress>

To use the controller to start a session, the following conditions must apply.

- The target software must be installed on the computer where you want the controller to run.
- A Java™ Runtime Environment supported by Remote Control is installed on the controller computer.
- The computer that you enter the command from must be able to establish a TCP connection, on the remote control port set at installation, to the computer where you are starting the controller.

**options****-S**

Use with the **rc** action.

**A**

If the rc action is set, set **-S** to A to start an Active session .

**M**

If the rc action is set, set **-S** to M to start a Monitor session.



**Note:** If you use this option with an action other than **rc**, the value set in the **Action** parameter determines the type of remote control session. The **-S** value is ignored.

## Examples of usage

The examples listed here use target IP address **192.0.2.1**, controller computername **testcontroller**, userid **newuser1** and password **newuser100**.

1. The command below activates a guidance session between the target and the machine that the command is being issued from.

```
wrc newuser1:newuser100 guidance @Endpoint:192.0.2.1
```

2. Either of the commands below will activate an active session between the target and the machine that the command is being issued from.

```
wrc newuser1:newuser100 rc @Endpoint:192.0.2.1 -S:A
```

```
wrc newuser1:newuser100 active @Endpoint:192.0.2.1
```

3. Either of the commands below will activate a monitor session between the target and controller **testcontroller**.

```
wrc newuser1:newuser100 rc @Endpoint:192.0.2.1 @Endpoint:testcontroller -S:M
```

```
wrc newuser1:newuser100 monitor @Endpoint:192.0.2.1 @Endpoint:testcontroller
```

## Running commands on the target from the command line

Use the **wrcmdpcr** command to connect to a target and run a non-interactive command-line command.

You can specify the command that you want to run on the target, and the output from that command is displayed on the computer that the command is started from. This command can be useful for debugging a target when you do not have access to the BigFix® Remote Control Server user interface.

To start a command on a target, complete the following steps:

1. At a command prompt, go to the directory where you installed the command-line tools.
2. Type in the following command

```
wrcmdpcr user:password Rtarget command [argument ...]
```

**user:password**

Use to specify a valid user ID and password that you would use to log on to the BigFix® Remote Control Server.

### **Rctarget**

Use to specify the computer name or the IP address of the target that you want to connect to and run a command on. It has the following syntax:

*@Endpoint:<computername or ipaddress>*

### **command**

Use to specify a command that runs from the command line. For commands that are built into the operating system's shell and do not have a binary executable file. For example, dir or tree in a Windows™ operating system. In a Linux™ operating system, cd or echo. You must also add the command shell command.

#### **Windows™ systems**

You must type **cmd /c** before the command. For more information, see [Examples of usage \(on page 101\)](#).

For example, cmd /c dir

#### **Linux™ systems**

You must type **sh -c** before the command. For more information, see [Examples of usage \(on page 101\)](#).



#### **Note:**

- a. The command that you run must be specific to the operating system that is running on the target. If you are entering the command from a Windows™ computer to a target that has a Linux™ operating system installed, you must specify the Linux™ command.
- b. If you are entering the command from a Linux™ computer to a target that has a Windows™ operating system installed and you are using path names in the argument, you must use a double backslash in the argument. For example, `\windows`.
- c. The command that you want to run must be in the PATH statement of the target, otherwise the full path to the command must be used.

### **argument**

Use to provide arguments for the command that you want to run on the target.

## Examples of usage

The examples listed here use target IP address **192.0.2.1**, userid **newuser1** and password **newuser100**.

1. The command below displays a directory listing, of the temp directory, on the machine that is issuing the command.

```
To display the contents of temp on a windows target

wrcmdpcr newuser1:newuser100 @Endpoint:192.0.2.1 cmd /c dir \temp


To display the contents of temp on a linux target

wrcmdpcr newuser1:newuser100 @Endpoint:192.0.2.1 ls /temp
```

2. The command below copies a file from the temp directory to the match directory of a windows target. Type the whole command on one line.

```
wrcmdpcr newuser1:newuser100 @Endpoint:192.0.2.1 cmd /c
copy c:\temp\1.csv c:\match
```

3. The command below displays the network statistics of a windows target

```
wrcmdpcr newuser1:newuser100 @Endpoint:192.0.2.1 cmd /c netstat
```

## Error messages for the wrc and wrcmdpcr commands

If there is an error executing the wrc or wrcmdpcr command, the following error codes are returned as the program exit code and the corresponding message is displayed.

Table 6. Error messages for the wrc command

Ex- it Code	Message	Reason	Ap- plies to
1	Invalid argument: Mal- formed user:password  Invalid argument: Un- known action  Invalid argument: Target endpoint definition: {0}  Invalid argument: Con- troller endpoint defini- tion: {0}  Error reserving memory for arguments	Invalid parameters passed to command. Verify the parameters in the com- mand line are valid and comply with the expected command syntax	both

**Table 6. Error messages for the wrc command (continued)**

Ex- it Code	Message	Reason	Ap- plies to
	Invalid argument: Un- known option: {0}		
2	Error: No settings for the Server URL found	There is no ServerURL setting in the registry or properties file. Ensure the configuration is correct and the ServerURL configuration field has the correct URL for the remote control server.	both
3	Error {0} (RC_SERVER_CONN_ER- ROR): Unable to connect to the Server	Unable to connect to the configured server. Ensure the configuration is correct and the ServerURL configuration field has the correct URL for the remote control server.	both
4	Error {0} (RC_LOGIN_ER- ROR): Unable to login to the Server with the specified credentials	Cannot log in to the Remote Control server with the credentials provided in the command parameters. Ensure the correct user credentials are entered in the command line.	both
5	Error {0} (RC_CREATE_SESSION_- ERROR): Unable to create RC ses- sion	The remote control session to launch the command cannot be created. The normal causes are that the user does not have permissions or the target cannot be found.	both
6	Error {0} (RC_LOCAL_LAUNCH_- ERROR): Unable to launch the Ja- va™ Web Start controller	The Java™ Web Start Remote Control Controller cannot be launched on the local machine. Usually this would be caused by a supported JRE not being installed and set up to handle Java™ Web Start applications correctly.	wrc
7	Error: Failed to load FIPS support libraries	The settings specify FIPS mode but the required libraries cannot be loaded. This can be caused by the installed files being corrupted.	both

