Remote Control Console User's Guide

Special notice

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

Edition notice

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

Contents

Chapter 1. Overview of the Remote Control system....6

Chapter 2. Definition of terms that are used in Remote Control....8

Chapter 3. The Remote Control console.... 9

Components....9

Chapter 4. Dashboards overview....12

View deployment distribution data....13

Chapter 5. Functions within Remote Control 16

Deploy remote control components....16

Deploy the components on a Windows® system....17

Deploy the components on a Linux™ system.... 28

Deploy the components on a macOS system....39

Update the remote control components....44

Update the components on a Windows™ system....44

Update the Linux® components.... 48

Download the remote control server component....53

Downloading the Windows server installer file.... 53

Downloading the Linux server installer file.... 54

Start a remote control session.... 54

Start a peer-to-peer session.... 54

Start a remote control session from the server.... 57

Respond to warnings 57

Manage target and server configurations....57

Creating server installation tasks....58

Creating target configuration tasks.... 71

Run remote control tasks.... 93

Analyses.... 94

Retrieving target installation and security data.... 94

Retrieving audit events data.... 95

Retrieve user, session, and performance data....95

Retrieve session connection data.... 95

Retrieve session activity data....96

Enable smart card authentication....96

Determining whether smart card support is enabled....96

Installing the driver and certificate by using a Fixlet 97

Removing the driver and certificate by using a Fixlet 97

Installing the certificates by using a Fixlet....98

Downloading the certificates 98

Configure single sign-on (SSO) on the server....99

Configuring the server for single sign-on during installation.... 99

Configuring the server for single sign-on after installation....100

Enable secure target registration....103

Distributing a secure registration token to targets 105

Chapter 6. Viewing web reports.... 107

Appendix A. Frequently asked questions....108

Appendix B. Support.... 110

Notices.... cxi

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. Definition of terms that are used in Remote Control

Definitions of some common terms that are used in Remote Control.

Remote control session

Establishing 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. For more information about remote control sessions, see the *BigFix® Remote Control Controller User's Guide*.

Peer-to-peer session

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 are set on the target are used for the session. For more information, see Manage target and server configurations *(on page 57)*. For more information about using the controller UI during a session, see the *BigFix® Remote Control Controller User's Guide*.

Managed remote control session

A remote control session in which the controller user initiates 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 about 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.

Session policies

Session policies define the actions that can be carried out by the controller user and the features available on the target system during a remote control session. In a peer to peer session the policies are determined by the local properties that are defined on the target. In a managed session, the policies and permissions that are resolved from user and target group relationships determine what actions can be carried out. For more information about how policies and permissions are derived for a managed remote control session, see the *BigFix® Remote Control Administrator's Guide*.

Chapter 3. The Remote Control console

Remote Control encompasses a host of features that provide the components that are required for remote takeover and monitoring of workstations and servers in your deployment.

The navigation tree in the BigFix® console, which is available for all BigFix® products, serves as your central command for all Remote Control functions. The navigation tree gives you easy access to all reports, wizards, Fixlet messages, analyses, and tasks that are related to controlling and managing the target systems in your network.

Components

The BigFix® Console organizes content into four parts:

Domain pane

Includes navigation tree and list of all domains.

Navigation Tree

Includes list of nodes and subnodes that contain site content.

List pane

Contains listing of tasks and Fixlets.

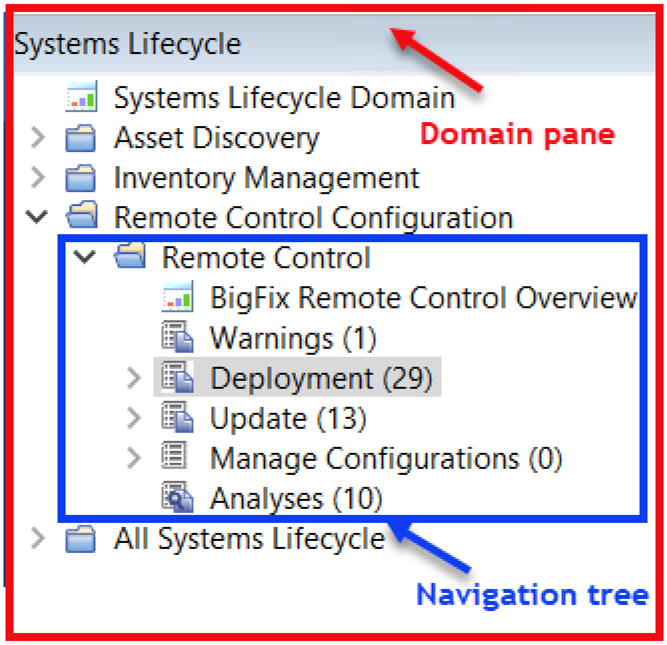
Work Area

Work pane where Fixlet and dialogs display.

In the context of the BigFix® Console, products or sites are grouped by categories or domains. For example, Remote Control is one of the sites that are contained within the Systems Lifecycle domain.

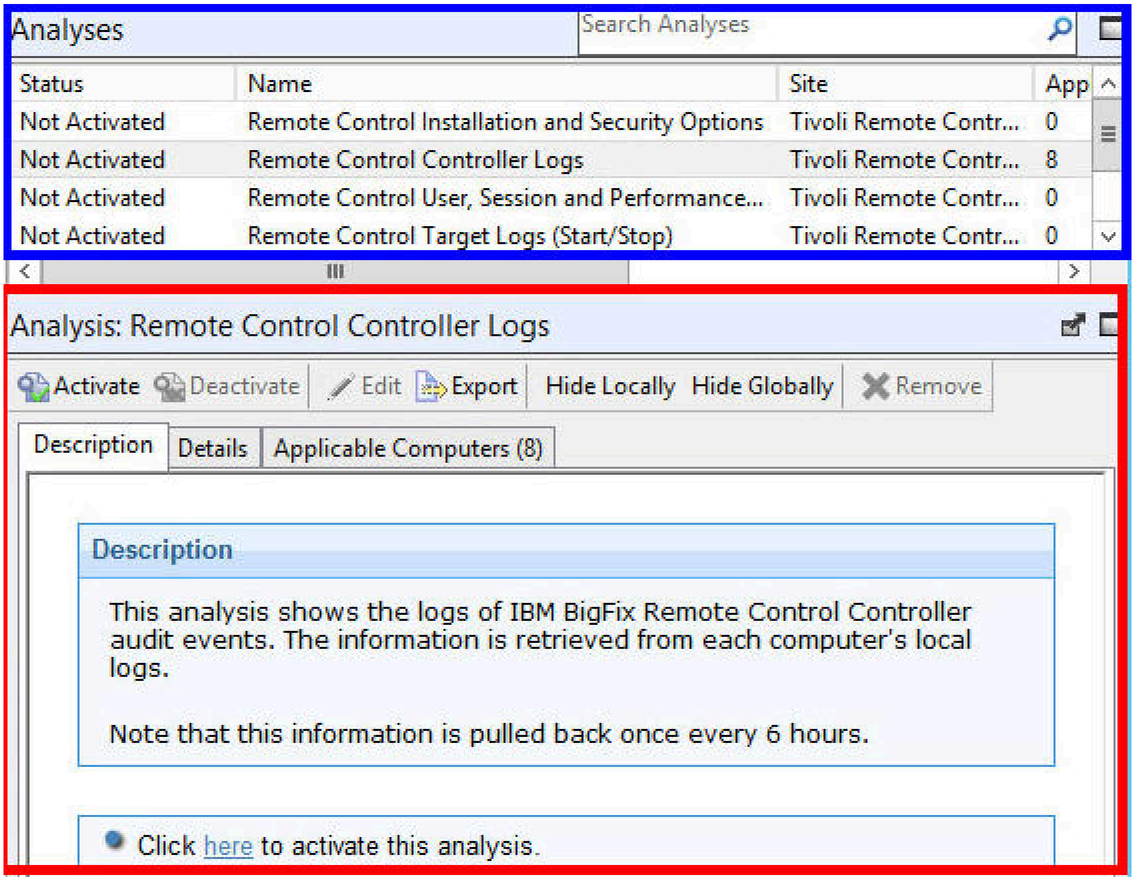
The Domain pane is the area on the left side of the Console that includes a navigation tree and a list of all domains. The Navigation Tree includes a list of nodes and subnodes that contain site content.

Click the Systems Lifecycle domain to see a list of sites that are associated with that domain.



The red outer area represents the entire Domain pane, including the navigation tree and list of domains. The blue inner area contains just the Navigation Tree for the Remote Control site.

Remote Control tasks are sorted by using upper and lower task panes, that are on the right side of the Console.



Status	Name	Site	App
Not Activated	Remote Control Installation and Security Options	Tivoli Remote Contr...	0
Not Activated	Remote Control Controller Logs	Tivoli Remote Contr...	8
Not Activated	Remote Control User, Session and Performance...	Tivoli Remote Contr...	0
Not Activated	Remote Control Target Logs (Start/Stop)	Tivoli Remote Contr...	0

Analysis: Remote Control Controller Logs

Description

This analysis shows the logs of IBM BigFix Remote Control Controller audit events. The information is retrieved from each computer's local logs.

Note that this information is pulled back once every 6 hours.

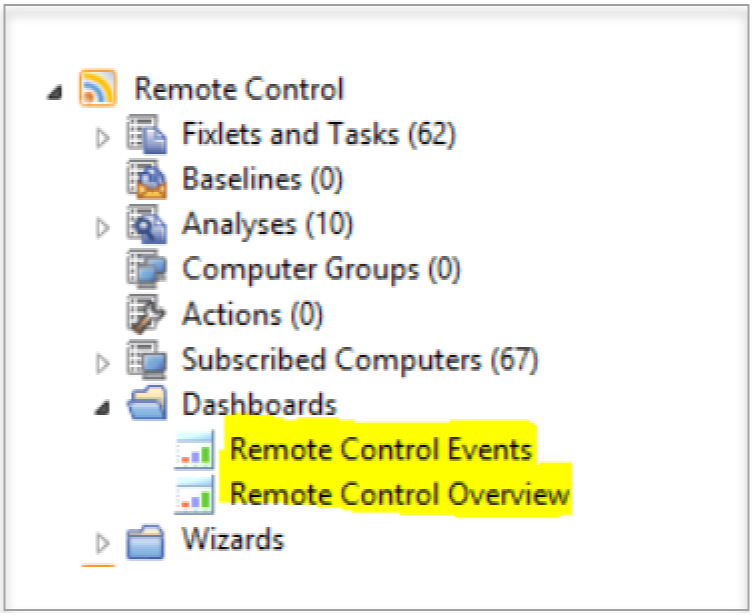
Click here to activate this analysis.

The upper pane, called the List pane, contains columns that sort data according to type, for example, Status, Name, Site, Applicable Computer Count. The lower pane or Work Area presents the Fixlet task pane from which you are directed to take specific actions to customize the content in your deployment.

Chapter 4. Dashboards overview

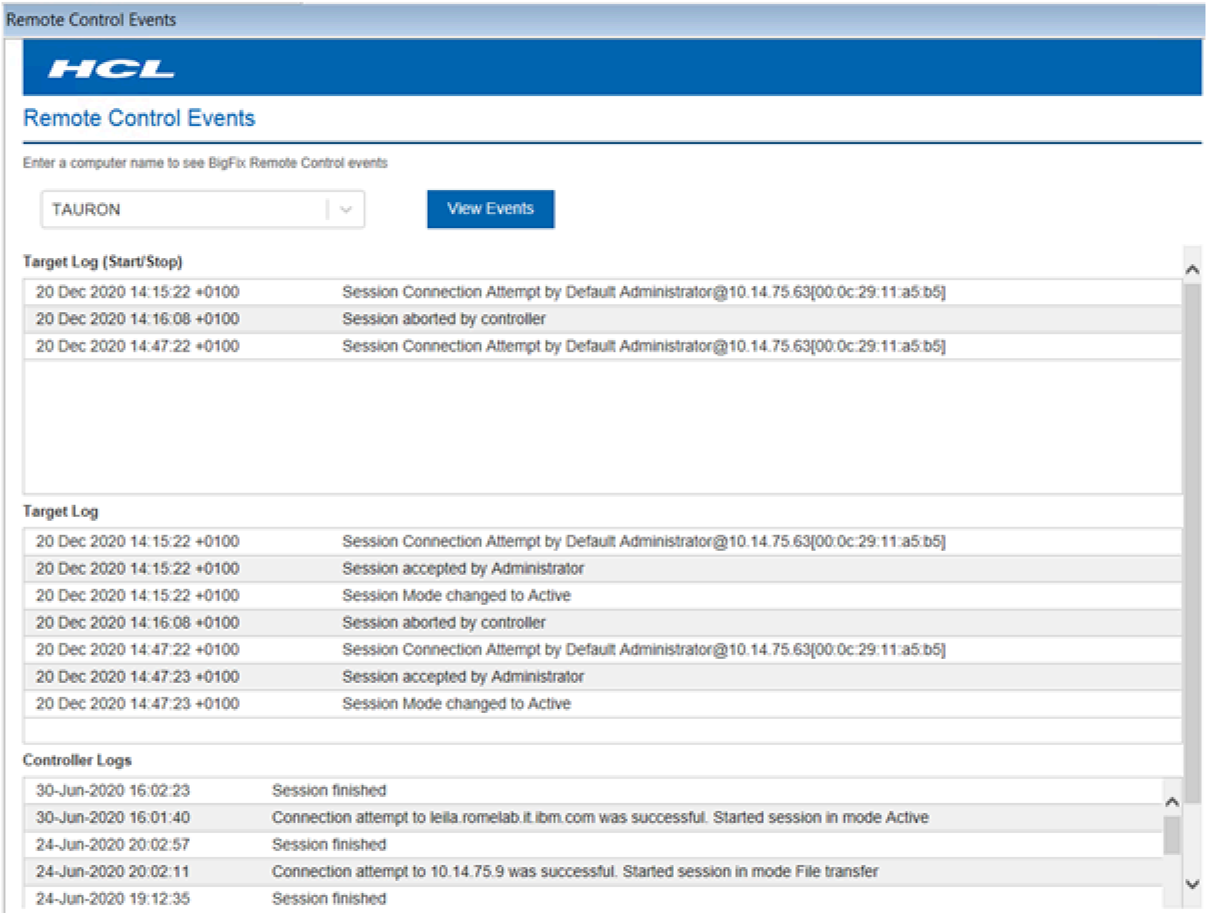
Remote Control offers a couple of convenient dashboards, the **Remote Control Events** for viewing log data gathered from the controller and target logs about the specified computer and the **Remote Control Overview** for viewing the deployment distribution of the Remote Control components in your environment and the distribution of the type of target deployment carried out.

You can access these dashboards from the top of the Remote Control navigation tree by selecting **Remote Control Events** or **Remote Control Overview:**



View Remote Control events

The **Remote Control Events** dashboard includes three separate sections that show log data gathered from the controller and target logs about the specified computer:



Remote Control Events

Enter a computer name to see BigFix Remote Control events

TAURON

Target Log (Start/Stop)

20 Dec 2020 14:15:22 +0100	Session Connection Attempt by Default Administrator@10.14.75.63[00:0c:29:11:a5:b5]
20 Dec 2020 14:16:08 +0100	Session aborted by controller
20 Dec 2020 14:47:22 +0100	Session Connection Attempt by Default Administrator@10.14.75.63[00:0c:29:11:a5:b5]

Target Log

20 Dec 2020 14:15:22 +0100	Session Connection Attempt by Default Administrator@10.14.75.63[00:0c:29:11:a5:b5]
20 Dec 2020 14:15:22 +0100	Session accepted by Administrator
20 Dec 2020 14:15:22 +0100	Session Mode changed to Active
20 Dec 2020 14:16:08 +0100	Session aborted by controller
20 Dec 2020 14:47:22 +0100	Session Connection Attempt by Default Administrator@10.14.75.63[00:0c:29:11:a5:b5]
20 Dec 2020 14:47:23 +0100	Session accepted by Administrator
20 Dec 2020 14:47:23 +0100	Session Mode changed to Active

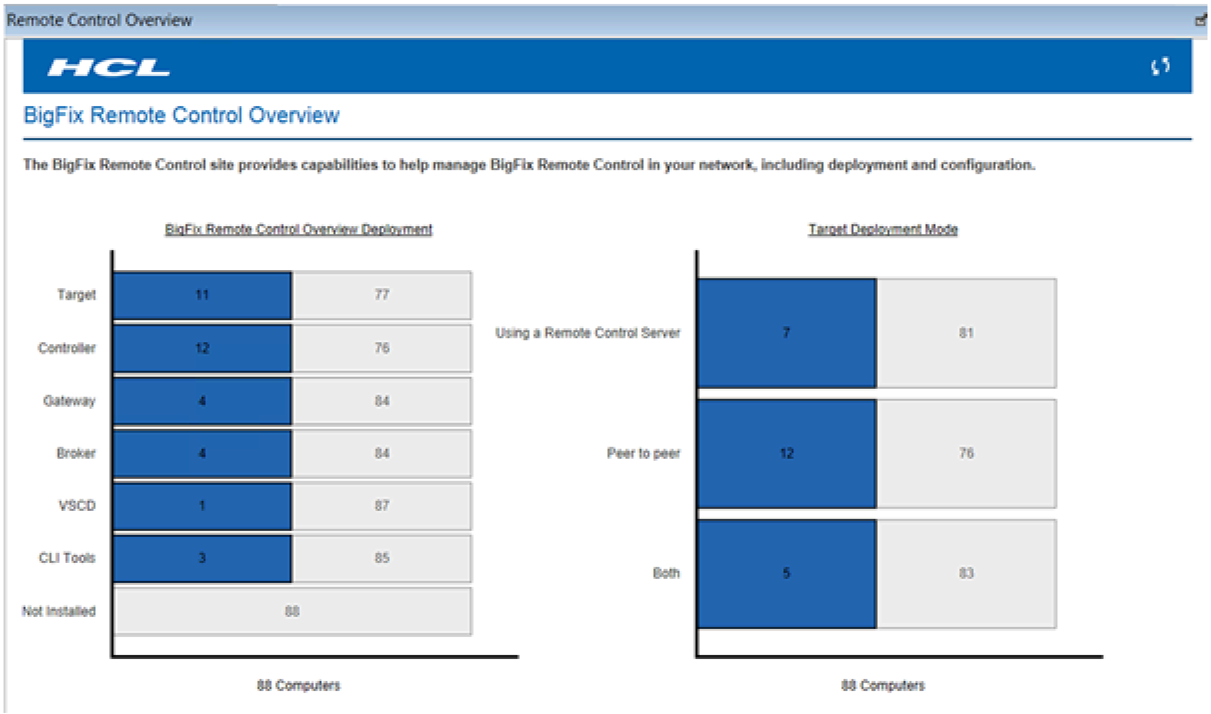
Controller Logs

30-Jun-2020 16:02:23	Session finished
30-Jun-2020 16:01:40	Connection attempt to leila.romelab.it.ibm.com was successful. Started session in mode Active
24-Jun-2020 20:02:57	Session finished
24-Jun-2020 20:02:11	Connection attempt to 10.14.75.9 was successful. Started session in mode File transfer
24-Jun-2020 19:12:35	Session finished

View deployment distribution data

The Remote Control Overview dashboard includes two separate sections that show the deployment distribution of Remote Control and the target deployment type distribution.