**Table 6. Error messages for the wrc command (continued)**

Ex- it Code	Message	Reason	Ap- plies to
8	Error: Failed to load OpenSSL support libraries	There was an error loading the OpenSSL libraries. This can be caused by the installed files being corrupted.	both
10	Error {0} (RC_REMOTE_CONNEC- T_ERROR): Unable to connect to the remote controller to launch the session	The connection to the remote controller cannot be established. Verify that the target software is running on the specified remote controller endpoint and it is possible to establish remote control sessions to it.	wrc
10	Error {0} (RC_REMOTE_CONNEC- T_ERROR): Unable to connect to the target	The connection to the target endpoint cannot be established. Verify that the target software is running on the specified target endpoint and it is possible to establish remote control sessions to it.	wr- cmd- pcr
16	Error {0} (RC_REMOTE_- LAUNCH_ERROR): Unable to launch con- troller on the remote machine	After connecting to the target, launching the controller failed. Usually this would be caused by a supported JRE not being installed and set up to handle Java™ Web Start applications correctly.	wrc
16	Error {0} (RC_REMOTE_CMD_EX- EC_ERROR): Unable to launch the command in the remote machine	After connecting to the target, the specified command could not be executed. Verify the command is correct and is not interactive, and can be executed locally on the target machine.	wr- cmd- pcr
17	Error {0} (RC_REMOTE_CMD_- TERM_ERROR):	After connecting to the target and successfully launching the command, the command has terminated abnormally. Verify the command is correct and is not interactive, and can be executed locally on the target machine.	wr- cmd- pcr



**Table 6. Error messages for the wrc command (continued)**

Ex- it Code	Message	Reason	Ap- plies to
	The remote command terminated abnormally		
20	Error {0} (RC_UNKNOWN_TARGET): The specified target is not registered with Remote Control	The specified endpoint is not a registered remote control target. This could apply to the specified target endpoint or the controller endpoint. Verify the host names or IP addresses are correct and belong to machines that have a correctly registered remote control target.	both
21	Error{0 (RC_UNREACHABLE_TARGET): The specified target is offline or does not have any connectivity information associated with it.	The specified endpoint is a registered remote control target but it has no connectivity information or the connection cannot be established. This could apply to the specified target endpoint or the controller endpoint. Ensure the remote control target is running and has reported the current connectivity details to the remote control server and verify a remote control session can be established with that target.	both
22	Error {0} (RC_NO_PERMISSIONS): No permissions to start the session in the selected mode.	The specified endpoint is a registered remote control target but the user specified in the command line is not allowed to connect to the remote control target in the specified endpoint. This could apply to the specified target endpoint or the controller endpoint. Contact your remote control Administrator to verify the permissions	both
23	Error {0} (RC_TARGET_TOO_OLD): The target on the remote machine is too old and should be updated	The endpoint the CLI tool is attempting to connect to has an installed version of the remote control target software that is too old. This could apply to the specified target endpoint or the controller endpoint. Upgrade the target software in the endpoint.	both

Table 6. Error messages for the wrc command (continued)

Ex- it Code	Message	Reason	Ap- plies to
24	Error {0} (RC_TARGET_IS_- BUSY): The target on the remote machine is already in a session	The endpoint the CLI tool is attempting to connect to is already in a remote control session so it cannot handle the connection by the CLI tool. This could apply to the specified target endpoint or the controller endpoint. Try the CLI command again once the target is free.	both

## Chapter 6. Configuring global controller properties

Edit the `trc_controller.cfg` file to create and configure global controller properties. The properties are used by the Remote Control controller component during a peer to peer remote control session. The property values are the same for every user who runs the controller.

For more information about configuring global controller properties for managed remote control sessions, see the section on editing property files in the *BigFix® Remote Control Administrator's Guide*.

A user can also configure a set of properties locally, by using the **Configure Controller** feature in the controller UI. The local property values override the global property values. For more information about configuring local properties, see [Creating a local configuration for the controller \(on page 91\)](#).

To enforce the global property value, you can set a property to *mandatory* so that a user cannot edit the property in the **Configuration Window** in the controller UI. The *mandatory* global property overrides the local property.

To configure the controller properties, complete the following steps:

1. Edit the `trc_controller.cfg` file.



**Note:** To edit the file, you must have administrator authority on the system that the controller component is installed on.

### Windows® systems

```
[controller install dir]\trc_controller.cfg
```

Where *[controller install dir]* is the directory that the controller is installed in.

### Linux® systems

```
opt/bigfix/trc/controller/trc_controller.cfg
```

2. Add or configure the relevant property.

To set a property as *mandatory*, copy the property name and add `.mandatory = true` to the end.

For example, to make the **Enable Address History** property *mandatory* so that it cannot be edited in the **Configuration Window**.

```
enable.address.history=false
```

```
enable.address.history.mandatory=true
```

3. Save the file.
4. Stop and start the controller component.

The new property values are in effect for any new peer-to-peer sessions that the controller starts with a target.

## Run tools on the target during a peer to peer session

You can create and configure controller properties to run specific tools on the target computer during a remote control session.

The configured properties are displayed as menu items in the **Perform Action in target** menu in the controller window, in alphabetical order.



**Note:** If too many items are added to the **Perform Action in Target** menu, the last items in the menu might extend beyond the bottom of the screen. This issue is seen particularly on a smaller screen size because there is no support for scrolling menus.

Only the tools entries that commands exist for on the target computer are displayed during the session. At the start of the session, the controller sends a list with all the configured tools to the target. The target verifies that each command exists and returns a list back to the controller with all the available commands. The action menu for the session is populated with the available tools.



**Note:** For a target where a Linux™ operating system is installed. In addition to checking that the tools exist it is also checked whether the target has permission to run the tools.

Each tool can be defined by using a number of entries in the controller properties file, some of which are optional. Entries that belong to the same tool must all have the same prefix. There are seven preconfigured tools by default that you can change to your own requirements. There are also three blank tools available by default. For details of editing the properties file for a peer to peer session see, [Configuring global controller properties \(on page 107\)](#). For details of editing the properties file for a managed session, see the BigFix® Remote Control Administrator's Guide. Create and configure the properties in the following format.