The **Remote Control Overview Deployment** section displays the number of computers in your environment that have the various Remote Control components installed.



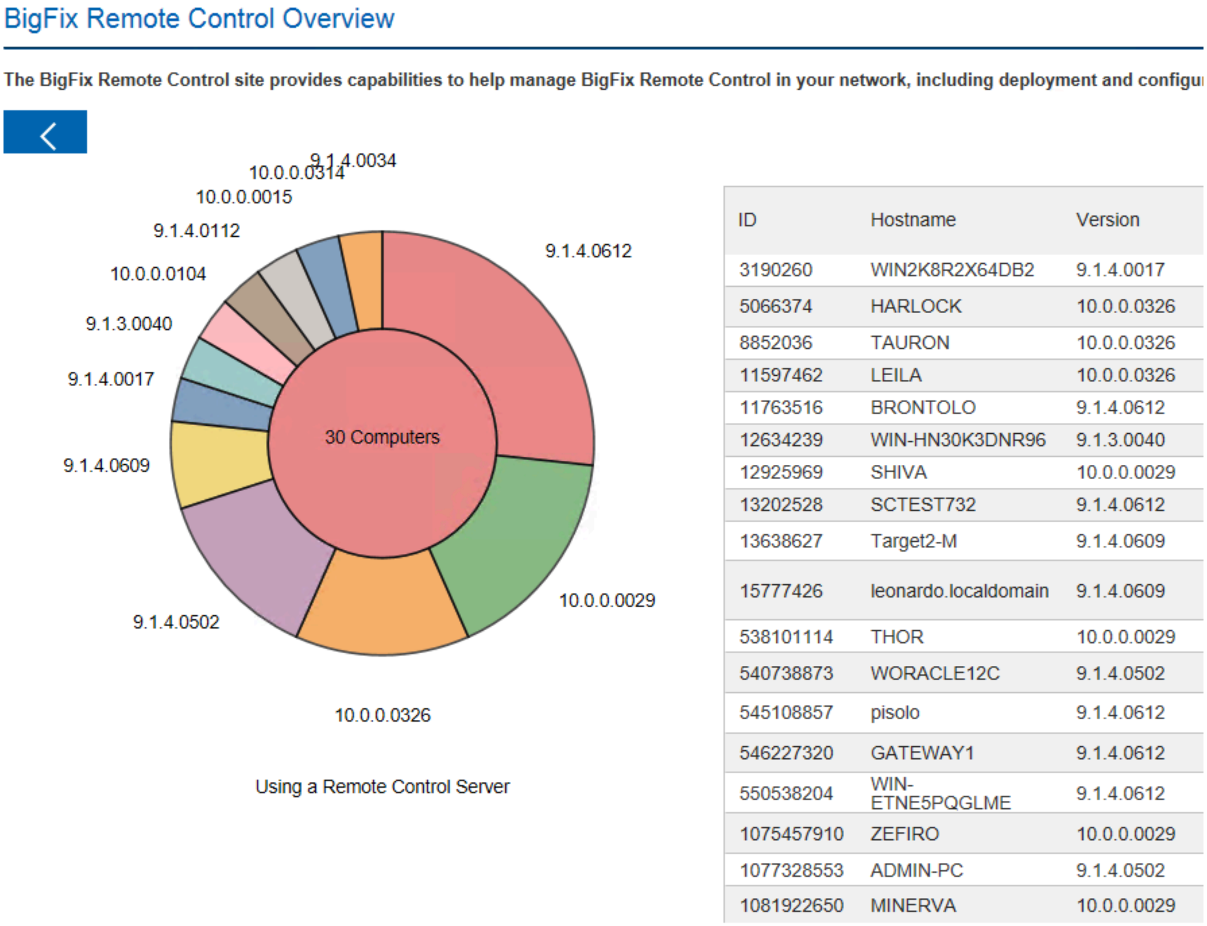
Remote Control Overview

BigFix Remote Control Overview

The BigFix Remote Control site provides capabilities to help manage BigFix Remote Control in your network, including deployment and configuration.

The **Target Deployment Mode** section shows the distribution of the type of target deployment that was carried out, on the computers in your environment. For more information about the different target deployment types, see Deploy the Remote Control components *(on page 16)*.

- To display the latest deployment distribution data, use the refresh icon
- To explore the results of the loaded statistics, click the blue bar. You can view more details such as version of the computer, version of the component installed.



BigFix Remote Control Overview

The BigFix Remote Control site provides capabilities to help manage BigFix Remote Control in your network, including deployment and configu

ID	Hostname	Version
3190260	WIN2K8R2X64DB2	9.1.4.0017
5066374	HARLOCK	10.0.0.0326
8852036	TAURON	10.0.0.0326
11597462	LEILA	10.0.0.0326
11763516	BRONTOLO	9.1.4.0612
12634239	WIN-HN30K3DNR96	9.1.3.0040
12925969	SHIVA	10.0.0.0029
13202528	SCTEST732	9.1.4.0612
13638627	Target2-M	9.1.4.0609
15777426	leonardo.localdomain	9.1.4.0609
538101114	THOR	10.0.0.0029
540738873	WORACLE12C	9.1.4.0502
545108857	pisolo	9.1.4.0612
546227320	GATEWAY1	9.1.4.0612
550538204	WIN-ETNE5PQGLME	9.1.4.0612
1075457910	ZEFIRO	10.0.0.0029
1077328553	ADMIN-PC	9.1.4.0502
1081922650	MINERVA	10.0.0.0029

- To further filter the component by version, click on the desired pie slice.
- To come back to the complete statistics, click the circle at the center of the graph.
- To come back to the main page, click the back button ‹.

Chapter 5. Functions within Remote Control

The Remote Control navigation tree provides a suite of Fixlets, tasks, and wizards. Use the functions to deploy, configure, and update the components that you need to run remote control sessions in your environment. You can also gather data from the components.

Deploy the Remote Control components

The **Deployment** node in the Remote Control navigation tree provides subnodes that are operating system specific. Within the subnodes, you can deploy the components that you need to establish a remote control session. You can also deploy utilities that you can use to connect to targets by using the command line. Select the node that is relevant to your operating system.

Note: The Remote Control components can also be deployed by using the installation files. For more information, see the *BigFix® Remote Control Installation Guide*.

Controller

The controller component must be deployed on the computers that initiate the remote control session when you do not have access to an Remote Control server.

Target

The target component must be deployed on the computers that are controlled during a remote control session. Remote Control offers two ways of deploying the target component. You can install the target for peer-to-peer sessions or for managed sessions. Both of these session types are explained in Definition of terms that are used in Remote Control *(on page 8)* and in more detail in the *BigFix® Remote Control Controller User's Guide*.

Note: The "Using the Remote Control server" method requires an Remote Control server to be installed in your environment.

CLI tools

The command line tools contain two utilities that you can run from the command line. Use the utilities to start a remote control session with a target or run commands on a target system without target user interaction. The tools can be useful if you want to connect to a target without accessing the Remote Control Server interface. You can also use them in scripts to run multiple commands in an automated fashion.

Note: To deploy the CLI tools, you must have the URL of an Remote Control server that you have access to.

Gateway

If you have targets, controllers, and servers on different networks that cannot directly contact each other you can install and configure gateway support. Use the gateway support, to configure your network to allow the connections to be established.

Broker

Deploy the broker component when you have targets that are outside of the enterprise network, on the internet. The broker component is used to make the connection between the controller and target in a remote control session through the internet.

Deploy the components on a Windows® system

The **Windows** deployment node provides a set of tasks that you can use to install or remove the following components in a Windows® operating system environment.

- Target and controller software
- CLI tools
- Gateway support
- Broker support

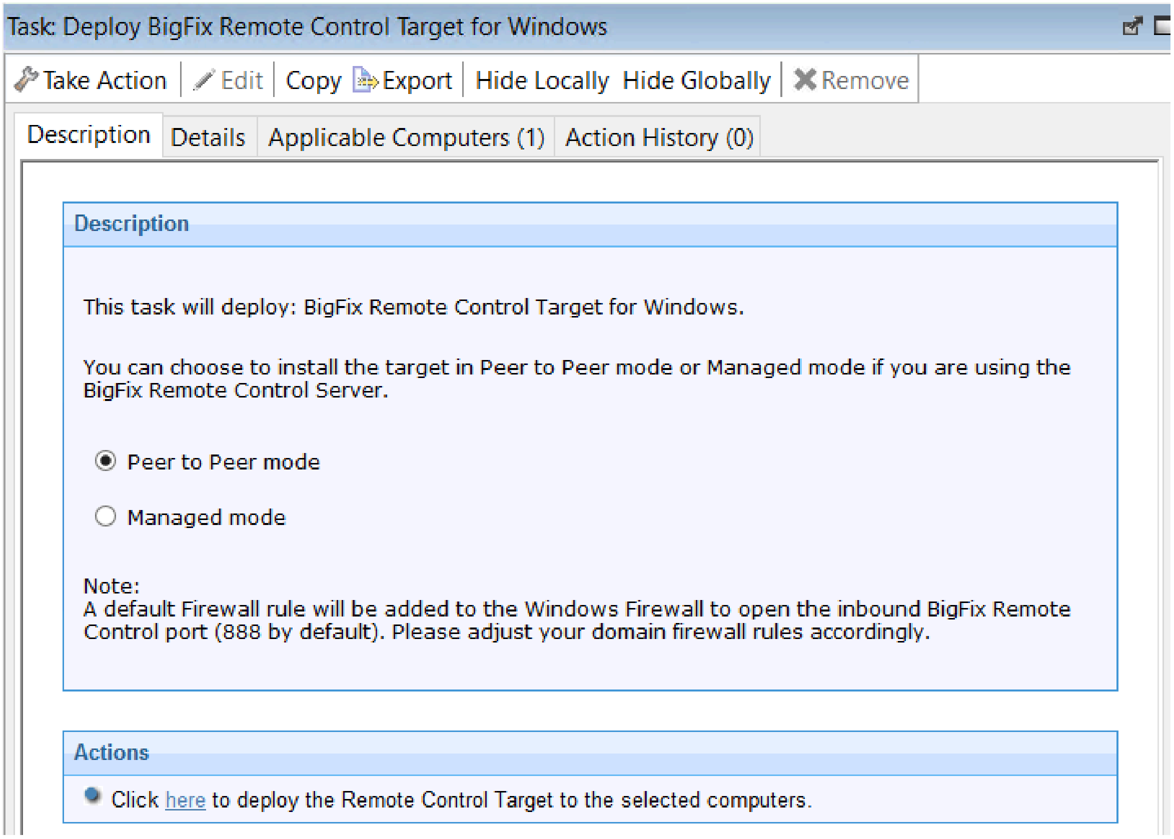
Deploying the Windows® target

Use the **Deploy Remote Control Target for Windows** task to install the target software on a Windows® computer.

To start this task, complete the following steps:

1. In the navigation tree, click **Deployment > Windows**.
2. Click **Deploy Remote Control Target for Windows**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.

   Determine your relevant installation method and follow the instructions that are given.



Description

This task will deploy: BigFix Remote Control Target for Windows.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

● Peer to Peer mode

○ Managed mode

Note:
A default Firewall rule will be added to the Windows Firewall to open the inbound BigFix Remote Control port (888 by default). Please adjust your domain firewall rules accordingly.

Actions

- Click here to deploy the Remote Control Target to the selected computers.

Peer to Peer mode

With this installation method, you can establish remote control sessions directly between the controller and the target without the need for an Remote Control server. This deployment method installs the target without requiring an Remote Control server URL to be specified. The local target policies set by this installation method are used when a remote control session is established. For more information about the target installation properties, see Manage target and server configurations *(on page 57)*.

In the Take Action pane on the Target tab, select the relevant option for determining the computers on which to deploy the Remote Control target.

Click **OK**.

The summary screen shows the progress of the task and displays status *complete* when it is finished.

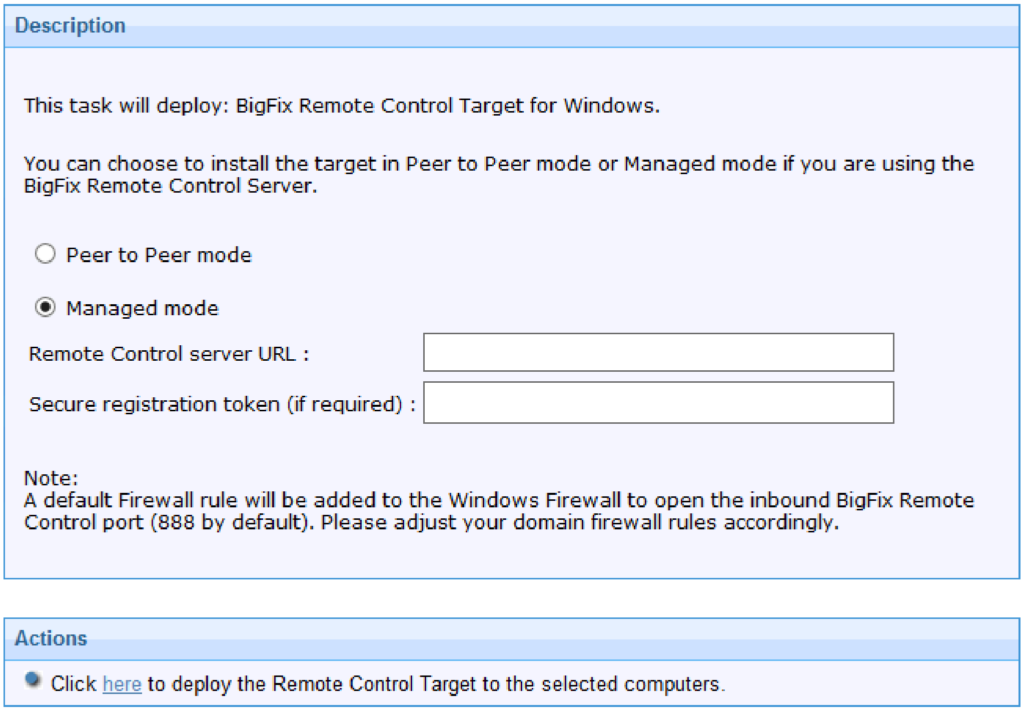
Note: For the target to register with the Remote Control server in the future, use the Remote Control Target wizard. Create a configuration task and specify the server URL of the relevant server. Run the task on the selected target to reconfigure it so that it can contact the server. For more information about target configuration tasks, see Creating Remote Control target configuration tasks *(on page 71)*. If the secure registration feature is enabled on the server you can distribute a secure registration token to the target. For more information, see Distributing a secure registration token to targets *(on page 105)*.

Managed mode

Choose this installation option for targets to register with the Remote Control server and take part in remote control sessions that are started from the server. This deployment method requires an Remote Control server URL to be specified. If a remote control session is requested with this target, the specified server is contacted to authenticate the request. When the request is authenticated, the policies for the session are passed from the remote control server to the target and the session is established. For more information about target installation properties, see Manage target and server configurations *(on page 57)*.

Enter the URL of your Remote Control server.

Enter a valid secure registration token if the secure target registration feature is enabled on the server.



Description

This task will deploy: BigFix Remote Control Target for Windows.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

○ Peer to Peer mode

● Managed mode

Remote Control server URL :

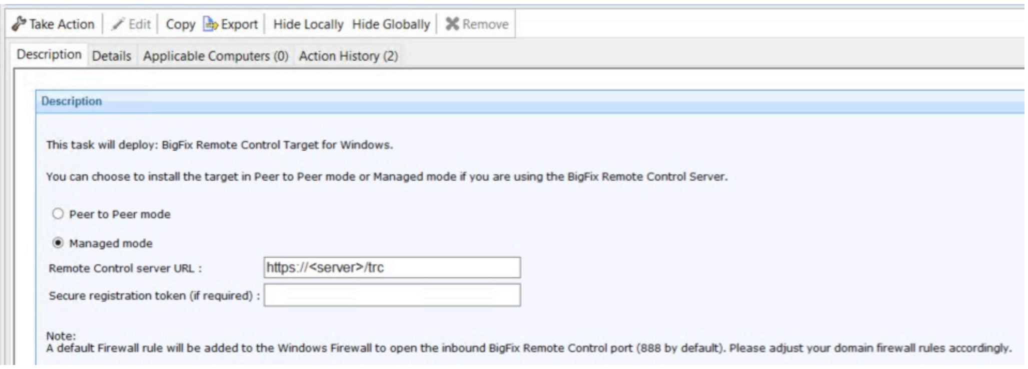
Secure registration token (if required) :

Note:
A default Firewall rule will be added to the Windows Firewall to open the inbound BigFix Remote Control port (888 by default). Please adjust your domain firewall rules accordingly.