Property name	Re- quired	Default value	Description
prefix.ToolName	Yes	N/A	Display name that is used in the <b>Perform Action in target</b> menu.
prefix.ToolName.\$lang\$	No	N/A	Translation of display name. \$lang\$ is ISO language code.
prefix.ToolCommand	Yes	N/A	Command to run the tool, without parameters.
prefix.ToolParameters	No	N/A	Optional parameters for the command to run.
prefix.ToolUser	No	<blank>	Determines which privileges or credentials the command is run with.
		<blank>	Run the tool as the logged on user.

Property name	Re- quired	Default value	Description
---------------	---------------	------------------	-------------



**Note:** Might trigger UAC prompts depending on the version of Windows™.

#### admin


Run the tool with UAC prompt to elevate privileges.

### Required property definitions

```
prefix.ToolName=
```

Modifiable Field	<b>prefix.ToolName</b>
Field Description	Display name that is used in the <b>Perform Action in target</b> menu. Each defined tool name must have a different prefix.
Possible Values	User Defined. For example,  <code>wincmd.ToolName=Command Prompt</code>  The text, <b>Command Prompt</b> , is displayed in the <b>Perform Action in target</b> menu.
Value Definition	

```
prefix.ToolCommand=
```

Modifiable Field	<b>prefix.ToolCommand</b>
Field Description	Command to run the tool, without parameters.
Possible Values	User Defined.  The tool command can be a fully qualified path or just the file name. For example, <code>wincmd.ToolCommand=cmd.exe</code> and <code>wincmd.ToolCommand=[SystemFolder]\\cmd.exe</code> are equivalent.   <b>Note:</b> When you use a backslash in the path you must enter two backslashes.  The file must be on the PATH environment variable of the logged in user. You can specify executable files and also files that are associated with an exe-

	<p>cutable file. Do not use quotation marks, even when there are spaces in the path or file name.</p> <p>For example, services.msc is associated with <code>mmc.exe</code> (Microsoft™ Management Console).</p> <p>All of the following examples are equivalent:</p> <pre>prefix1.ToolCommand = services.msc</pre> <pre>prefix2.ToolCommand = [SystemFolder]\services.msc</pre> <pre>prefix3.ToolCommand = [SystemFolder]\mmc.exe</pre> <pre>prefix3.ToolParameters = [SystemFolder]\services.msc</pre> <p>You can use the following folder properties when you define tools parameters on a Windows™ system. The target substitutes these properties with the actual path on the target system.</p> <p><b>[WindowsFolder]</b></p> <p>The target uses the following path to run the tool. <code>[WindowsVolume]\Windows</code></p> <p><b>[SystemFolder]</b></p> <p>The target uses the following path to run the tool. <code>[WindowsFolder]\System32</code></p> <p>Folder properties are not relevant for Linux™ targets. <code>lnxcontrol.ToolCommand = /usr/bin/gnome-control-center</code></p>
Value Definition	

## Preconfigured tools

tool01.ToolName = Control Panel

tool01.ToolCommand = [SystemFolder]\\control.exe

tool01.ToolParameters =

tool01.ToolUser =

tool02.ToolName = Command Prompt

tool02.ToolCommand = [SystemFolder]\\cmd.exe

tool02.ToolParameters =

tool02.ToolUser =

tool03.ToolName = Administrator Command Prompt

tool03.ToolCommand = [SystemFolder]\\cmd.exe

```
tool03.ToolParameters =
```

```
tool03.ToolUser = admin
```

```
tool04.ToolName = Task Manager
```

```
tool04.ToolCommand = [SystemFolder]\\taskmgr.exe
```

```
tool04.ToolParameters =
```

```
tool04.ToolUser =
```

```
tool05.ToolName = Windows™ Explorer
```

```
tool05.ToolCommand = [WindowsFolder]\\explorer.exe
```

```
tool05.ToolParameters =
```

```
tool05.ToolUser =
```

```
tool06.ToolName=Terminal
```

```
tool06.ToolCommand=/usr/bin/gnome-terminal
```

```
tool06.ToolParameters =
```

```
tool06.ToolUser =
```

```
tool07.ToolName=Control Panel
```

```
tool07.ToolCommand=/usr/bin/gnome-control-center
```

```
tool07.ToolParameters =
```

```
tool07.ToolUser =
```

## Send key sequences to the target during a remote control session

You can create and configure controller properties to send special keys, or often repeated sequences of special keys, to the target during a remote control session.

The configured properties are displayed as menu items in the **Perform Action in target** menu in the controller window, in alphabetical order.



**Note:** If too many items are added to the **Perform Action in Target** menu, the last items in the menu might extend beyond the bottom of the screen. This issue is seen particularly on a smaller screen size because there is no support for scrolling menus.

These menu items are available for every session that the controller takes part in. Define the key sequences in the controller properties files. Each key sequence can be defined using a number of entries in the properties file, some of which are optional. Entries that belong to the same key sequence should all have the same prefix. For details of editing the properties file for a peer to peer session see, [Configuring global controller properties \(on page 107\)](#). For details of editing the properties file for a managed session, see the BigFix® Remote Control Administrator's Guide. Create the properties in the following format.

## Property definitions

```
prefix.KeySequenceName=
```

Modifiable Field	<b>prefix.KeySequenceName</b>
Field Description	Display name that is used in the <b>Perform Action in target</b> menu. Each defined key sequence name must have a different prefix.
Possible Values	User Defined. For example,  <code>injectF1.KeySequenceName = Inject F1</code>  The text, <b>Inject F1</b> , is displayed in the <b>Perform Action in target</b> menu.
Value Definition	

```
prefix.KeySequenceName.language=
```

Modifiable Field	<b>prefix.KeySequenceName.language</b>
Field Description	Translations for display name. This property is optional.
Possible Values	User Defined. For example,  <code>injectF1.KeySequenceName.es = Inyectar F1</code>
Value Definition	

```
prefix.KeySequenceValue=
```

Modifiable Field	<b>prefix.KeySequenceValue</b>
Field Description	Macro sequence. The sequence of keys defined here is sent to the target computer.
Possible Values	User Defined. For example,  <code>injectF1.KeySequenceValue = [F1]</code>
Value Definition	

## Example configuration file entries

```
injectF1.KeySequenceName = Inject F1
```

```
injectF1.KeySequenceName.es = Inyectar F1
```

```
injectF1.KeySequenceValue = [F1]
```



injectCTRLALTS.KeySequenceName = Inject CTRL+ALT+S

injectCTRLALTS.KeySequenceValue = [CTRL ALT S]

injectCTRLALT.X.KeySequenceName = Inject CTRL+ALT+X

injectCTRLALT.X.KeySequenceValue = [CTRL+][ALT+]x[ALT-][CTRL-]

injectALTF.KeySequenceName = File Menu

injectALTF.KeySequenceValue = [alt+]f[alt-]

The following explanation can be used for any of the macros that are used. The control key is used as an example.