Actions

- Click here to deploy the Remote Control Target to the selected computers.

Enter the URL of your Remote Control server and click **OK**.



Description

This task will deploy: BigFix Remote Control Target for Windows.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

○ Peer to Peer mode

● Managed mode

Remote Control server URL : https://<server>/trc

Secure registration token (if required) :

Note:
A default Firewall rule will be added to the Windows Firewall to open the inbound BigFix Remote Control port (888 by default). Please adjust your domain firewall rules accordingly.

In the Take Action pane on the Target tab, select the relevant option for determining the computers on which to deploy the Remote Control target.

Click **OK**.

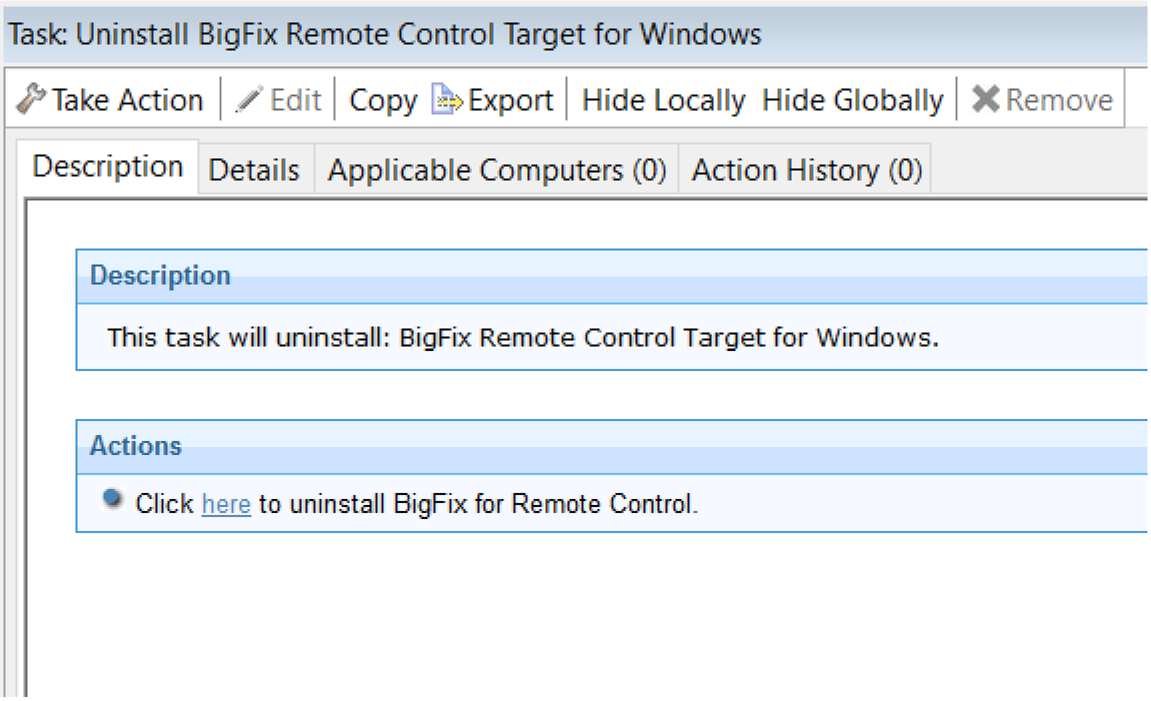
The summary screen shows the progress of the task and status *complete* when it is finished.

Removing the Windows® target

You can use the **Uninstall Remote Control Target for Windows** task to remove the target software from a Windows® computer that has the target software already installed.

To start the task, complete the following steps:

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Uninstall Remote Control target for Windows**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



This task will uninstall: BigFix Remote Control Target for Windows.

Click here to uninstall BigFix for Remote Control.

4. In the **Take Action** pane, on the Target tab, select the relevant option for determining which targets to remove the Remote Control target from.
5. Click **OK**.

The summary screen shows the progress of the task.

Note: After the removal of the target, some files might not be deleted automatically. The files are created as part of the installation of the target. These files are in `C:\ProgramData\BigFix\Remote Control\`.

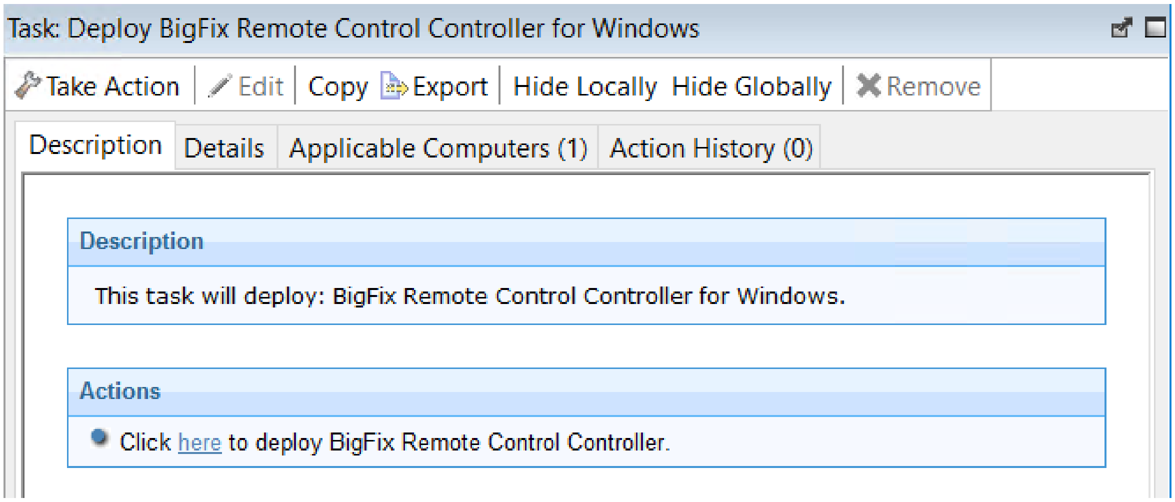
Deploying the Windows® controller

You can use the **Deploy Remote Control Controller for Windows** task to install the controller software onto a Windows® computer.

Note: To start a remote control session from the BigFix® console, deploy the controller to the same computer as the console is installed on. However, when the controller is deployed, only the current user who is logged on to the computer that you are deploying to has the rights to see the menu item to start a session. The menu item is not visible to other users.

To start this task, complete the following steps:

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Deploy Remote Control Controller for Windows**.
3. In the **Task pane**, review the description and follow the instructions in the **Actions** box to start the task.



Task: Deploy BigFix Remote Control Controller for Windows

Description

This task will deploy: BigFix Remote Control Controller for Windows.

Actions

- Click here to deploy BigFix Remote Control Controller.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the controller on.
5. Click **OK**.

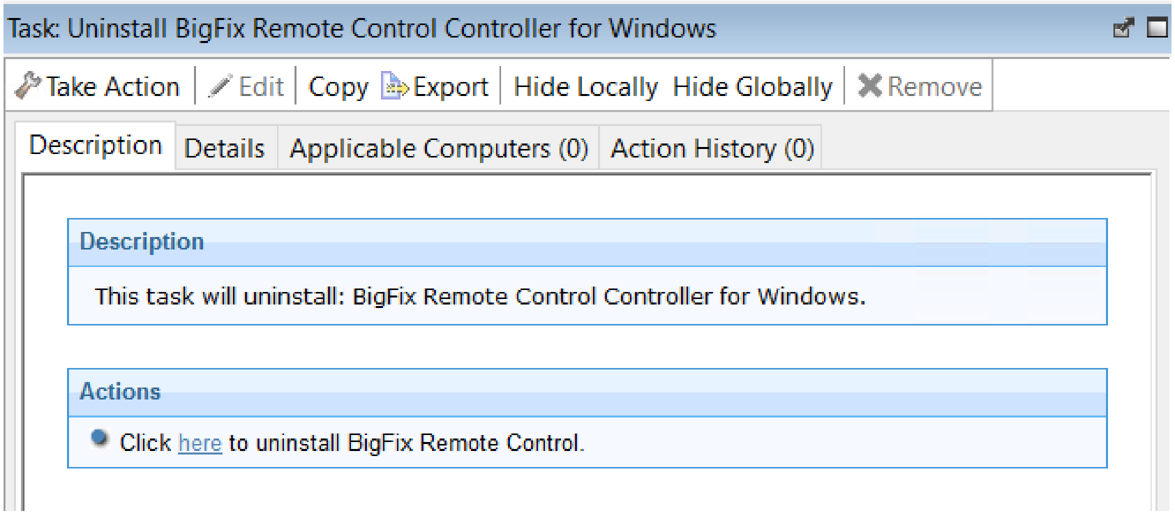
The summary screen shows the progress of the task.

Removing the Windows® controller

You can use the **Uninstall Remote Control Controller for Windows** task to remove the controller software from a Windows® computer that has the controller software already installed.

To start this task, complete the following steps:

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Uninstall Remote Control Controller for Windows**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Task: Uninstall BigFix Remote Control Controller for Windows

Description

This task will uninstall: BigFix Remote Control Controller for Windows.

Actions

- Click here to uninstall BigFix Remote Control.

4. In the Take Action pane, in the Target tab, select the relevant option for determining which targets to remove the Remote Control controller from.
5. Click **OK**.

The summary screen shows the progress of the task.

Deploying the Windows® CLI tools

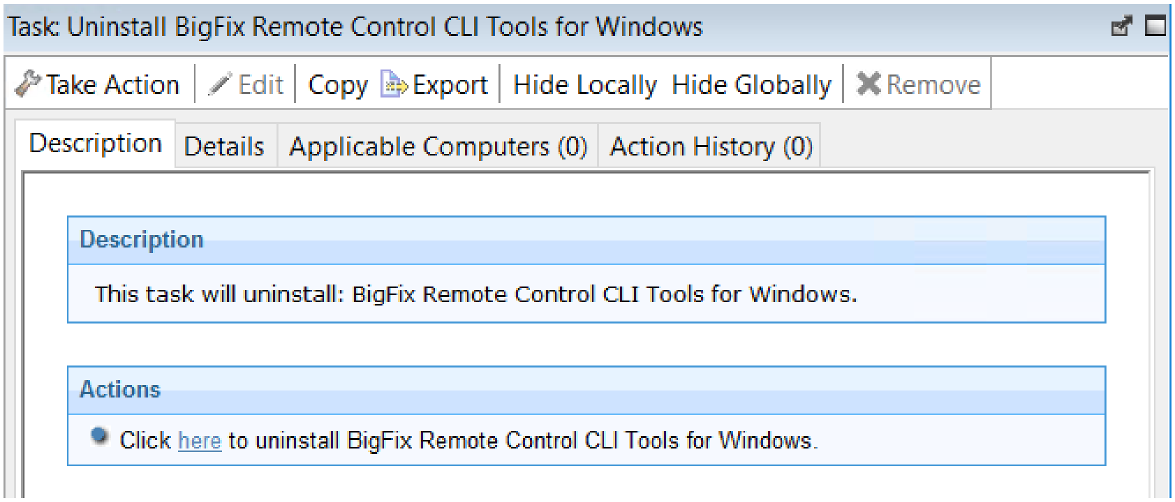
You can use the **Deploy Remote Control CLI Tools for Windows** task to install the CLI tools onto a Windows® computer. Use the CLI tools to start a session from the command line. You can also use the tools to run commands on the remote target.

To initiate this task, complete the following steps:

Note:

1. The CLI tools are also installed when you install the target software. Therefore, use the **Deploy Remote Control CLI Tools for Windows** Fixlet to deploy the CLI tools only on computers that do not have the target software installed.
2. To deploy this task, you need the URL for an Remote Control server that you have access to.

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Deploy Remote Control CLI Tools for Windows**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will uninstall: BigFix Remote Control CLI Tools for Windows.

Actions

- Click here to uninstall BigFix Remote Control CLI Tools for Windows.

4. Enter the URL of the Remote Control server and click **OK**.
5. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the CLI tools on.
6. Click **OK**.

The summary screen shows the progress of the task.

The two CLI utilities are installed in the `\Program Files\BigFix\Remote Control\Target` directory on the targets that you selected when you ran the deployment task.

`wrc.exe`

Use this tool to start a remote control session with a target.

`wrcmdpcr.exe`

Use this tool to run a command on a target. The output from the command is displayed on the computer that you ran the command from.

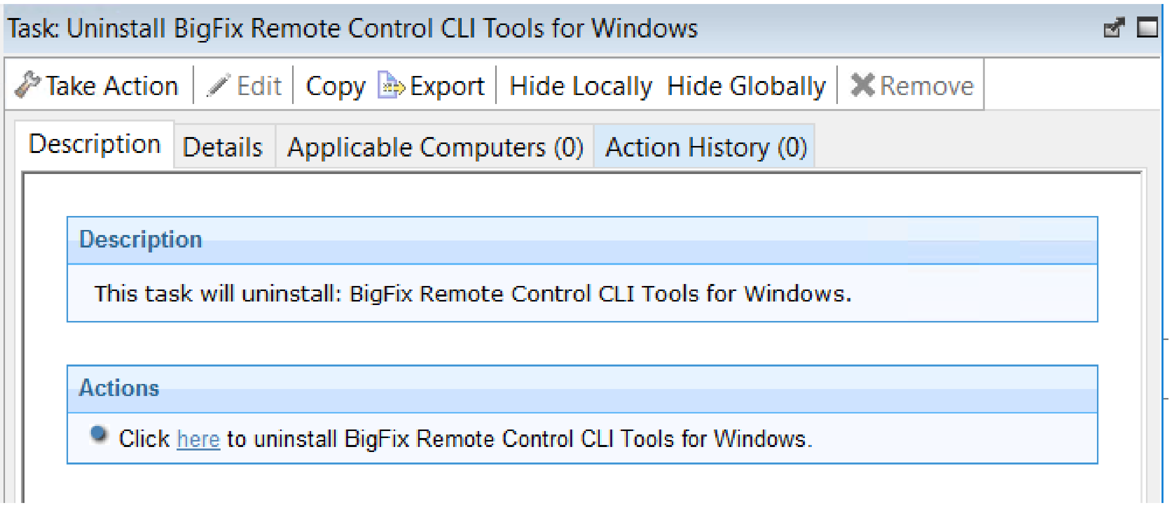
For more information about how to use the command line tools, see the *BigFix® Remote Control Controller User's Guide*.

Removing the Windows® CLI tools

You can use the **Uninstall Remote Control CLI Tools for Windows** task to remove the CLI tools from a Windows® computer that has the CLI tools already installed.

To start this task, complete the following steps:

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall Remote Control CLI Tools for Windows**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Task: Uninstall BigFix Remote Control CLI Tools for Windows

Description

This task will uninstall: BigFix Remote Control CLI Tools for Windows.

Actions

Click here to uninstall BigFix Remote Control CLI Tools for Windows.

4. In the Take Action pane, in the Target tab, select the relevant option for determining which targets to remove the CLI tools from.
5. Click **OK**.

The summary screen shows the progress of the task. The CLI tools are removed from the selected targets.

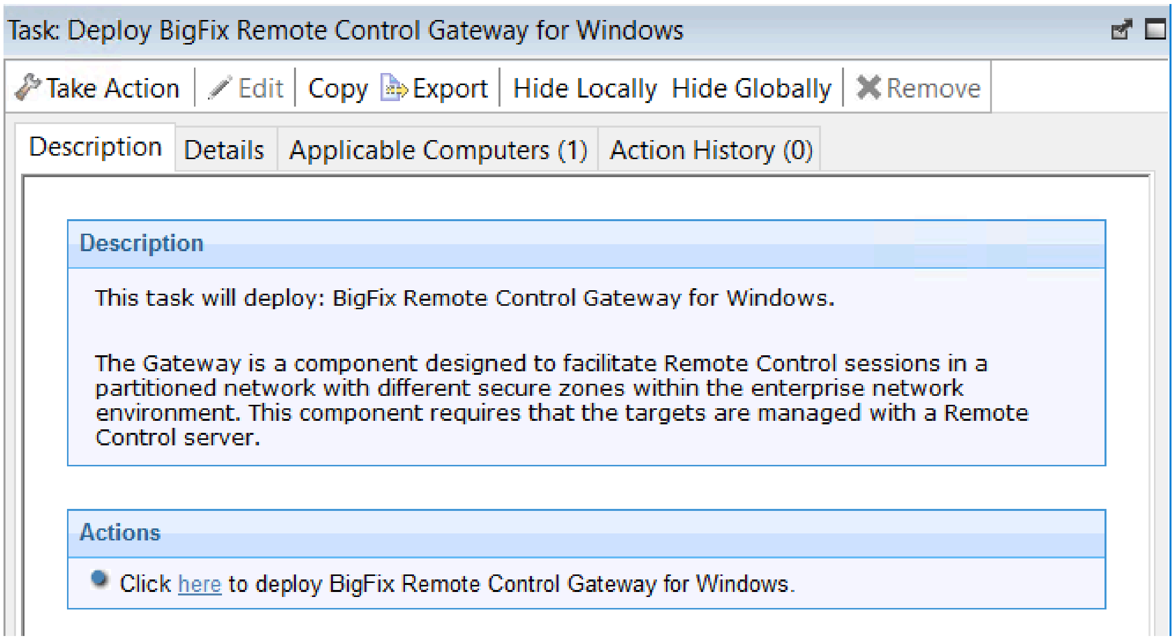
Note: After the removal of the cli tools, some files might not be deleted automatically. The files were created during the installation of the cli tools. These files are in `C:\ProgramData\BigFix\Remote Control\`.