To press and release the control key, use [CTRL]

To press but not release the control key, use [CTRL+]

To release the control key, use [CTRL-]

## Macros that you can use

CMD	CTRL	CTRL	CTRL	ALT	ALT	ALT
SHIFT	SHIFTL	SHIFTR	META	METAL	METAR	SPECIAL
F1	F2	F3	F4	F5	F6	F7
F8	F9	F10	F11	F12	F13	F14
F15	F16	F17	F18	F19	F20	F21
F22	F23	F24	F25	F26	F27	F28
F29	F30	CAPS	SCROLL	NUM	BACKSPACE	TAB
UP	DOWN	RIGHT	LEFT	PGDN	PGUP	HOME
END	ENTER	ESC	INS	DEL	MENU	PAUSE
BREAK	SYSRQ	PRTSC	CLEAR	UNDO	REDO	CUT
COPY	PASTE	KPSLASH	KPSTAR	KPMINUS	KPLUS	KPENTER
KPINS	KPDEL	KPEND	KPDOWN	KPPGDN	KPLEFT	KPRIGHT
KPCENTER	KPUP	KPPGUP	ALTGR	SYSREQ	SLEEP	APPS
ZOOM	STOP	CANCEL	PROPS	FRONT	OPEN	FIND
VOLUP	VOLDN	MUTE	POWER	CONTRAST_UP	CONTRAST_DN	BRIGHT_UP
BRIGHT_DN	DEGAUSS					

## Retain previously used logon credentials for a peer to peer session

You can configure controller properties to store a history of the target IP addresses, user IDs, and domain names that are used to start a peer to peer session.

These items are then available for selection in the open connection window when a controller user starts a peer to peer session. The history is stored in the `trc_history.properties` file in the home directory of the controller user. Edit the `trc_controller.cfg` file to configure these properties. For more information about configuring properties, see [Configuring global controller properties \(on page 107\)](#).

## Property definitions

```
enable.address.history=
```

Modifiable Field	<b>enable.address.history</b>
Field Description	Determines whether the controller stores a history of recently used IP addresses that were used when you started a peer to peer session. Any IP address that was used to successfully start a session is stored in the IP address history. The history is stored in a file named <code>trc_history.properties</code> . Default value is true.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>the IP address history is enabled in the connection window when you are starting a peer to peer session. Select the required IP address from the list.</p> <p><b>False</b></p> <p>the IP address history is not enabled in the connection window.</p>

```
enable.user.history=
```

Modifiable Field	<b>enable.user.history</b>
Field Description	Determines whether the controller stores a history of recently used user IDs that were used when you started a peer to peer session. Any user ID that was used to successfully start a session is stored in the IP address history. The history is stored in a file named <code>trc_history.properties</code> . Default value is false.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>the user history is enabled in the connection window when you are starting a peer to peer session. Select the required user ID from the list.</p> <p><b>False</b></p> <p>the user history is not enabled in the connection window.</p>

```
enable.domain.history=
```

Modifiable Field	<b>enable.domain.history</b>
Field Description	Determines whether the controller stores a history of recently used domain names that were used when you started a peer to peer session. Any domain name that was used to successfully start a session is stored in the domain history. The history is stored in a file named <code>trc_history.properties</code> . Default value is true.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>the domain history is enabled in the connection window when you are starting a peer to peer session. Select the required domain name from the list.</p> <p><b>False</b></p> <p>the domain history is not enabled in the connection window.</p>

```
history.max.items=
```

Modifiable Field	<b>enable.address.history</b>
Field Description	Sets a limit to the size of the history lists for IP addresses, user IDs, and domains. The oldest item in the history list is removed if the list reaches the <b>history.max.items</b> limit and a new item needs to be added.
Possible Values	0 - 20
Value Definition	A value greater than 20 gives a maximum length of 20 items only in the lists in the connection window. A value of 0 disables the history lists.

## Hiding the master controller acceptance window

When you are the master controller in a collaboration session, you are asked to accept each new participant into the collaboration session. If you are starting collaboration in peer to peer remote control sessions, you can create a controller property and configure it to hide the acceptance prompt so that you do not have to accept each time.

To hide the acceptance prompt, complete the following steps:

1. Edit the **trc\_controller.cfg** file.
2. Add the following entry.  
**enable.join.collab.prompt=false.**
3. Save the file.

When a new participant requests to join the collaboration session, you are not asked to accept the request to share the session. Set **enable.join.collab.prompt=true** to re enable the acceptance prompt. For more information about controller properties, see [Configuring global controller properties \(on page 107\)](#).



**Note:** If you hand over full control of the session to a new master controller, the properties that are defined in their controller properties file, take effect.

## Enabling and Disabling the execution of tools on the target during a remote session

Learn how to enable or disable the execution of tools on the target during a remote session.

To prevent the execution of tools on the target machine from **Perform Action in target** menu in the controller window, a new property has been added in `trc_controller.cfg` and `controller.properties`. Enabling this feature in the target removes the command entries in the **Perform Action in target** menu.

Property name	Required	Default	Description
allow.user.commands	Yes	True	Display/Hide the command entries under <b>Perform Action in target</b> menu.

To configure this controller property, complete the following steps:

### Procedure

#### Peer-to-peer sessions

1. Edit the `trc_controller.cfg` file.

##### Windows systems

```
[controller install dir]\trc_controller.cfg
```

Where `[controller install dir]` is the directory that the controller is installed in.

##### Linux systems

```
opt/bigfix/trc/controller/trc_controller.cfg
```

2. Configure the property by setting true or false.
3. Save the file.

#### Managed sessions

1. Edit the `controller.properties` from the Server console.
2. Configure the property by setting true or false.
3. Save the file.

# Chapter 7. Auditing

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

On the controller computer, you can view the events in a log file. For peer-to-peer sessions, open the `trcaudit.log` file. For managed sessions, open the `trcaudit_[ipaddress]_[token].log`, where `[ipaddress]` is the IP address of the target and `[token]` is the session token value. Both log files are in the user's home directory.

You can also view the events on the target computer.

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

To access the Application Event Viewer in Windows, click **Start > Control Panel > Administrative Tools > Event Viewer > Windows Logs > Application**. You can filter the listed entries by using the following source: `TRCTARGET`.

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.

## User acceptance audit events

The following audit events are triggered by the user acceptance process during the start of a remote control session.

The session audit log from the target showed the same event to indicate that a session was accepted that is `Session Accepted. Reason: User Allowed`. It was not possible to tell from the audit event whether the session was accepted by the user or whether it was accepted automatically for another reason. To improve auditing, the following audit event was deprecated and replaced with four new audit events.

**Table 7. Deprecated audit event**

Event ID	Event Description
ibm.trc.audit- .0003	Session Accepted. Reason: {\0}

**Table 8. New audit events**

Event ID	Event Description	Comments
ibm.trc.audit.0046	Session Accepted by {0}	The session was accepted by the user on the target system. {0} is replaced with the user ID of the current user
ibm.trc.audit.0047	Session accepted automatically after timeout	The session was accepted automatically because the user did not respond to the user acceptance prompt before the <b>Acceptance grace time</b> policy expired. The <b>Acceptance timeout action</b> policy is set to proceed.

**Table 8. New audit events (continued)**

Event ID	Event Description	Comments
ibm.trc.audit.0048	Session accepted automatically because connect at logon is allowed	The session was accepted automatically because there was no user logged on to the target system console and <b>Connect at logon</b> was enabled and set to Yes.
ibm.trc.audit.0049	Session accepted. User acceptance is disabled.	The session was accepted automatically because user acceptance was not enabled.



**Note:** User acceptance can be disabled by using the **Enable user acceptance for incoming connections** policy. However, when this policy is enabled and set to Yes, user acceptance can be disabled for other reasons. If the **Acceptance grace time** policy is set to less than 5 seconds, user acceptance is disabled automatically. This is because the target user would not have enough time to react to the user acceptance prompt. User acceptance is also disabled automatically whenever the target is unable to start the graphical user interface.



**Note:** Take note of the following values for the user ID that is displayed in the user acceptance window:

- If the session is started from the remote control server, the user ID that the controller uses to authenticate against the Remote Control server is displayed.
- If the session is started by running the stand-alone controller console, the user ID that the controller user uses to log on to their local system is displayed.

## Authentication audit events

The following audit events are triggered for peer to peer remote control sessions that require user ID and password authentication against the target system.

That is, those sessions where the target property **CheckUserLogin** is enabled. The session rejected audit event was improved to allow authentication to be audited in sufficient detail. To improve auditing, the following audit event was deprecated and replaced with new audit events.

**Table 9. Deprecated audit event**

Event ID	Event Description
ibm.trc.audit- .0002	Session Rejected by{\0}

**Table 10. New audit events**

Event ID	Event Description
ibm.trc.audit.005A	Authenticating user ID {0} using system logon. Allowed groups: {1}
ibm.trc.audit.005B	Session rejected because the user ID or password is incorrect
ibm.trc.audit.005C	Session rejected because the user is not a member of an allowed group.
ibm.trc.audit.005D	Session rejected by {0}
ibm.trc.audit.005E	Session rejected automatically after {0} seconds
ibm.trc.audit.005F	Session rejected because the session token is invalid
ibm.trc.audit.0060	Session rejected because the session token has expired
ibm.trc.audit.0061	Session rejected because the session token is for a different target
ibm.trc.audit.0062	Session rejected by the server for unknown reason {0}
ibm.trc.audit.0063	Session rejected because {0} mode is not allowed
ibm.trc.audit.0064	Session rejected due to a connection error

The following audit message is written to the audit log by the controller. This message shows which user is logged in to the target computer and which user ID they used to log in Remote Control to control this session.

**Table 11. New controller audit event**

Event ID	Event Description
Audit.logged- .user	User {0} is logged in as {1} in the controller machine

## Smart card audit events

The following audit events can be triggered during a remote control session where smart card authentication is enabled.

## Controller smart card audit events

**Table 12. Controller smart card audit events**

Event ID	Event Description	Comments
Audit.SMC.connectreader	Connecting reader {0}	The controller is connecting to the smart card reader that the controller user selects in the <b>Smartcard selection</b> menu. {0} is replaced with the card reader name.
Audit.SMC.connectreader.failed	Unable to mount reader {0}.	An error is reported during the initialization of the virtual driver.
Audit.SMC.disconnectreader.1	System disconnecting reader {0}	The controller user unplugs the physical card reader from their system.{0} is replaced with the card reader name.
Audit.SMC.disconnectreader.2	Disconnecting reader {0}	The controller user selects a connected reader in the <b>Smartcard selection</b> menu to disconnect it. {0} is replaced with the card reader name.
Audit.SMC.cardinserted	Card present in reader {0}	The controller user inserts a card into the smart card reader. {0} is replaced with the card reader name.
Audit.SMC.cardremoved	Card not present in the reader {0}	The controller user removes a card from the smart card reader. {0} is replaced with the card reader name.

## Target smart card audit events

**Table 13. Target smart card audit events**

Event ID	Event Description	Comments
ibm.trc.audit.00C0	Virtual smart card device connected	The target connects to the virtual smart card reader.
ibm.trc.audit.00C1	Virtual smart card device failed to connect	The target cannot connect to the virtual smart card reader.
ibm.trc.audit.00C2	Virtual smart card device disconnected	The target is disconnected from the virtual smart card reader. Reported when the controller user selects a connected reader in the <b>Smartcard selection</b> menu to disconnect it.
ibm.trc.audit.00C3	Virtual smart card device failed to disconnect	The target fails to disconnect from the virtual smart card reader.



**Table 13. Target smart card audit events (continued)**

Event ID	Event Description	Comments
ibm.trc.audit.00C4	Virtual smart card device disconnected due to an error	The target is disconnected from the virtual smart card reader because an unexpected error occurred.