Deploying the Windows® gateway support

You can use the **Deploy Remote Control Gateway for Windows** task to install gateway support onto a Windows® computer.

To start this task, complete the following steps:

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Deploy Remote Control Gateway for Windows**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will deploy: BigFix Remote Control Gateway for Windows.

The Gateway is a component designed to facilitate Remote Control sessions in a partitioned network with different secure zones within the enterprise network environment. This component requires that the targets are managed with a Remote Control server.

Actions

- Click here to deploy BigFix Remote Control Gateway for Windows.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the gateway support on.
5. Click **OK**.

The summary screen shows the progress of the task.

Gateway support is installed on the targets that you selected when you ran the deployment task. The files are in the `\Program Files\BigFix\Remote Control\Gateway` directory on the selected targets.

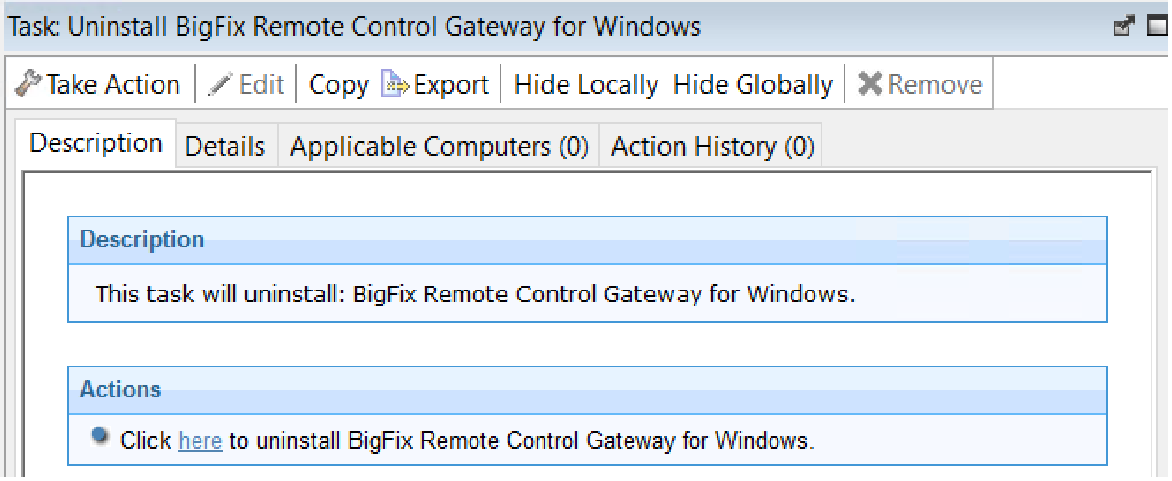
To use the gateway support, you must set up a gateway configuration for your environment. For more information about configuring the gateways, see the *BigFix® Remote Control Administrator's Guide*

Removing the Windows® gateway support

You can use the **Uninstall Remote Control Gateway support for Windows** task to remove the gateway support files from a Windows® computer.

To initiate this task, complete the following steps:

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Uninstall Remote Control Gateway for Windows** .
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Task: Uninstall BigFix Remote Control Gateway for Windows

Description

This task will uninstall: BigFix Remote Control Gateway for Windows.

Actions

- Click here to uninstall BigFix Remote Control Gateway for Windows.

4. In the Take Action pane, in the Target tab, select the relevant option for determining which targets to remove the gateway support from.
5. Click **OK**.

The summary screen shows the progress of the task.

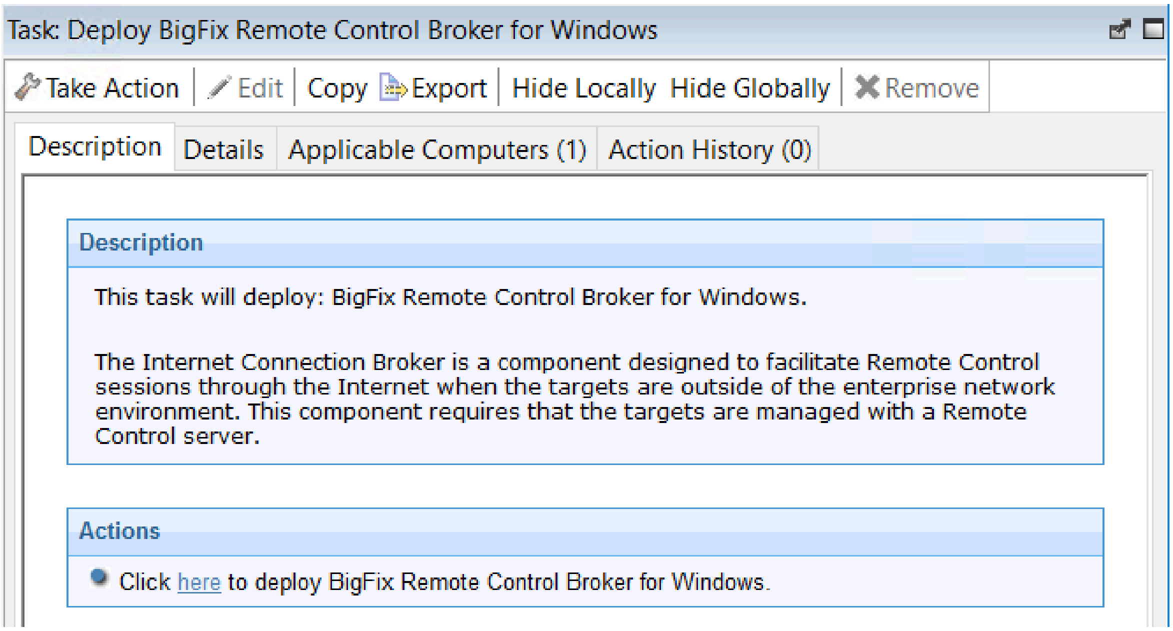
The gateway support files are removed from the selected targets.

Deploying Windows™ broker support

You can use the **Deploy Remote Control Broker for Windows** task to install broker support on a Windows™ computer

To initiate this task, complete the following steps:

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Deploy Remote Control Broker for Windows**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will deploy: BigFix Remote Control Broker for Windows.

The Internet Connection Broker is a component designed to facilitate Remote Control sessions through the Internet when the targets are outside of the enterprise network environment. This component requires that the targets are managed with a Remote Control server.

Actions

- Click here to deploy BigFix Remote Control Broker for Windows.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the broker support on.
5. Click **OK**.

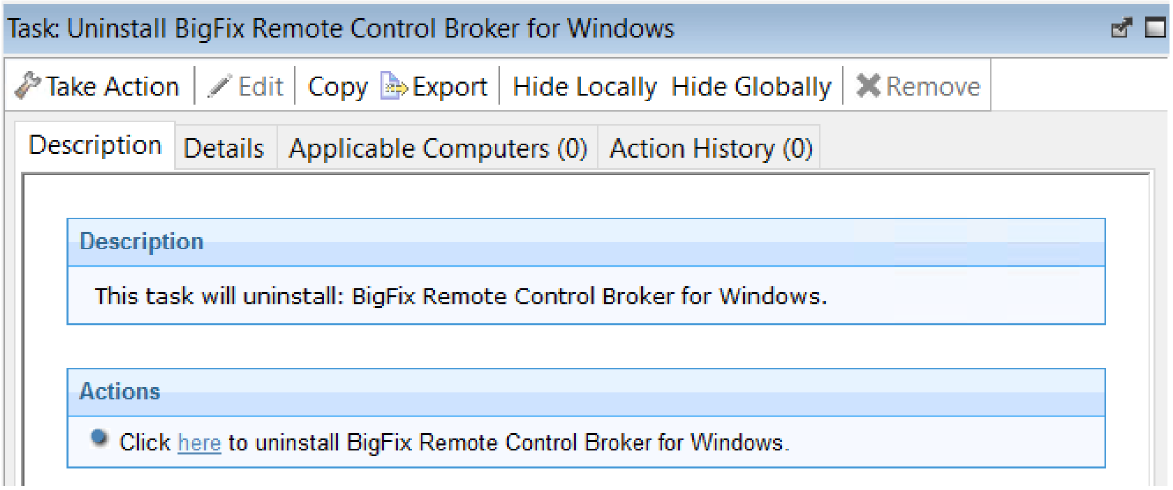
The summary screen shows the progress of the task. Broker support is installed on the targets that you selected when you ran the deployment task. The files are installed in the `[working dir]\Broker` directory on the selected targets. The value of *[working dir]* is determined by the version of Windows™ operating system that you are installing the broker support on. For example, `C:\ProgramData\BigFix\Remote Control`. To use the broker support, you must set up a broker configuration for your environment. For more information about configuring the broker, see the *BigFix® Remote Control Administrator's Guide*.

Removing Windows™ broker support

You can use the **Uninstall Remote Control Broker for Windows** task to remove broker support from a Windows™ computer

To initiate this task, complete the following steps:

1. Click **Deployment > Windows** in the navigation tree.
2. Click **Uninstall Remote Control Broker for Windows** .
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will uninstall: BigFix Remote Control Broker for Windows.

Actions

● Click here to uninstall BigFix Remote Control Broker for Windows.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to remove the broker support from.
5. Click **OK**.

The summary screen shows the progress of the task. The broker support files are removed from the chosen targets.

Deploy the components on a Linux™ system

The **Linux** deployment node provides a set of tasks that you can use to install or remove the following components in a Linux™ environment.

- Target and controller software
- CLI tools
- Gateway support
- Broker support

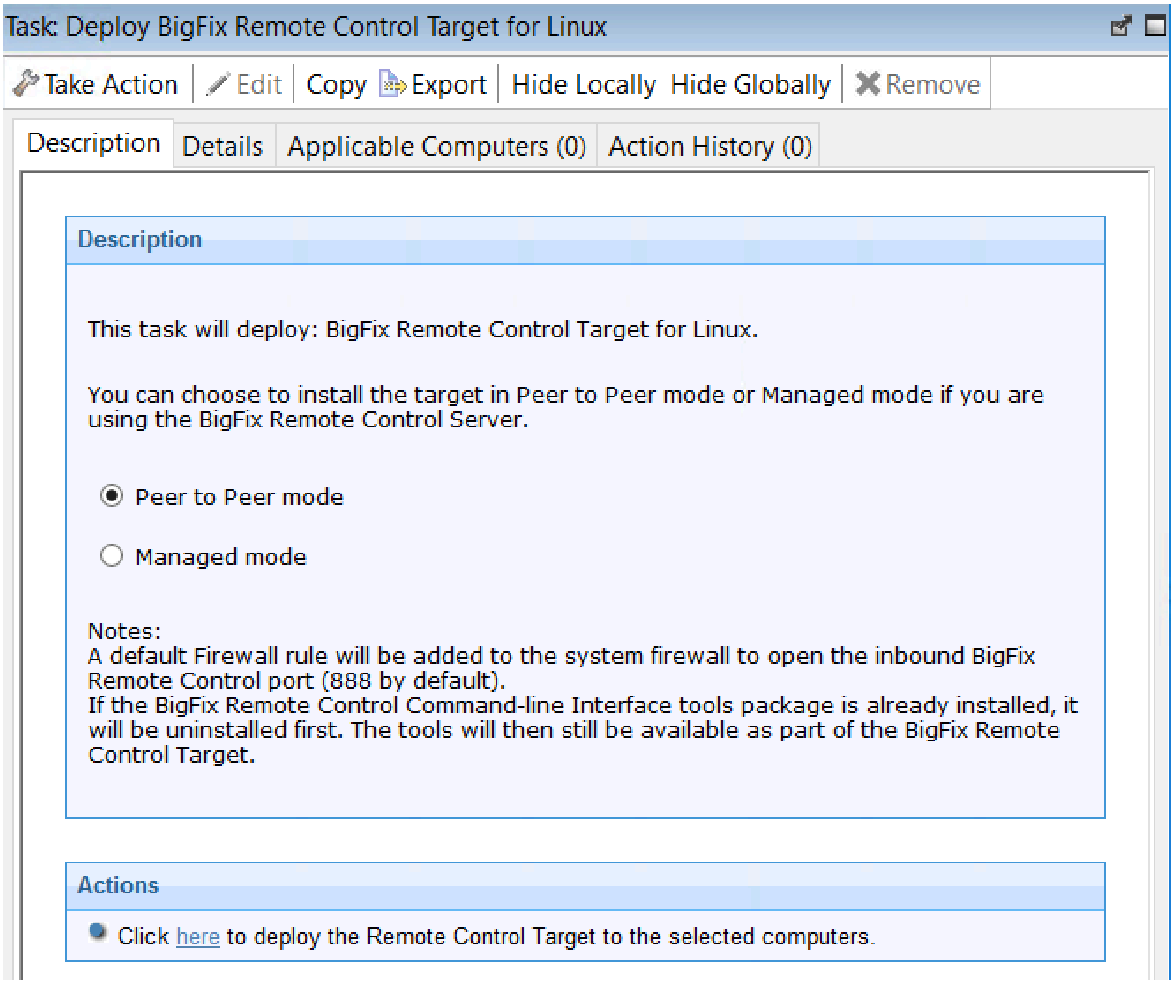
Deploying the Linux® target

You can use the **Deploy Remote Control Target for Linux** task to install the target software onto a Linux® computer.

To initiate this task, complete the following steps:

1. In the navigation tree, click **Deployment > Linux**.
2. Click **Deploy Remote Control target for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.

   Determine your installation method and follow the instructions that are given.



Description

This task will deploy: BigFix Remote Control Target for Linux.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

● Peer to Peer mode

○ Managed mode

Notes:
A default Firewall rule will be added to the system firewall to open the inbound BigFix Remote Control port (888 by default).
If the BigFix Remote Control Command-line Interface tools package is already installed, it will be uninstalled first. The tools will then still be available as part of the BigFix Remote Control Target.

Actions

- Click here to deploy the Remote Control Target to the selected computers.

Peer to Peer mode

With this installation method, you can establish remote control sessions directly between the controller and the target without the need for an Remote Control server. This deployment method installs the target without requiring an Remote Control server URL to be specified. The local target policies that are set by this installation method are used when a remote control session is established. For more information about target installation properties, see Manage target and server configurations *(on page 57)*.

In the Take Action pane on the Target tab, select the relevant option for determining the computers on which to deploy the Remote Control target.

Click **OK**.

The summary screen shows the progress of the task.

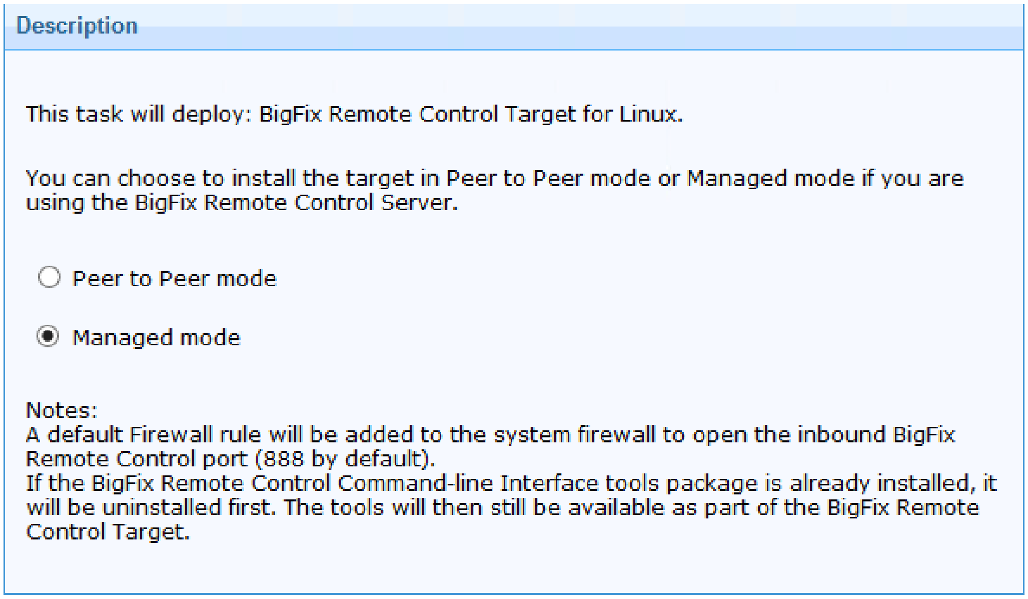
Note: To register the target on the Remote Control server in the future, use the Target wizard to create a configuration task and specify the server URL of your server. Running this task on the selected target reconfigures it so that it can contact the server. For more information about target configuration tasks, see Creating Remote Control target configuration tasks *(on page 71)*. If the secure registration feature is enabled on the server you can distribute a secure registration token to the target. For more information, see Distributing a secure registration token to targets *(on page 105)*.

Managed mode

Choose this installation option for targets to register with the Remote Control server and take part in remote control sessions started from the server. This deployment method requires an Remote Control server URL to be specified. If a remote control session, started from the Remote Control server, is requested with this target, the specified server is contacted to authenticate the request. When the request is authenticated, the policies that are set for the session are passed from the Remote Control server to the target and the session is started. For more information about target installation properties, see Manage target and server configurations *(on page 57)*.

Enter the URL of your Remote Control server.

Enter a valid secure registration token if the secure target registration feature is enabled on the server.



Description

This task will deploy: BigFix Remote Control Target for Linux.