## Chapter 8. Ensuring that current data is reported

Whenever a report is generated in BigFix® Remote Control Server a query is run against the database to retrieve the required data and display it on the screen. This data is held in a temporary location for the next time the same report is run so that the data is displayed more quickly on the screen. To ensure that the latest data is reported to the screen, including any updates that have taken place since the last time the report data was displayed, click **Refresh** at the right of the screen. The report data is updated with the changes or updates and displayed on the screen.

For example, if you create a new user and do not see the user's details in the **All Users** report, click **Refresh** to update the report with the new entry.

# Appendix A. Error messages

In most of cases, connectivity problems that are experienced in Remote Control are related to the surrounding network infrastructure. Error messages in Remote Control help to pin point these problems.

The following list of error messages might be displayed to the controller user.

Unable to connect to <IP> because of timeout:

An example of this error is that the controller cannot establish basic connectivity to the target or there was an error with the connection before it was accepted or refused.

The target has refused the session:

Example of this error is that either the server does not validate the session attempt, or the target user refuses the session request, when user acceptance policies are enabled.

Session rejected because the pre-session script was not found:

Examples of this error are that the **Run pre-session script policy** is set but the script cannot be found or the pre-script times out, and the pre/post-script fail operation is set to **abort**.

Session rejected because the post-session script was not found:

Examples of this error are that the **Run post-session script policy** is set but the script cannot be found or the post-script times out, and the pre/post-script fail operation is set to **abort**.

Session rejected because the pre-session script failed with error code: <X>:

This error is similar to the Session rejected because the pre-session script was not found error. However, in this error message if the pre-script fails, the error code that the script returned is also displayed.

Session rejected because the limit of allowed clients has been reached:

This error message is used specifically when you join a collaboration session and the number of participants already in the session reaches the limit of allowed controllers.

Session rejected because the provided credentials are invalid:

This error message is used when an invalid user name and password are entered when you start a Peer to Peer session.

The file transfer was rejected. The current configuration requires a logged on user on the target :

This error message is displayed when establishing a peer to peer file transfer session and there is no logged on user on the target.

```
Session rejected because the provided credentials have expired:
```

When the Windows™ operating system user ID and password are required to start a peer to peer session, this error message is displayed if the ID or password expires.

```
Session rejected because it is out of the allowed times:
```

This error message is used when the session is not started within the allowed times.

```
Session rejected because there is no user logged to confirm the session:
```

This error message is used when the **connect at logon** policy is set to Yes but there is no user logged on at the target who can accept the session.

```
The target might be busy with another session or listening on a different port. Error in the session handshake with target at {0}.
```

This error message is displayed when the controller can establish a network connection but it is unable to exchange Remote Control data. This issue usually happens because there is already an active remote control session on that target or a service other than the Remote Control target is listening on that port. The IP address of the target is substituted for the {0}.

```
Error initializing the local FIPS certified cryptographic provider. The session to {0} cannot be established.:
```

This error message is used when FIPS compliance is not set up on the controller correctly. The controller is not running on a FIPS capable Java™ Runtime Environment. The IP address of the target is substituted for the {0}.

```
The target does not support FIPS certified encryption. The session to {0} cannot be established.:
```

This error message is used when FIPS compliance is not supported on the target. The session to {0} cannot be established. The IP address of the target is substituted for the {0}.

```
Session rejected because of acceptance timeout:
```

This error message is used when the session is not accepted by the target user in the time that is specified by the **acceptance grace time** policy and the **acceptance timeout action** is also set to **abort**.

```
The network connection to {0} timed out:
```

This error message is used when the network connection attempt fails with a time-out. Usually this issue occurs when the connection is stopped by a firewall that is configured to not give any kind of response to the connection attempts it rejects. The IP address of the target is substituted for the {0}.

```
The network connection to {0} was refused:
```

This error message is used when the network connection attempt fails because it was rejected. Usually this issue happens when the host is not listening for connections on the port or a firewall is intercepting the connection and is configured to explicitly reject the connections to that port.



**Note:** This issue is not related to an Remote Control Session refusal, which happens after the basic network connection is established.

```
Unable to resolve the address for host {0}:
```

This error message is used when a host name is provided in the connection details and it cannot be resolved to an IP address.

```
Failed to connect to {0}:
```

This error message is a generic connection failure message. It is only displayed if the code cannot figure out why the connection failed so it cannot display any more information than this generic failure message.

```
Unable to listen for incoming connections:
```

This error is displayed if the controller is unable to start listening for connections from other controllers in collaboration mode.

## Appendix B. Session resilience for sessions that are connected by using a broker

During a remote control session that is connected by using a broker, when connection failure is detected, reconnection to the session is attempted automatically. The controller user and target user are informed of what is happening with the session connection through various message windows.

The messages that are displayed to the users depend on which participant loses connection to the session.

### The controller disconnects from the session

If the controller loses connection to the session, it cannot communicate with the broker. For example, due to a network issue. The following message is displayed on the controller computer.

```
Please wait, trying to re-establish your session
```

```
Lost connection to the broker, attempting connection recovery.
```

The connection attempt is tried every 30 seconds until the controller reconnects. During this time, you can click **Cancel session reconnection** to end the session. If the controller does not connect after 10 minutes, the connection attempt ends.

During the reconnection attempt, the following session suspended message is displayed on the target computer while the controller tries to reconnect to the broker. The target user can click **End session**.

```
The session is temporarily suspended because the connection from the controller is lost.
```

```
Please wait while the controller tries to reconnect.
```

When the controller reconnects to the broker, a connecting message is displayed on the controller. If user acceptance is enabled for the session, a user acceptance message is displayed on the target. The target user must accept or refuse the session. However, if the target loses connection to the broker when the controller reconnects, the following message is displayed on the controller.

```
Please wait, trying to re-establish your session
```

```
Reconnected to the broker, trying to reconnect to the end-point.
```

The connection attempt is tried every 30 seconds until the target reconnects. The session ends if the target does not reconnect after 10 minutes.

### The target disconnects from the session

If the target loses connection with the broker, the following message is displayed on the controller computer.

```
Please wait, trying to re-establish your session
```

```
Lost connection to an endpoint, connection through the broker is still active.
```

```
Attempting connection recovery.
```

A session suspended message is displayed on the target computer while the target tries to reconnect to the broker. The connection attempt is tried every 30 seconds until the target reconnects. If user acceptance is enabled for the session, a user acceptance message is displayed on the target when the target reconnects. The target user must accept or refuse the session. While the target is trying to reconnect, the controller can click **Cancel session reconnection** to end the session. A quit session message is displayed. The controller user can click **Yes** to quit the session. However, because the target is still trying to connect to the broker, if it does reconnect now, the following message is displayed on the target.

```
Unable to re-establish the connection because the session has ended.
```

```
Try again with a new connection code?
```

The target user can click **OK** to start a new session or **Cancel** to quit.

### Sessions with multiple participants

During remote control sessions that have multiple participants, if the master controller user loses connection to the broker, the following message is displayed. The message is displayed on the master controller.

```
Please wait, trying to re-establish your session
```

```
Lost connection to the broker, attempting session recovery.
```

At the same time, the following message is displayed to all other participants that are in the session.

```
Please wait, trying to re-establish your session
```

```
Lost connection to an endpoint, connection through the broker is still active.
```

```
Attempting session recovery.
```

If the controller does not reconnect within 3 minutes, and the automatic handover policy is enabled, session control automatically passes to another controller. However, if user acceptance is enabled, the target user must accept or refuse the new master controller. If the old master controller does reconnect, they can join the session if the new master controller accepts the request to join. They rejoin the session as a participant and are no longer the master controller.

## Appendix C. Smart card status messages

The following status messages can be displayed on the controller during a remote control session in which smart card authentication is enabled. A **Hide** button is displayed on some of the message windows. Click **Hide** to minimize the message window and continue in the session.

**Table 14. Controller smart card status messages**

Status message	Comments
<i>Initializing controller smart card subsystem</i>	Displayed at the start of the session. The controller queries, which smart cards are present.
<i>Creating Virtual card and connecting</i>	Displayed when the controller user selects a card reader. The target is now trying to create a virtual card reader and then connect to the controller physical card reader.
<i>Getting list of attached smart card readers</i>	Displayed when the controller user selects <b>Refresh card list</b> in the <b>Smart card selection</b> menu.
<i>Disconnecting Virtual smart card</i>	Displayed when the controller user selects an already selected card reader to disconnect it.
<i>Error creating remote virtual driver. Please check the target log</i>	Displayed if an error is returned when the target tries to create the virtual reader.
<i>Resetting the smart card subsystem</i>	Displayed at the end of the session when you disconnect.



## Appendix D. Keyboard shortcuts for the BigFix® Remote Control Target for macOS

During a remote control session with a BigFix® Remote Control Target for macOS, you can inject the following keyboard shortcuts. The shortcuts are displayed in the **Perform Action in Target** menu in the controller UI.

**Table 15. Keyboard shortcuts that can be used on the BigFix® Remote Control Target for macOS**

Controller menu display name ( macOS)	Controller menu display name ( Windows™ controller)	Function
Inject ⌘ Q	Inject Command + Q	Quit the selected application.
Inject ⇧ ⌘ ⌫	Inject Option + Command + Escape	Force quit an application. The Force quit menu opens
Inject ⌘ ⌵	Inject Command + Space	Show or hide the Spotlight search field.
Inject ⌘ ⇧ →	Inject Command + Tab	To switch between active applications on the target.
Inject ⌘ `	Inject Command + Grave	Switch to the last used window of the active application.

# Appendix E. 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

## A

- access request
  - registered user18
- access requests
  - creating18
  - viewing20
- active session
  - changing to55
- auditing
  - improvements
    - session acceptance117
    - session rejection118
  - smartcard119
- auto scrolling
  - disabling89
  - enabling89

## B

- balanced89
- best performance89
- broker session70
  - collaboration70, 70
  - starting48

## C

- changing your password21
- chat session

- changing to56
- clipboard menu
  - receiving text87
  - sending text87
- collaboration
  - broker session
    - join from server72
    - join using URL73
  - joining72
  - connection URL73
  - starting70
- collaboration session
  - acceptance prompt
    - hiding115
- audit events77
- broker70
  - handing over73
- controlling74
- disconnecting participants74
- ending76, 76
- giving control74
- limiting participants74
- peer to peer

- 66
  - handing over
    - 69
  - joining
    - 68, 69
  - starting
    - 66
- requesting control
  - 75
- returning control
  - 75
- revoking control
  - 74
- server initiated
  - handing over
    - 65
  - joining
    - 64
  - starting
    - 63
- using the server UI
  - 62
- command line software
  - downloading
    - Linux
      - 31
    - Windows
      - 30
- command line tools
  - using
    - 97
  - wrc command
    - 98
  - wrcmdpcr command
    - 100
- command mode
  - shell mode
    - 43
- command session
  - changing to
    - 57
- configure controller
  - 91
- Configuring controller properties
  - 107
- Connecting to a target that is already in a session
  - 50
- controller
  - establishing sessions
    - 34
  - help
    - 95
- controller configuration
  - local
    - 91
- controller interface
  - 52
  - capture screen
    - 78
  - clipboard menu
    - 86
  - controller tools
    - 77
  - enable / disable autoscroll
    - 89
  - enable / disable scaled view
    - 89
  - enable / disable true colour
    - 91
  - open chat window
    - 61
  - perform action in target
    - 57
  - performance settings
    - 89
- controller properties
  - configuring
    - 107
  - enable.address.history
    - 113
  - enable.domain.history
    - 113
  - enable.user.history
    - 113



history.max.items	
113	
running tools on the target	
108	
send key sequences	
111	
controller software	
downloading	
Linux	
29	
Windows	
29	
<b>D</b>	
debug property	
controller	
95	
debug.trace	
95	
downloads	
agent download	
28	
download trc player	
28	
launch remote control player	
27	
drawing tool	
using	
41	
<b>E</b>	
ending a collaboration session when you disconnect	
76	
entering text on the target screen	
78	
error messages	
wrc command	
102	
execution of tools in target	
enabling and disabling	
remote session	
116	
exporting data	
26	
<b>F</b>	
favourite targets list	
creating	
13	
removing targets	
14	
viewing	
13	
file transfer	
display columns	
37	
hide columns	
37	
Open controller file transfer directory	
85	
Open target file transfer directory	
85	
synchronize columns	
37	
view transfer list	
85	
file transfer directory	
changing the location	
86	
file transfer menu	
open remote transfer folder	
85	
open transfer folder	
85	
receiving a file	
84	
sending a file	
84	
toggle show transfers	
85	
file transfer session	
creating directories	
38	
deleting files	
38	
show transferred file list	
39	