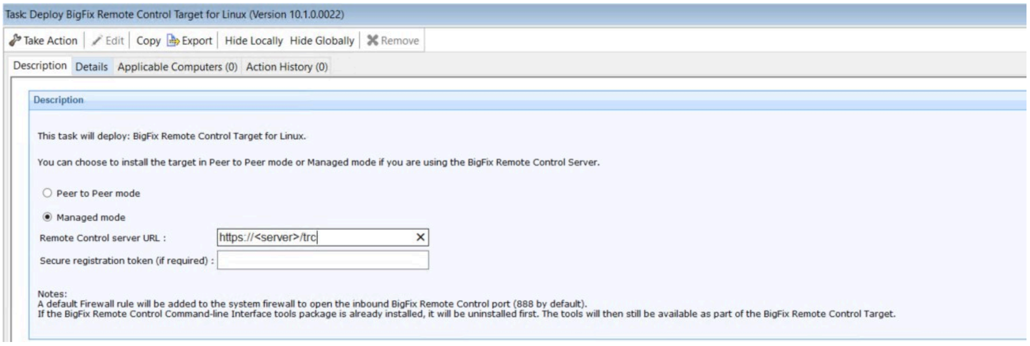
You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

○ Peer to Peer mode

● Managed mode

Notes:
A default Firewall rule will be added to the system firewall to open the inbound BigFix Remote Control port (888 by default).
If the BigFix Remote Control Command-line Interface tools package is already installed, it will be uninstalled first. The tools will then still be available as part of the BigFix Remote Control Target.

Enter the URL of your Remote Control server and click **OK**.



This task will deploy: BigFix Remote Control Target for Linux.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

○ Peer to Peer mode

● Managed mode

Remote Control server URL : https://<server>/trc

Secure registration token (if required) :

Notes:
A default Firewall rule will be added to the system firewall to open the inbound BigFix Remote Control port (888 by default).
If the BigFix Remote Control Command-line Interface tools package is already installed, it will be uninstalled first. The tools will then still be available as part of the BigFix Remote Control Target.

In the Take Action pane on the Target tab, select the relevant option for determining the computers on which to deploy the Remote Control target.

Click **OK**.

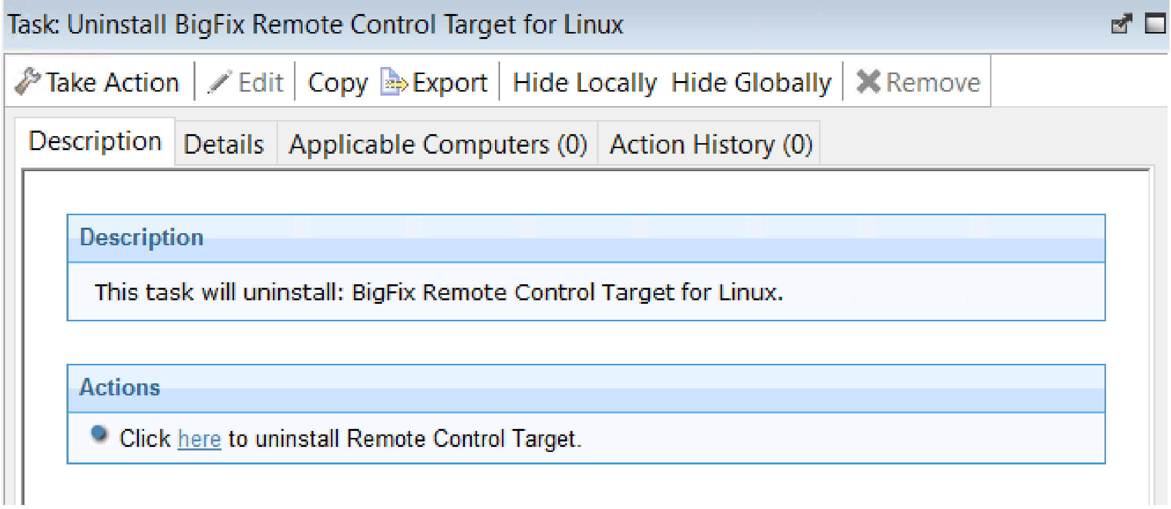
The summary screen shows the progress of the task and status *complete* when it is finished.

Removing the Linux® target

You can use the **Uninstall Remote Control Target for Linux** task to remove the target software from a Linux® computer.

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** > in the navigation tree.
2. Click **Uninstall Remote Control target for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



This task will uninstall: BigFix Remote Control Target for Linux.

Click here to uninstall Remote Control Target.

4. In the Take Action pane, on the Target tab, select the relevant option for determining which targets to remove the Remote Control target from.
5. Click **OK**.

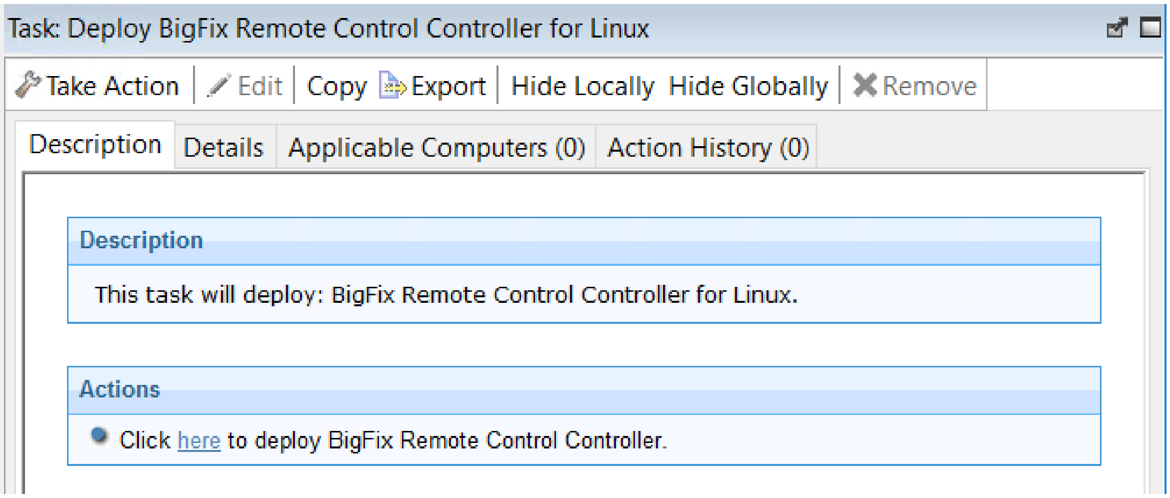
The summary screen shows the progress of the task.

Note: After the removal of the target, some files might not be deleted automatically. The files were created during the installation of the target. These files are in the following directories `/opt/bigfix` and `/var/opt/bigfix/trc/target`.

Deploying the Linux® controller

You can use the **Deploy Remote Control Controller for Linux** task to install the controller software onto a Linux® computer.

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Deploy Remote Control Controller for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Task: Deploy BigFix Remote Control Controller for Linux

This task will deploy: BigFix Remote Control Controller for Linux.

- Click here to deploy BigFix Remote Control Controller.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the controller on.
5. Click **OK**.

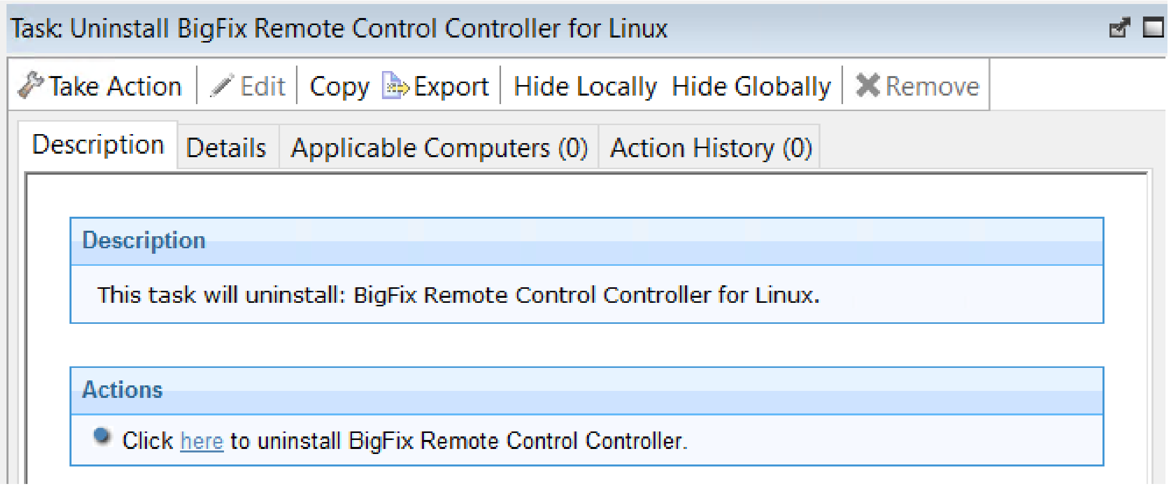
The summary screen shows the progress of the task.

Removing the Linux® controller

You can use the **Uninstall Remote Control Controller for Linux** task to remove the controller software from a Linux® computer.

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Uninstall Remote Control Controller for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Task: Uninstall BigFix Remote Control Controller for Linux

Description

This task will uninstall: BigFix Remote Control Controller for Linux.

Actions

● Click here to uninstall BigFix Remote Control Controller.

4. In the Take Action pane, in the Target tab, select the relevant option for determining which targets to remove the Remote Control controller from.
5. Click **OK**.

The summary screen shows the progress of the task.

Deploying the Linux® CLI tools

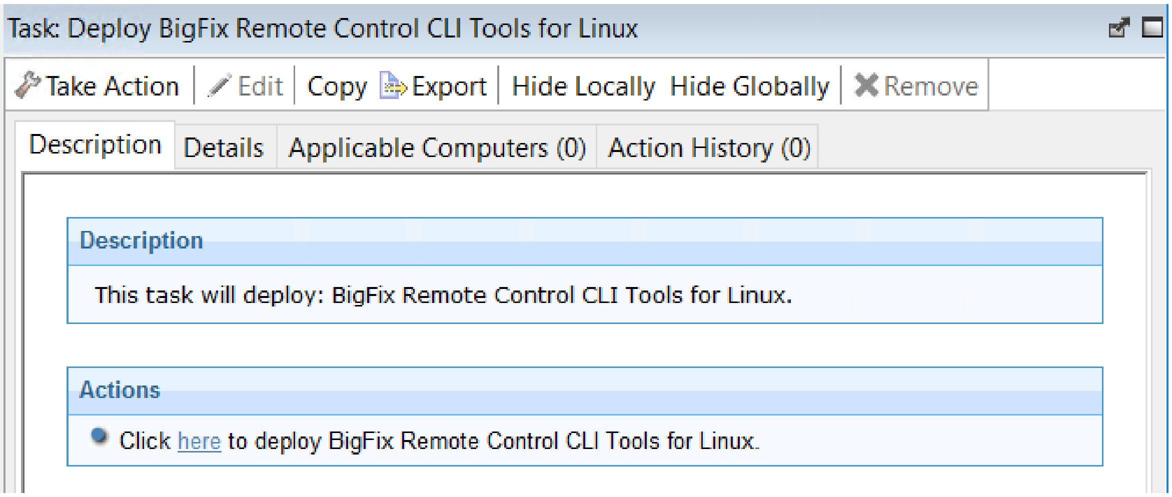
You can use the **Deploy Remote Control CLI Tools for Linux** task to install the CLI tools onto a Linux® computer.

Note:

1. The CLI tools are also installed when you install the target software. Therefore, use the **Deploy Remote Control CLI Tools for Linux** Fixlet to deploy the CLI tools only on computers that do not have the target software installed.
2. To deploy this task, you need the URL for an Remote Control server that you have access to.

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Deploy Remote Control CLI Tools for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



This task will deploy: BigFix Remote Control CLI Tools for Linux.

● Click here to deploy BigFix Remote Control CLI Tools for Linux.

4. Enter the URL of the Remote Control server and click **OK**.
5. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the CLI tools on.
6. Click **OK**.

The summary screen shows the progress of the task and displays status complete when it is finished.

The following two CLI utilities are installed in the `/opt/bigfix/trc/target` directory on the targets that were selected when you ran the deployment task.

`wrc`

Use this tool to start a remote control session with a target.

`wrcmdpcr`

Use this tool to run a command on a target. The output from the command is displayed on the computer that you ran the command from.

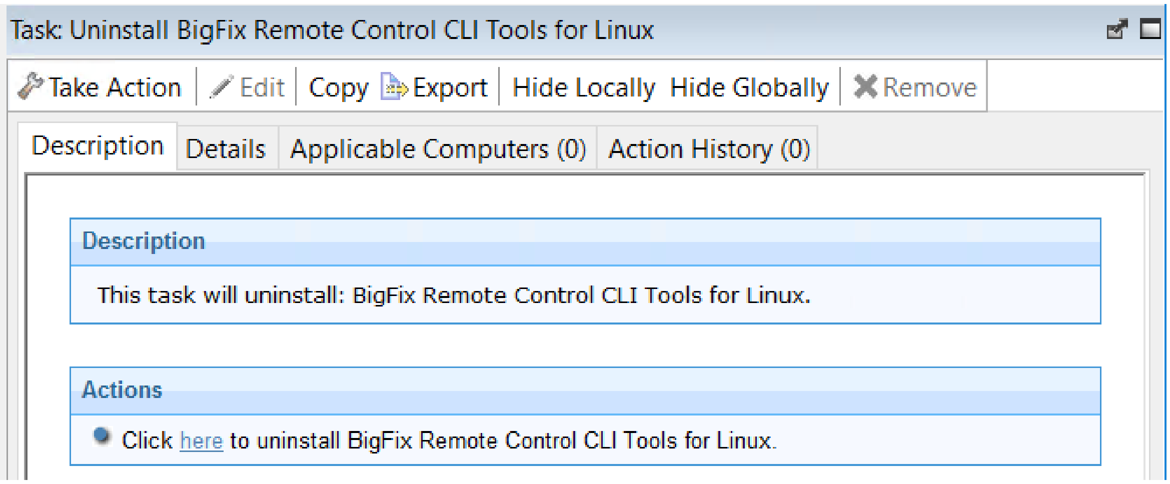
For more information about how to use the command line tools, see the *BigFix® Remote Control Controller User's Guide*.

Removing the Linux® CLI tools

You can use the **Uninstall Remote Control CLI Tools for Linux** task to remove the CLI tools from a Linux® computer that has the CLI tools already installed.

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Uninstall Remote Control CLI Tools for Linux** .
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.


Task: Uninstall BigFix Remote Control CLI Tools for Linux

Description

This task will uninstall: BigFix Remote Control CLI Tools for Linux.

Actions

- Click here to uninstall BigFix Remote Control CLI Tools for Linux.

4. In the Take Action pane, in the Target tab, select the relevant option for determining which targets to remove the CLI tools from.
5. Click **OK**.

The summary screen shows the progress of the task.

The CLI tools are longer present on the selected targets.

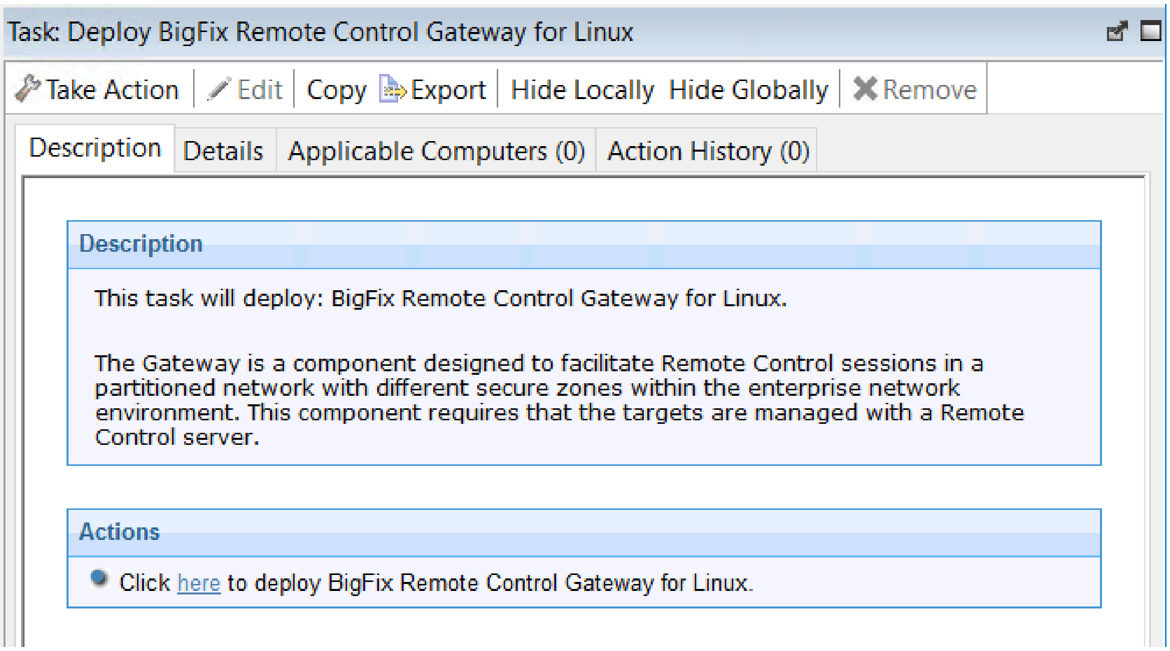
Note: After the removal of the CLI tools, some files might not be deleted automatically. The files were created during the installation of the tools. These files are in the following directories `/etc`,`/opt/bigfix`,`/var/opt/bigfix/trc/cli`, and `/var/opt/bigfix/trc/target`.

Deploying the Linux® gateway support

You can use the **Deploy Remote Control Gateway for Linux** task to install gateway support onto a Linux® computer.

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Deploy Remote Control Gateway for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will deploy: BigFix Remote Control Gateway for Linux.