transferring directories

controller to target

36

target to controller

36

transferring files

controller to target

36

target to controller

36

files

changing the file transfer directory

86

receiving a file

84

sending a file

84

transferring

83

## G

grayscale

89

guidance session

changing to

56

clear instructions

43

drawing tool

41

guidance tool

40

highlight tool

42

mouse tool

42

tools

39

guidance tool

symbols and action

40

using

40

## H

Handing over a collaboration session involving a broker

73

help

95

Help

server

32

Help Menu

server

32

high quality color

disabling

89

enabling

89

highlight tool

using

42

homepage

resetting

25

setting

24

## J

Joining a broker collaboration session

72

Joining a collaboration session from the server

64

Joining a peer to peer collaboration session

68

Joining or Disconnecting a session

50

## K

keyboard shortcuts

mac target

129

## L

local input

disabling

57

- enabling
    - 57
- local recording
  - making
    - 82
  - playing
    - 82
- logging off
  - 11
- logging on
  - forgotten password
    - 10
- logging on to the server
  - 10
- M**
  - master controller
    - acceptance prompt
      - hiding
        - 115
  - messages
    - smartcard
      - 128
  - monitor session
    - changing to
      - 56
  - mouse tool
    - enabling
      - 42
  - multiple screens
    - viewing
      - 88
- N**
  - network response indicator
    - 88
  - num icon
    - 57
- O**
  - options menu
    - exporting data
      - 26
    - output
      - 26
  - refresh results
    - 25
  - reset to default homepage report
    - 25
  - set current report as homepage
    - 24
  - Overview
    - 8
- P**
  - P2P session
    - disconnecting
      - 50
    - joining
      - 50
    - password
      - changing
        - 21
      - forgotten password
        - 10
    - peer to peer session
      - starting
        - 46
  - Q**
    - quick text input
      - enabling
        - 78
  - R**
    - recordings
      - starting the session player
        - 27
    - registry keys
      - looking up values
        - 57
      - viewing
        - 57
    - remote control session
      - collaboration session
        - 62
      - ending
        - 96
      - initiating
        - 33

- inviting multiple participants
  - 62
- managed
  - 33, 45
- peer to peer
  - 33
- recording
  - 80
- remote control session
  - broker
    - 33
- starting
  - 16, 45
- remote control sessions
  - active session
    - 34
  - chat session
    - 35
  - command session mode
    - 43
  - establishing
    - 34
  - file transfer
    - 36
  - guidance session
    - 39
  - reboot
    - 43
  - types of
    - 34
- reports
  - custom
    - running
      - 24
  - standard
    - running
      - 23
- Reports Menu
  - 23
- Retaining previously used logon credentials for a P2P session
  - 113
- running tools on the target
  - 108
- S**
  - scaled view
    - disabling
      - 89
    - enabling
      - 89
  - screen data
    - refreshing
      - 25
  - select screens
    - 88
  - Sending key sequences to the target during a session
    - 111
  - server interface
    - accessing
      - 10
  - Server Web Interface
    - logging off
      - 11
    - logging on
      - 10
    - options menu
      - 24
    - reports menu
      - 23
    - sessions menu
      - 21
    - targets menu
      - 11
    - tools menu
      - 27
    - Users Menu
      - 20
  - session
    - reconnection
      - 126
  - session details
    - playing a recording
      - 22, 23
    - viewing

- 22
- session history
  - viewing
    - 14, 21
- session player
  - downloading
    - 28
  - launching
    - 27
- session recording
  - 80
    - exporting and downloading
      - 80
- session resilience
  - 126
- session response
  - indicator
    - 88
- session type
  - changing
    - 55
- session types
  - active
    - 34
  - chat
    - 35
  - guidance
    - 39
- sessions
  - searching
    - 22
- sessions menu
  - my session history
    - 21
  - search
    - 22
  - session details
    - 22
- Sessions Menu
  - 21
- smart card
  - controller option

- 87
  - select smart card reader
    - 87
- smart card reader
  - selection
    - 87
- starting
  - 70
- starting a broker session
  - 48
- status messages
  - smartcard
    - 128
- system information
  - retrieving
    - 61
- T**
  - target menu
    - add to favourites
      - 13
  - target numlock led
    - setting the state
      - 57
  - target policies
    - viewing
      - 15
  - target software
    - downloading
      - Linux
        - 28
      - Windows
        - 28
  - target status
    - viewing
      - 15
  - targets
    - browsing for
      - 12
    - capturing the screen
      - 78
    - getting system information
      - 61

- rebooting
  - 43
- requesting temporary access
  - anonymous user
    - 19
  - at start of session
    - 19
  - request access
    - 18
- searching
  - 12
- view access requests
  - 20
- viewing
  - 12
- targets menu
  - 11
  - all targets
    - 12
  - browse targets
    - 12
  - join broker session
    - 11
  - recently accessed
    - 14
  - remove from favourites
    - 14
  - request access
    - 17
  - search
    - 12
  - session history
    - 14
  - start broker session
    - 11
  - Start Session
    - 16
  - target status
    - 15
  - view effective policies
    - 15
  - view favourites

- 13
- temporary access to a target
  - requesting
    - 17
- tools menu
  - downloads
    - 27
- transferring directories from controller to target
  - 36
- transferring directories from target to controller
  - 36
- transferring files
  - 36
- transferring files from controller to target
  - 36
- transferring files from target to controller
  - 36
- troubleshooting
  - auditing
    - 117
  - viewing current data
    - 122
- Troubleshooting Appendix
  - Error messages
    - 123
- true colour
  - disabling
    - 91
  - enabling
    - 91
- U**
  - user details
    - viewing
      - 20
  - users groups
    - viewing
      - 21
  - users menu
    - my details
      - 20
    - my groups
      - 21

Users Menu

20

Using

Remote Control

as a controller user

52

Using remote control commands from the command

line

97

## **W**

wrc

examples

100

wrc command

error messages

102

using

98

wrcmdpcr

examples

101

wrcmdpcr command

using

100