The Gateway is a component designed to facilitate Remote Control sessions in a partitioned network with different secure zones within the enterprise network environment. This component requires that the targets are managed with a Remote Control server.

Actions

- Click here to deploy BigFix Remote Control Gateway for Linux.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the gateway support on.
5. Click **OK**.

The summary screen shows the progress of the task and displays status complete when it is finished.

Gateway support is installed on the targets that you selected when you ran the deployment task. The files are installed in the `/opt/bigfix/trc/gateway` directory on the selected targets.

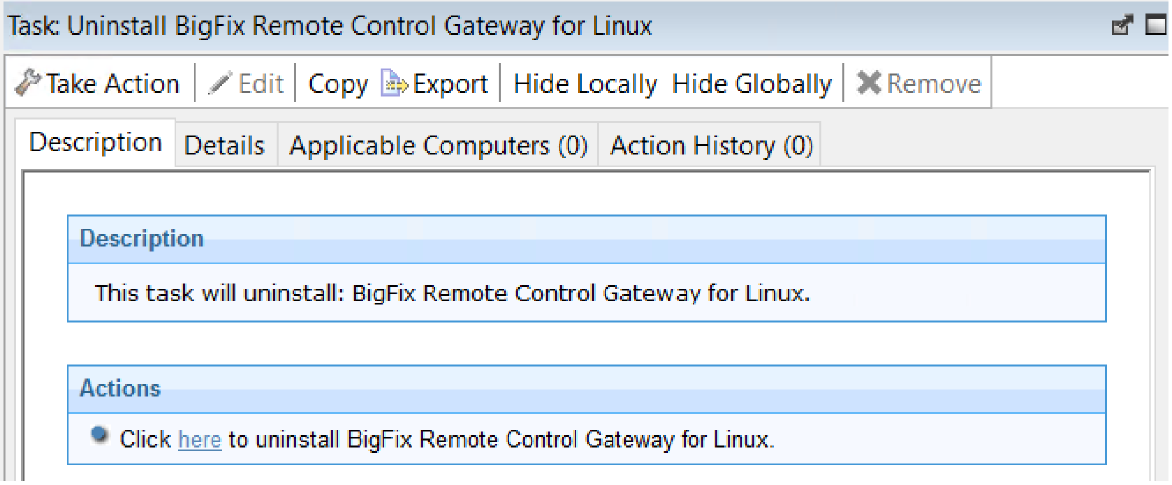
To use the gateway support, you must set up a gateway configuration for your environment. For more information about configuring the gateway, see the *BigFix® Remote Control Administrator's Guide*.

Removing the Linux® gateway support

You can use the **Uninstall Remote Control Gateway support for Linux** task to remove the gateway support files from a Linux® computer.

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Uninstall Remote Control Gateway for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will uninstall: BigFix Remote Control Gateway for Linux.

Actions

- Click here to uninstall BigFix Remote Control Gateway for Linux.

4. In the Take Action pane, in the Target tab, select the relevant option for determining which targets to remove the gateway support from.
5. Click **OK**.

The summary screen shows the progress of the task and displays status complete when it is finished.

The gateway support files are removed from the selected targets.

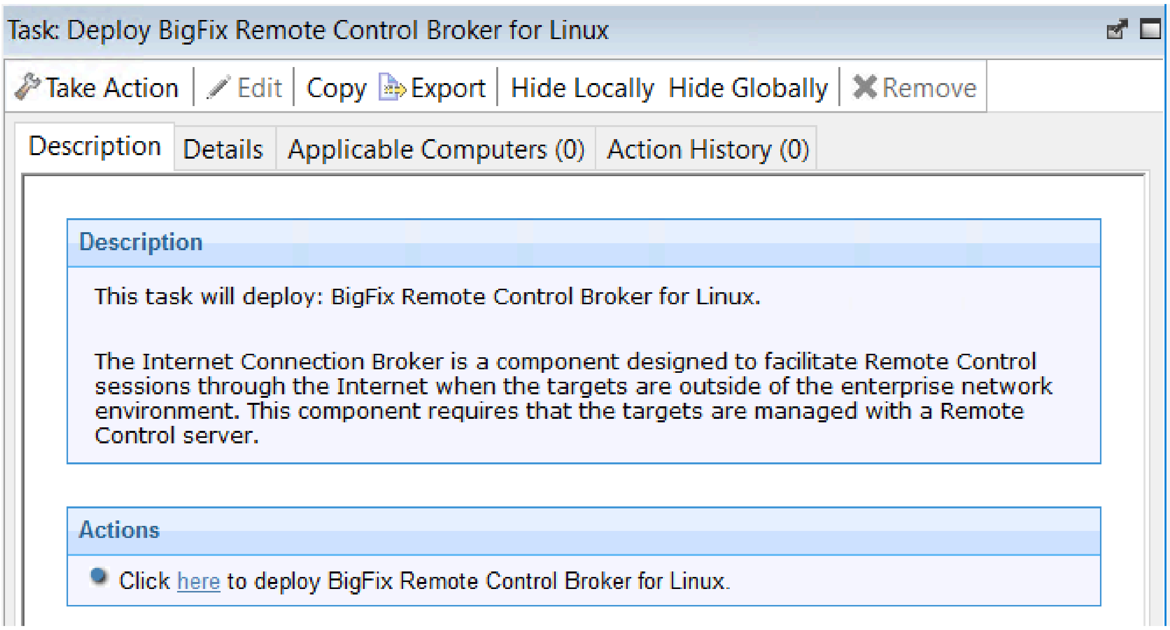
Note: After the removal of the gateway support, some files might not be deleted automatically. The files were created during the installation of the gateway component. The files are in the directory `/opt/bigfix` and `/var/opt/bigfix/trc/gateway`.

Deploying Linux broker support

You can use the **Deploy Remote Control Broker for Linux** task to install broker support on a Linux computer.

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Deploy Remote Control Broker for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will deploy: BigFix Remote Control Broker for Linux.

The Internet Connection Broker is a component designed to facilitate Remote Control sessions through the Internet when the targets are outside of the enterprise network environment. This component requires that the targets are managed with a Remote Control server.

Actions

- Click here to deploy BigFix Remote Control Broker for Linux.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to deploy the broker support on.
5. Click **OK**.

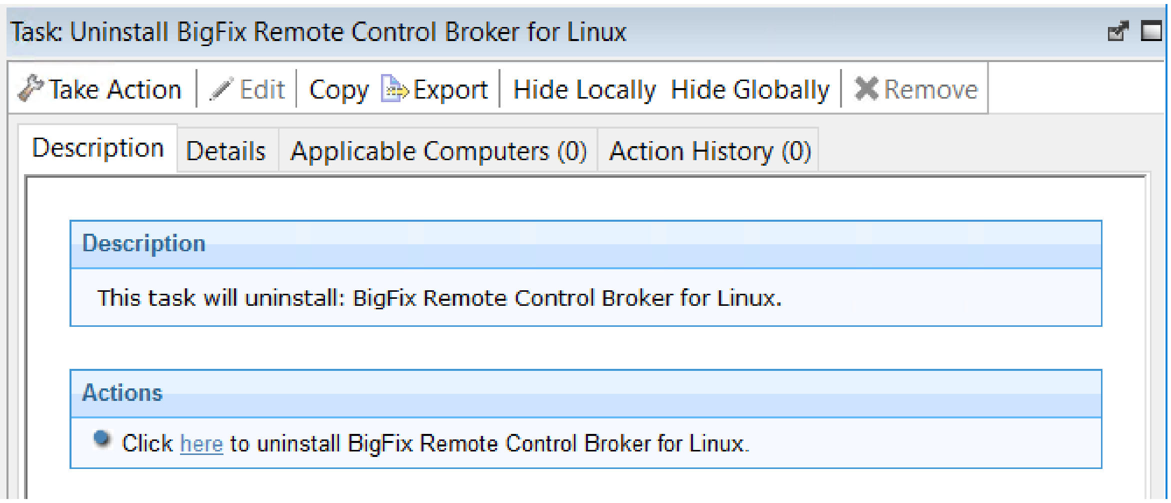
The summary screen shows the progress of the task. The broker support files are installed on the targets that you selected when you ran the deployment task. The files are installed in the `/opt/bigfix/trc/broker` directory on the selected targets. To use the broker support you must set up a broker configuration for your environment. For more information about configuring the broker, see the *BigFix® Remote Control Administrator's Guide*.

Removing Linux broker support

You can use the **Uninstall Remote Control Broker for Linux** task to remove broker support from a Linux computer

To initiate this task, complete the following steps:

1. Click **Deployment > Linux** in the navigation tree.
2. Click **Uninstall Remote Control Broker for Linux**.
3. In the Task pane, review the description and follow the instructions in the Actions box to start the task.



Description

This task will uninstall: BigFix Remote Control Broker for Linux.

Actions

- Click here to uninstall BigFix Remote Control Broker for Linux.

4. In the Take Action pane on the Target tab, select the relevant option for determining which targets to remove the broker support from.
5. Click **OK**.

The summary screen shows the progress of the task. The broker support files are removed from the chosen targets.

Deploy the components on a macOS system

The **macOS** deployment node provides a set of tasks that you can use to install or remove the following components in a macOS operating system environment.

- Target component
- Controller component

Deploying the BigFix® Remote Control Target for macOS

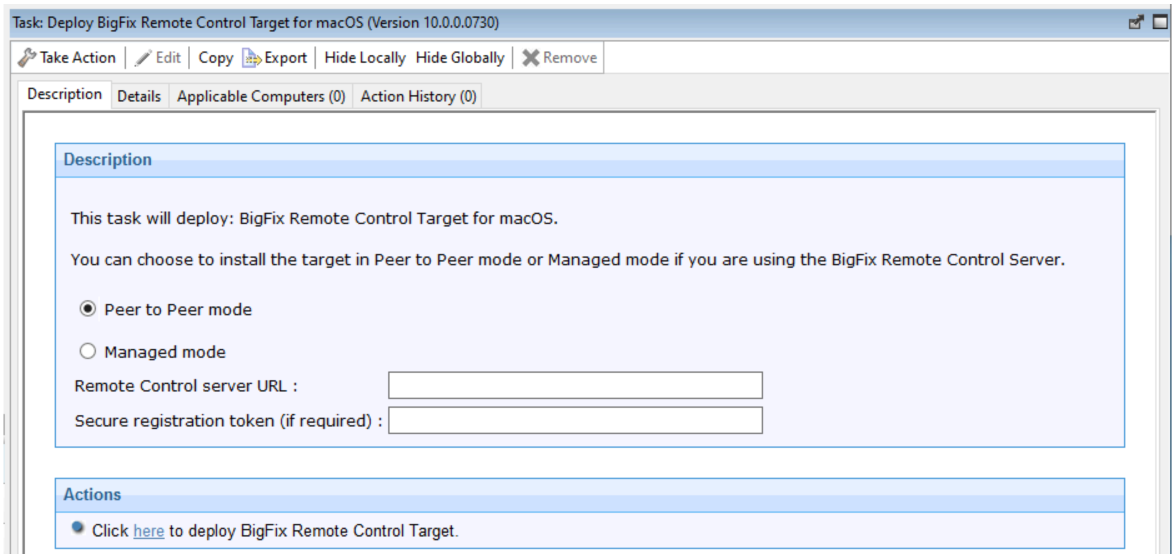
Use the **Deploy BigFix® Remote Control Target for macOS** task to install the target software onto a macOS system.

Note: Selecting the managed mode option prompts for a server URL and a secure registration token.

To install the target, complete the following steps:

1. In the navigation tree, click **Deployment > macOS**.
2. Click **Deploy BigFix® Remote Control Target for macOS**.
3. In the **Task** pane, review the description and follow the instructions in the **Actions** box to start the task.

   Select the option for your relevant installation method and follow the instructions to complete installation.


Task: Deploy BigFix Remote Control Target for macOS (Version 10.0.0.0730)
Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove
Description | Details | Applicable Computers (0) | Action History (0)

Description

This task will deploy: BigFix Remote Control Target for macOS.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

● Peer to Peer mode

○ Managed mode

Remote Control server URL :

Secure registration token (if required) :

Actions

- Click here to deploy BigFix Remote Control Target.

- **Peer to Peer mode**

  With this installation method, you can establish remote control sessions directly between the controller and the target without the need for an Remote Control server. This deployment method installs the target without requiring an Remote Control server URL to be specified. The local target policies set by this installation method are used when a remote control session is established. For more information about the target installation properties, see Manage target and server configurations *(on page 57)*.

  In the Take Action pane on the Target tab, select the relevant option for determining the computers on which to deploy the Remote Control target.

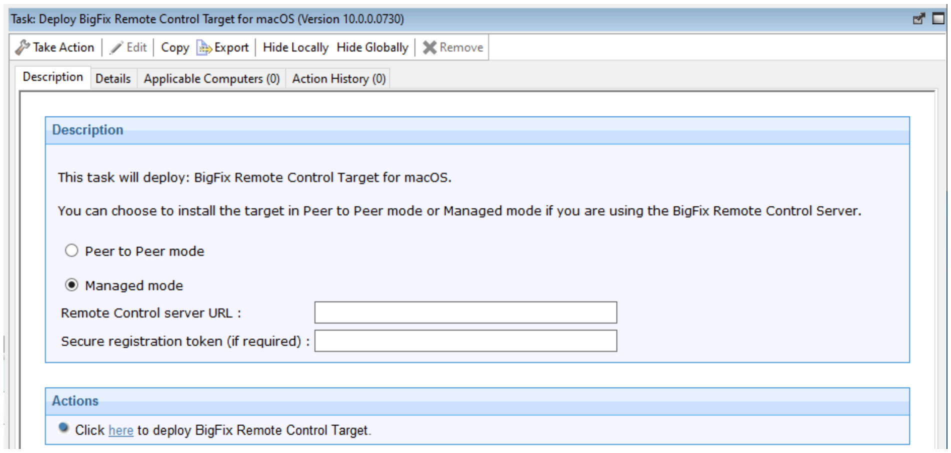
  Click **OK** .

  The summary screen shows the progress of the task and displays status *complete* when it is finished.

  Note: For the target to register with the Remote Control server in the future, use the Remote Control Target wizard. Create a configuration task and specify the server URL of the relevant server. Run the task on the selected target to reconfigure it so that it can contact the server. For more information about target configuration tasks, see Creating Remote Control target configuration tasks *(on page 71)*. If the secure registration feature is enabled on the server you can distribute a secure registration token to the target. For more information, see Distributing a secure registration token to targets *(on page 105)*.

- **Managed mode**

  Choose this installation option for targets to register with the Remote Control server and take part in remote control sessions started from the server. This deployment method requires an Remote Control server URL to be specified. If a remote control session is requested with this target, the specified server is contacted to authenticate the request. When the request is authenticated, the policies for the session are passed from the remote control server to the target and the session is established. For more information about target installation properties, see Manage target and server configurations *(on page 57)*.



Task: Deploy BigFix Remote Control Target for macOS (Version 10.0.0.0730)

Description

This task will deploy: BigFix Remote Control Target for macOS.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

○ Peer to Peer mode

● Managed mode

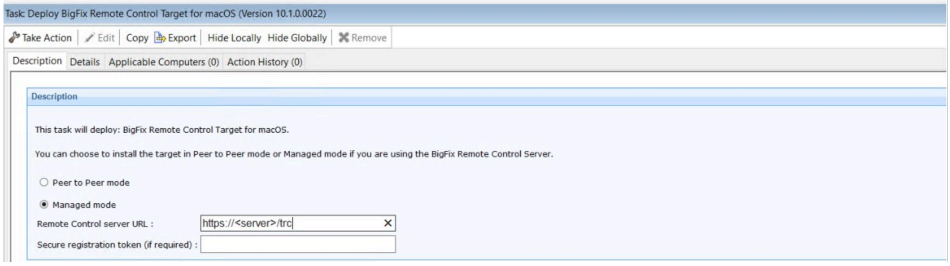
Remote Control server URL :

Secure registration token (if required) :

Actions

Click here to deploy BigFix Remote Control Target.

  Enter the URL of your Remote Control server and click **OK**.



Task: Deploy BigFix Remote Control Target for macOS (Version 10.1.0.0022)

Description

This task will deploy: BigFix Remote Control Target for macOS.

You can choose to install the target in Peer to Peer mode or Managed mode if you are using the BigFix Remote Control Server.

○ Peer to Peer mode

● Managed mode

Remote Control server URL : https://<server>/trc

Secure registration token (if required) :

  In the Take Action pane on the Target tab, select the relevant option for determining the computers on which to deploy the Remote Control target.

  Click **OK**.

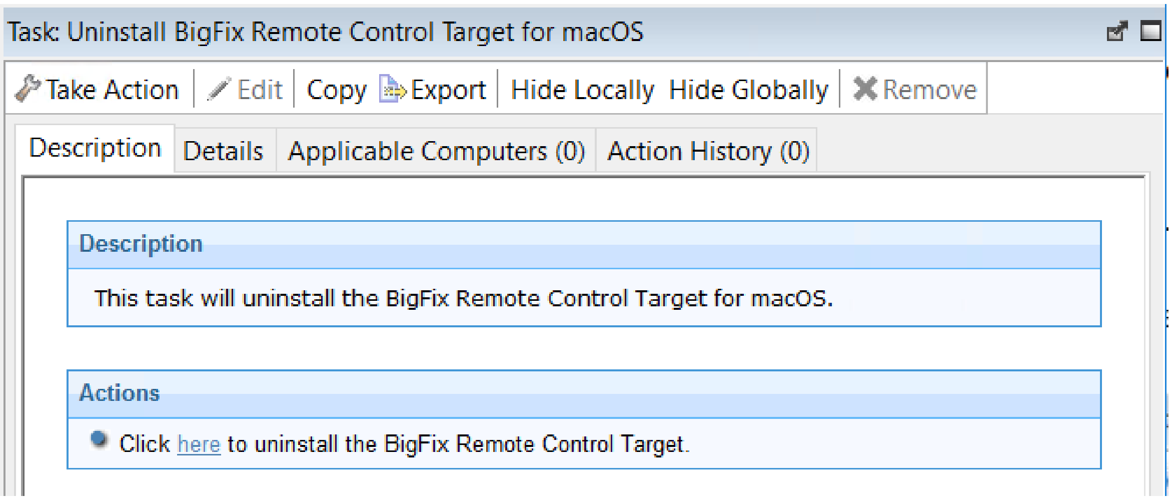
  The summary screen shows the progress of the task and status *complete* when it is finished.

Removing the BigFix® Remote Control Target for macOS

Use the **Uninstall BigFix® Remote Control Target for macOS** task to remove the target software from a macOS system.

To remove the target, complete the following steps:

1. Within the **Systems Lifecycle** domain, expand **Remote Control configuration > Remote Control**.
2. Expand the **Deployment** node.
3. Select **macOS**.
4. Select **Uninstall BigFix® Remote Control Target for macOS**.
5. In the **Task** pane, review the description and follow the instructions in the **Actions** box to start the task.



This task will uninstall the BigFix Remote Control Target for macOS.

Click here to uninstall the BigFix Remote Control Target.

6. In the **Take Action** pane on the **Target** tab, select the relevant option for determining which computers to remove the BigFix® Remote Control Target for macOS component from.
7. Click **OK**.

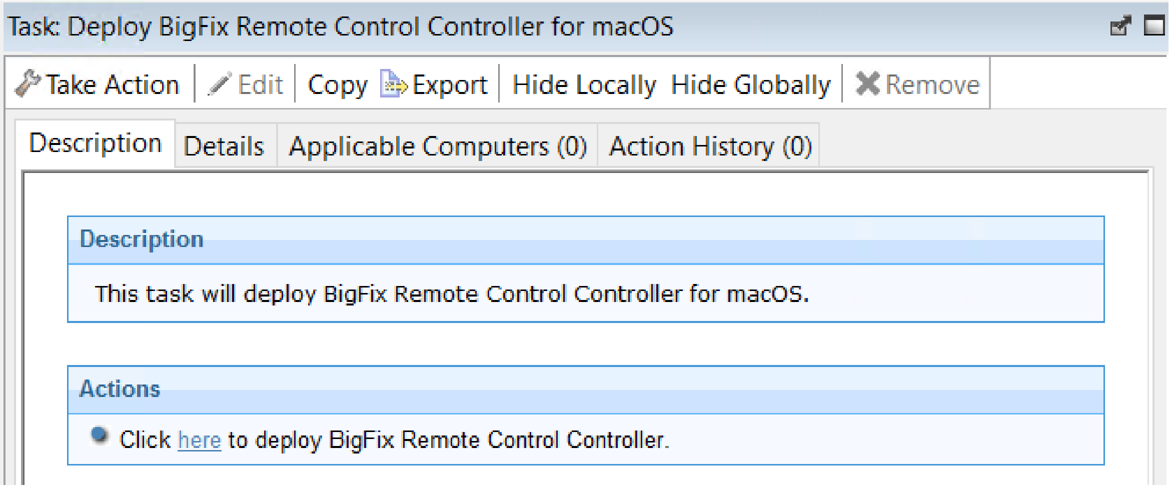
   The summary screen shows the progress of the task and the status is set to **Complete** when it is finished.

Deploying the BigFix® Remote Control Controller for macOS

Use the **Deploy BigFix® Remote Control Controller for macOS** task to install the controller software onto a macOS system.

To install the controller, complete the following steps:

1. Within the **Systems Lifecycle** domain, expand **Remote Control configuration > Remote Control**.
2. Expand the **Deployment** node.
3. Select **macOS**.
4. Select **Deploy BigFix® Remote Control Controller for macOS**.
5. In the **Task** pane, review the description and follow the instructions in the **Actions** box to start the task.



Task: Deploy BigFix Remote Control Controller for macOS

Description

This task will deploy BigFix Remote Control Controller for macOS.

Actions

- Click here to deploy BigFix Remote Control Controller.

6. In the **Take Action** pane on the **Target** tab, select the relevant option for determining which computers to deploy the BigFix® Remote Control Controller for macOS component on.
7. Click **OK**.

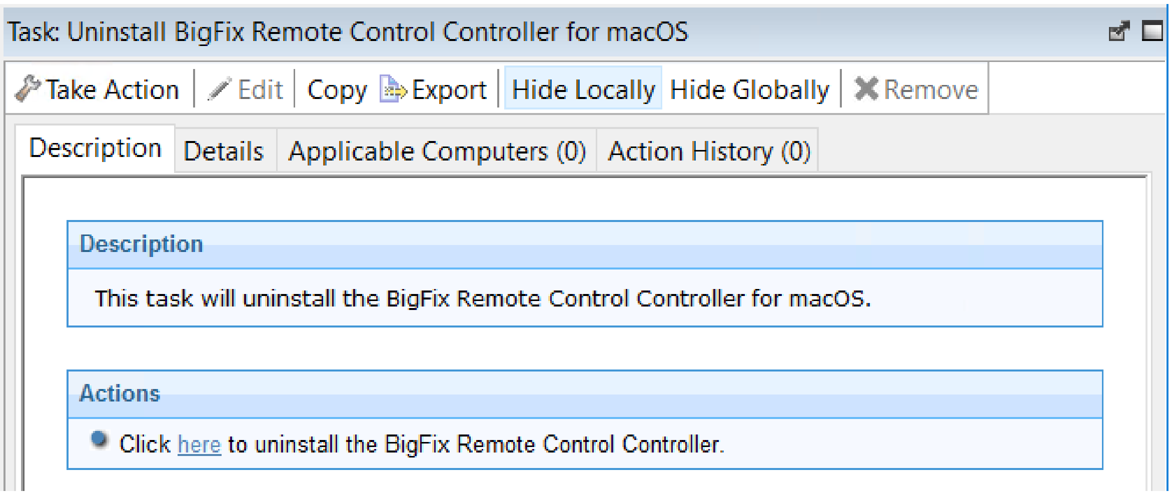
   The summary screen shows the progress of the task and the status is set to **Complete** when it is finished.

Removing the BigFix® Remote Control Controller for macOS

Use the **Uninstall BigFix® Remote Control Controller for macOS** task to remove the controller software from a macOS system.

To remove the controller, complete the following steps:

1. Within the **Systems Lifecycle** domain, expand **Remote Control configuration > Remote Control**.
2. Expand the **Deployment** node.
3. Select **macOS**.
4. Select **Uninstall BigFix® Remote Control Controller for macOS**.
5. In the **Task** pane, review the description and follow the instructions in the **Actions** box to start the task.



Task: Uninstall BigFix Remote Control Controller for macOS

Description

This task will uninstall the BigFix Remote Control Controller for macOS.

Actions

- Click here to uninstall the BigFix Remote Control Controller.

6. In the **Take Action** pane on the **Target** tab, select the relevant option for determining which computers to remove the BigFix® Remote Control Controller for macOS component from.
7. Click **OK**.

   The summary screen shows the progress of the task and the status is set to **Complete** when it is finished.

Update the Remote Control components

The **Update** node in the Remote Control navigation tree provides subnodes that are operating system specific. Use the **Update** node to upgrade the components to a later version. To view a list of tasks that you can use to upgrade the components, select the relevant operating system node.

Update the components on a Windows™ system

The **Windows** subnode provides the latest levels of Remote Control component software for use on a Windows™ system. The components contain the latest enhancements and fixes that are applied to Remote Control.

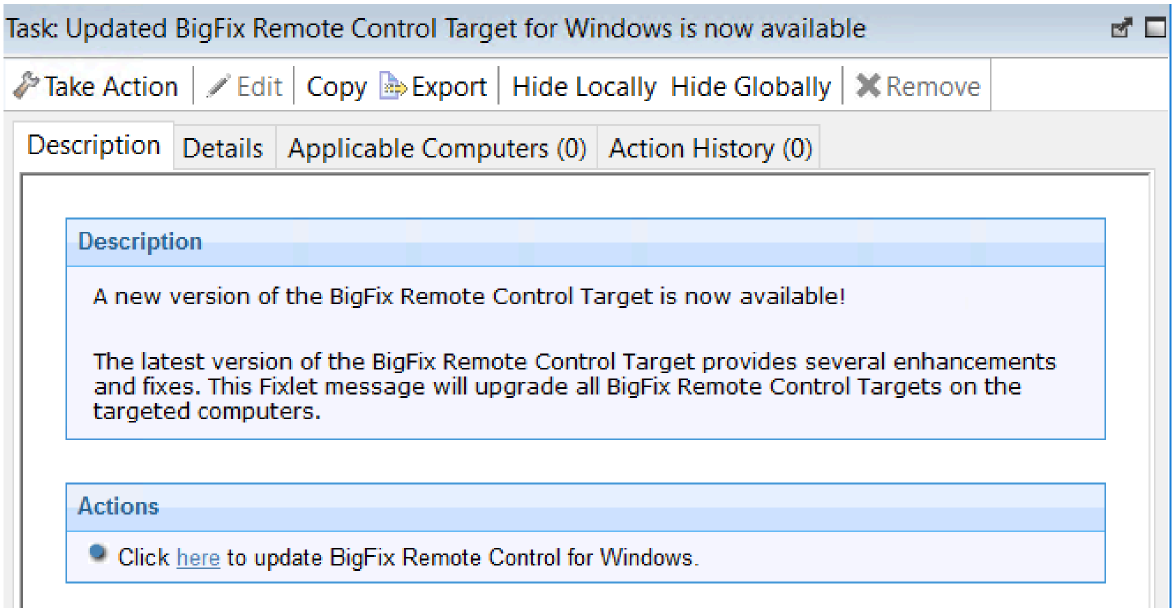
Updating the Windows™ target

You can use the Windows™ operating system tasks to update the target software, on a Windows™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the target configuration that is already installed. To initiate a task, complete the following steps:

1. Click **Updates > Windows** in the navigation tree.
2. Select the Fixlet that is relevant to the version of the target that you want to upgrade to.

   For example, **Updated Remote Control Target for Windows is now available! (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.

   For example,



A new version of the BigFix Remote Control Target is now available!

The latest version of the BigFix Remote Control Target provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Targets on the targeted computers.

Click here to update BigFix Remote Control for Windows.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the target update on.
5. Click **OK**.

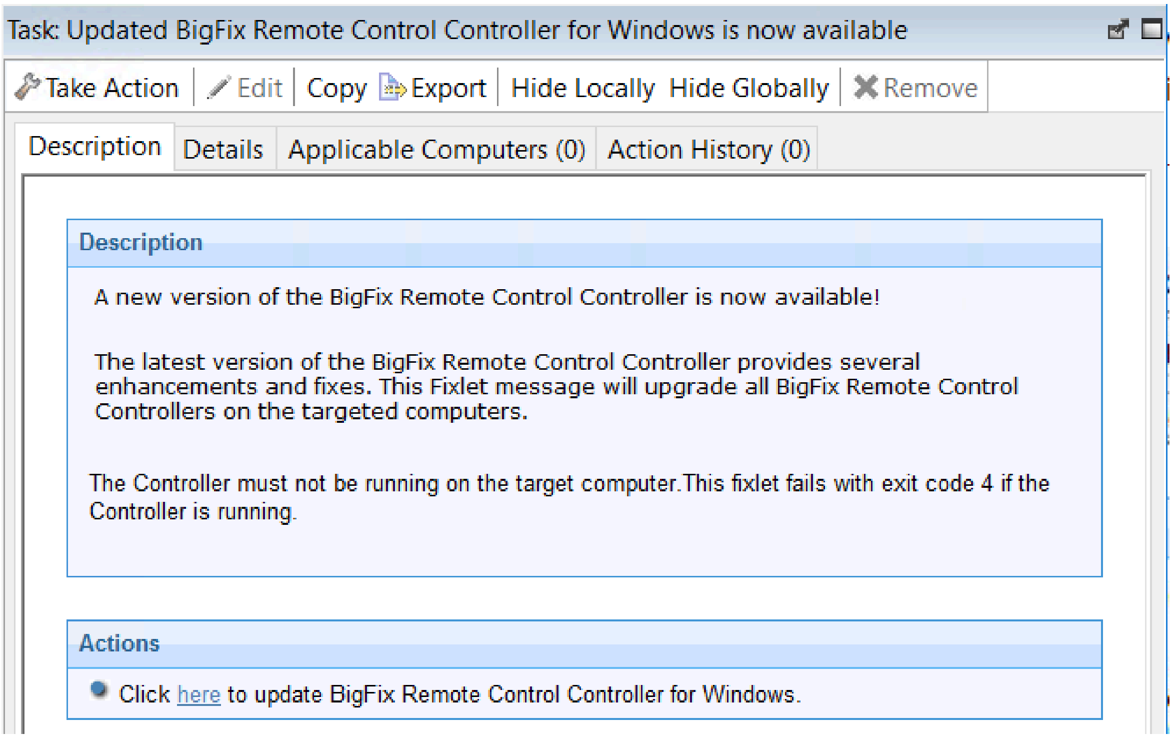
The summary screen shows the progress of the task.

The selected targets are upgraded to the version of target software that is applicable to the chosen update.

Updating the Windows™ controller

Use the Windows™ operating tasks to update the controller software, on a Windows™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the controller that is already installed. To initiate a task, complete the following steps:

1. Click **Updates > Windows** in the navigation tree.
2. Select the Fixlet that is relevant to the version of controller that you want to upgrade to.
   For example, **Updated Remote Control Controller for Windows is now available (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



A new version of the BigFix Remote Control Controller is now available!

The latest version of the BigFix Remote Control Controller provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Controllers on the targeted computers.

The Controller must not be running on the target computer.This fixlet fails with exit code 4 if the Controller is running.

- Click here to update BigFix Remote Control Controller for Windows.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the controller update on.
5. Click **OK**.

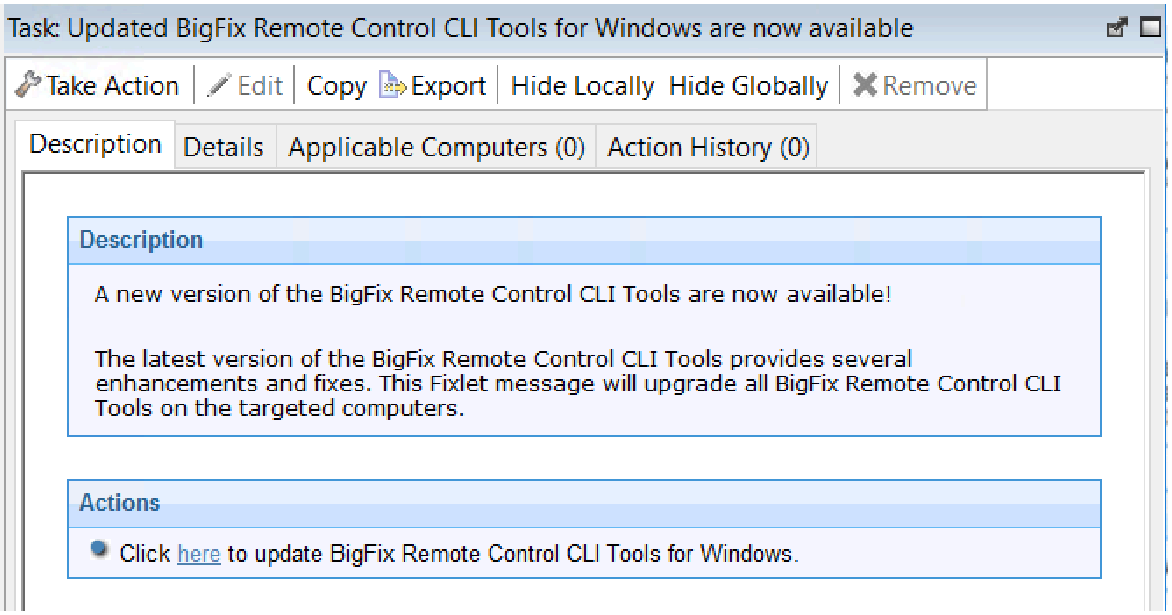
The summary screen shows the progress of the task.

The controller software on the selected targets is upgraded to the version of the chosen update.

Updating the Windows™ command line tools

Use the Windows™ operating system tasks to update the CLI tools, on a Windows™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the CLI tools configuration that is already installed. To initiate a task, complete the following steps:

1. Click **Updates > Windows** in the navigation tree.
2. Select the Fixlet that is relevant to the version of CLI tools that you want to upgrade to. For example, **Updated Remote Control CLI tools for Windows is now available! (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



Description

A new version of the BigFix Remote Control CLI Tools are now available!

The latest version of the BigFix Remote Control CLI Tools provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control CLI Tools on the targeted computers.

Actions

- Click here to update BigFix Remote Control CLI Tools for Windows.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the CLI update on.
5. Click **OK**.

The summary screen shows the progress of the task.

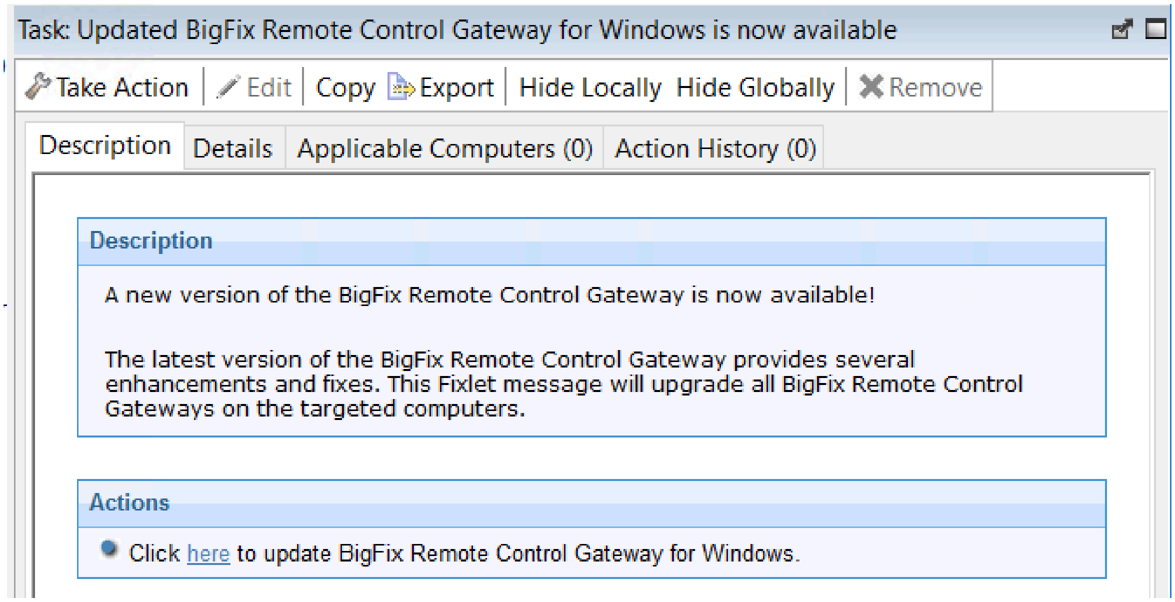
The CLI tools on the selected targets are upgraded to the version of the chosen update.

Updating the Windows™ gateway support

Use the Windows™ operating system tasks to update the gateway support files on a Windows™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the gateway configuration that is already installed.

To initiate a task, complete the following steps:

1. Click **Updates > Windows** in the navigation tree.
2. Select the Fixlet that is relevant to the version of gateway that you want to upgrade to. For example, **Updated Remote Control Gateway for Windows is now available! (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



Description

A new version of the BigFix Remote Control Gateway is now available!

The latest version of the BigFix Remote Control Gateway provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Gateways on the targeted computers.

Actions

● Click here to update BigFix Remote Control Gateway for Windows.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the gateway update on.
5. Click **OK**.

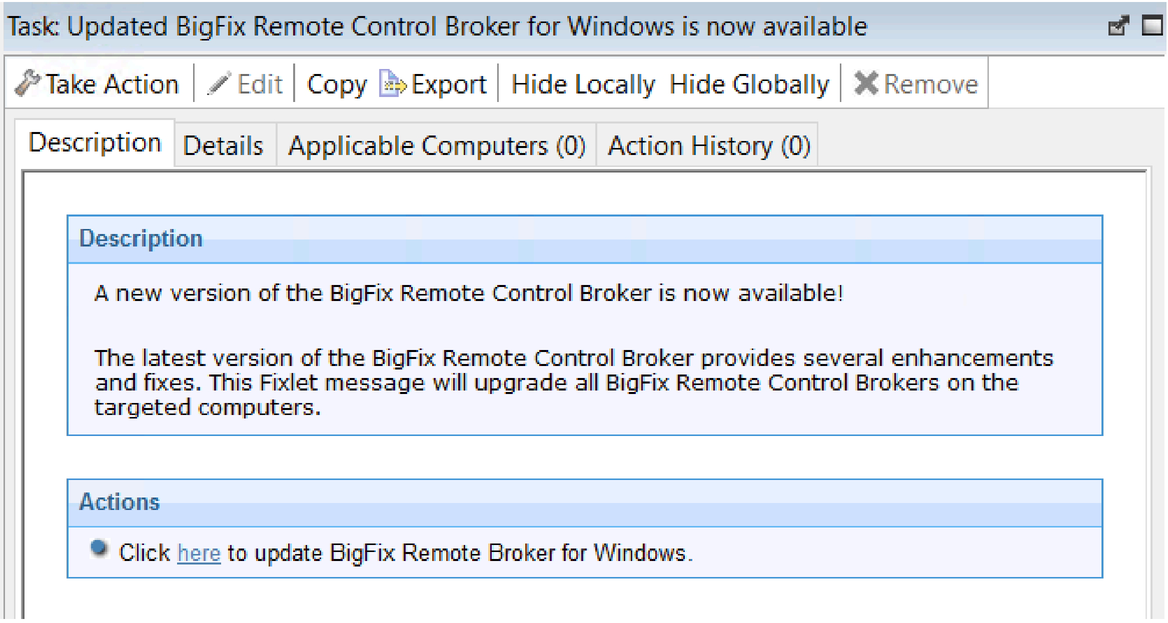
The summary screen shows the progress of the task.

The gateway support on the selected targets is upgraded to the version of the chosen update.

Updating the Windows™ broker support

Use the Windows™ operating system tasks to update the broker software, on a Windows™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the broker that is already installed. To initiate a task, complete the following steps:

1. Click **Updates > Windows** in the navigation tree.
2. Select the Fixlet that is relevant to the version of broker that you want to upgrade to.
   For example, **Updated Remote Control Broker for Windows is now available! (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



Description

A new version of the BigFix Remote Control Broker is now available!

The latest version of the BigFix Remote Control Broker provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Brokers on the targeted computers.

Actions

- Click here to update BigFix Remote Broker for Windows.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the broker update on.
5. Click **OK**.

The summary screen shows the progress of the task.

The broker software on the selected targets is upgraded to the version of the chosen update.

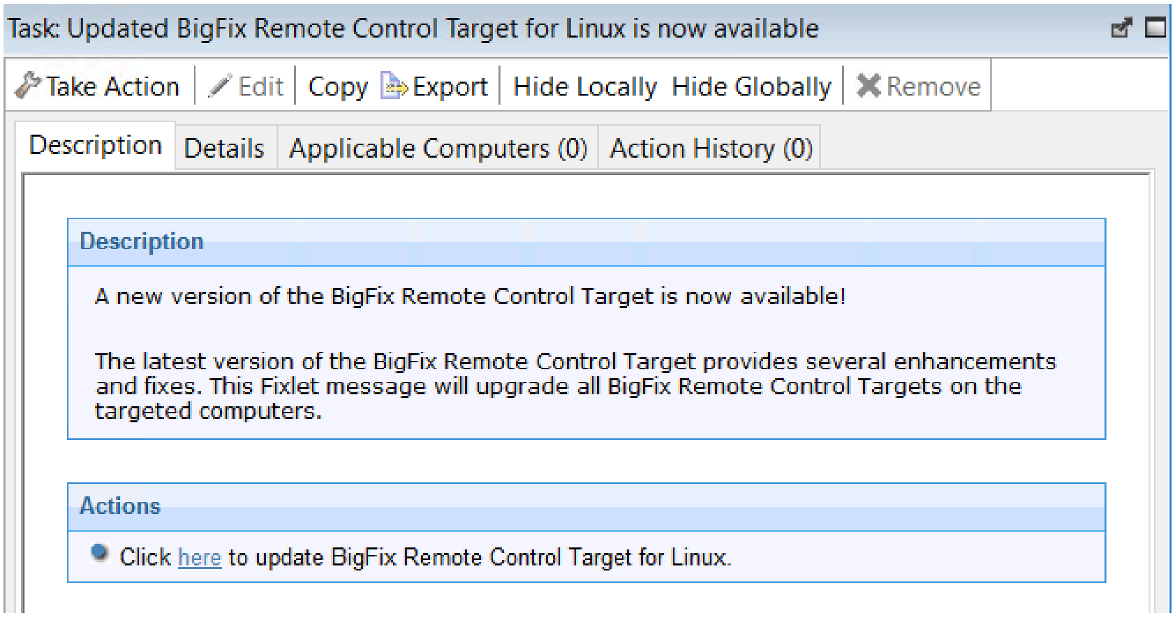
Update the Linux® components

The Linux® subnode provides the latest levels of Remote Control component software for use in a Linux® environment. These components contain the latest enhancements and fixes that are applied to Remote Control.

Updating the Linux™ target

Use the Linux™ tasks to update the target software, on a Linux™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the target configuration that is already installed. To initiate this task, complete the following steps:

1. Click **Updates > Linux** in the navigation tree.
2. Select the Fixlet that is relevant to the version of target that you want to upgrade to. For example, **Updated Remote Control Target for Linux is now available! (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



Task: Updated BigFix Remote Control Target for Linux is now available

Description

A new version of the BigFix Remote Control Target is now available!

The latest version of the BigFix Remote Control Target provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Targets on the targeted computers.

Actions

- Click here to update BigFix Remote Control Target for Linux.

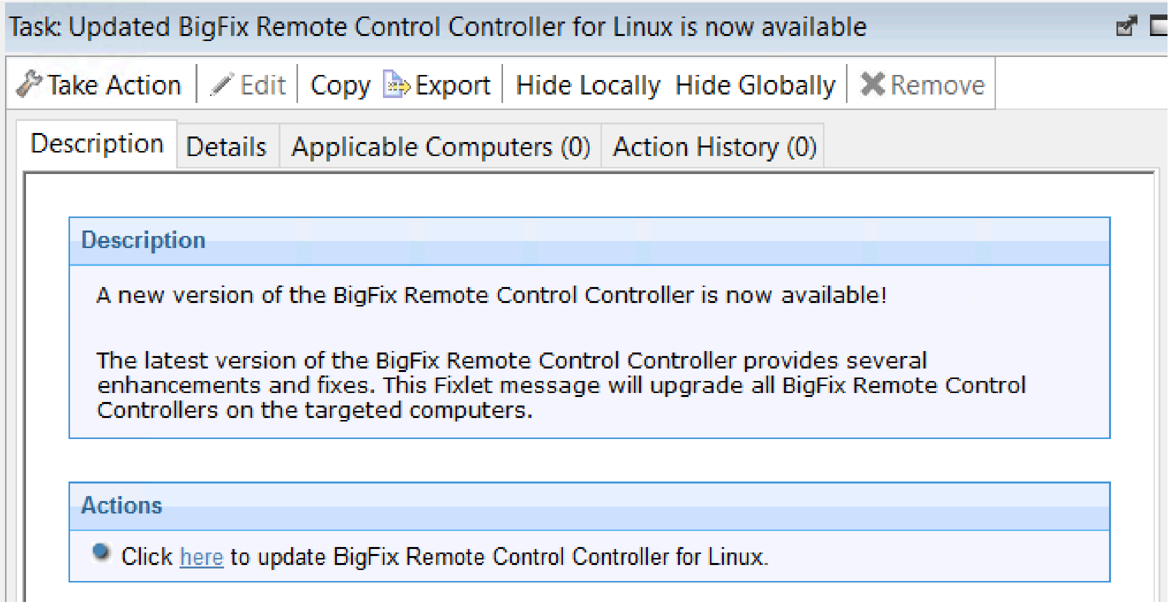
4. In the **Take Action** window on the Target tab, select the option for determining which targets to install the target update on.
5. Click **OK**.

The summary screen shows the progress of the task.

Updating the Linux™ controller

Use the Linux™ tasks to update the controller software, on a Linux™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the controller configuration that is already installed. To initiate a task, complete the following steps:

1. Click **Updates > Linux** in the navigation tree.
2. Select the Fixlet that is relevant to the version of controller that you want to upgrade to.
   For example, **Updated Remote Control Controller for Linux is now available (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



Task: Updated BigFix Remote Control Controller for Linux is now available

Description

A new version of the BigFix Remote Control Controller is now available!

The latest version of the BigFix Remote Control Controller provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Controllers on the targeted computers.

Actions

- Click here to update BigFix Remote Control Controller for Linux.

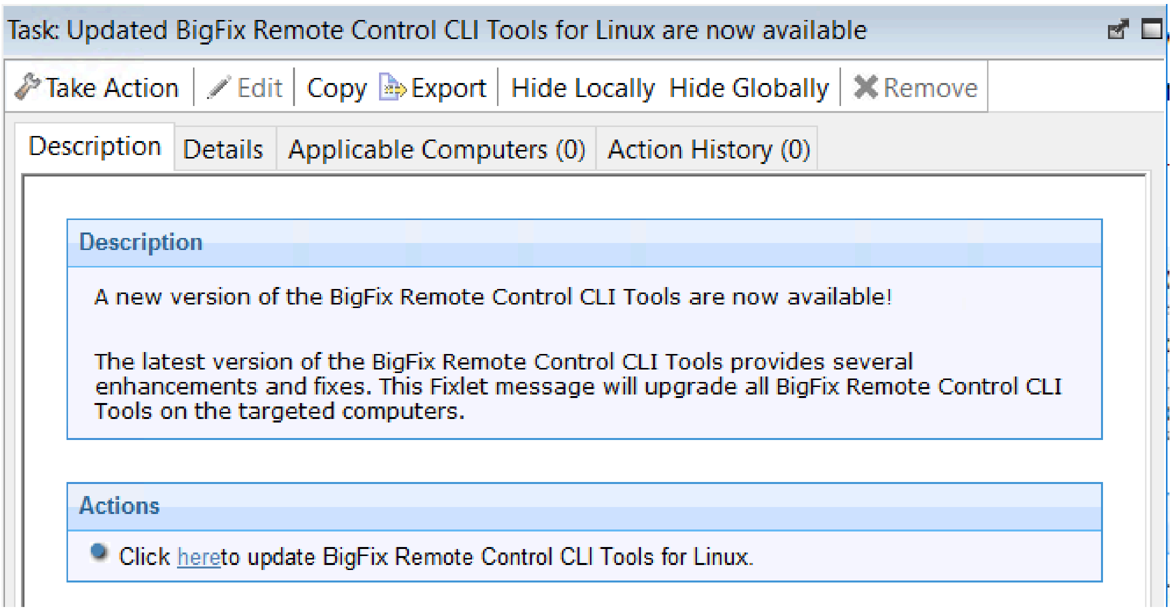
4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the controller update on.
5. Click **OK**.

The summary screen shows the progress of the task. The controller software on the selected targets is upgraded to the version of the chosen update.

Updating the Linux™ command line tools

Use the Linux™ tasks to update the CLI tools, on a Linux™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the CLI tools configuration that is already installed. To initiate this task, complete the following steps:

1. Click **Updates > Linux** in the navigation tree.
2. Select the Fixlet that is relevant to the version of CLI tools that you want to upgrade to. For example, **Updated Remote Control CLI tools for Linux is now available! (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



Task: Updated BigFix Remote Control CLI Tools for Linux are now available

Description

A new version of the BigFix Remote Control CLI Tools are now available!

The latest version of the BigFix Remote Control CLI Tools provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control CLI Tools on the targeted computers.

Actions

- Click hereto update BigFix Remote Control CLI Tools for Linux.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the CLI update on.
5. Click **OK**.

The summary screen shows the progress of the task.

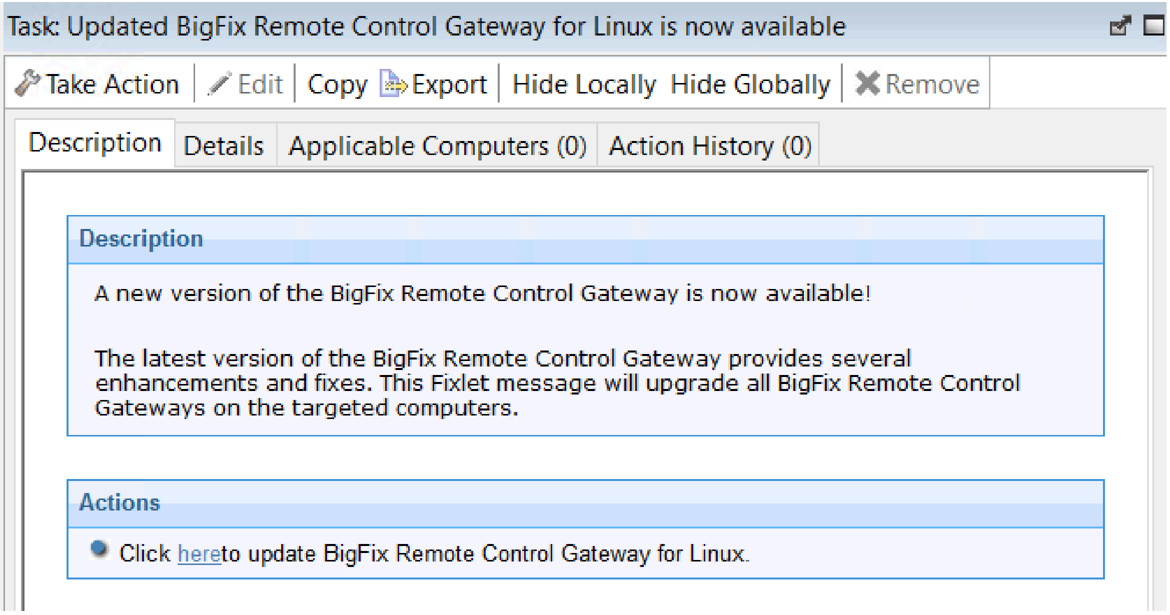
The CLI tools on the selected targets are upgraded to the version of the chosen update.

Updating the Linux™ gateway support

Use the Linux™ tasks to update the gateway support files, on a Linux™ computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the gateway configuration that is already installed.

To initiate this task, complete the following steps:

1. Click **Updates > Linux** in the navigation tree.
2. Select the Fixlet that is relevant to the version of gateway that you want to upgrade to. For example, **Updated Remote Control Gateway for Linux is now available (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



Description

A new version of the BigFix Remote Control Gateway is now available!

The latest version of the BigFix Remote Control Gateway provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Gateways on the targeted computers.

Actions

- Click hereto update BigFix Remote Control Gateway for Linux.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the gateway update on.
5. Click **OK**.

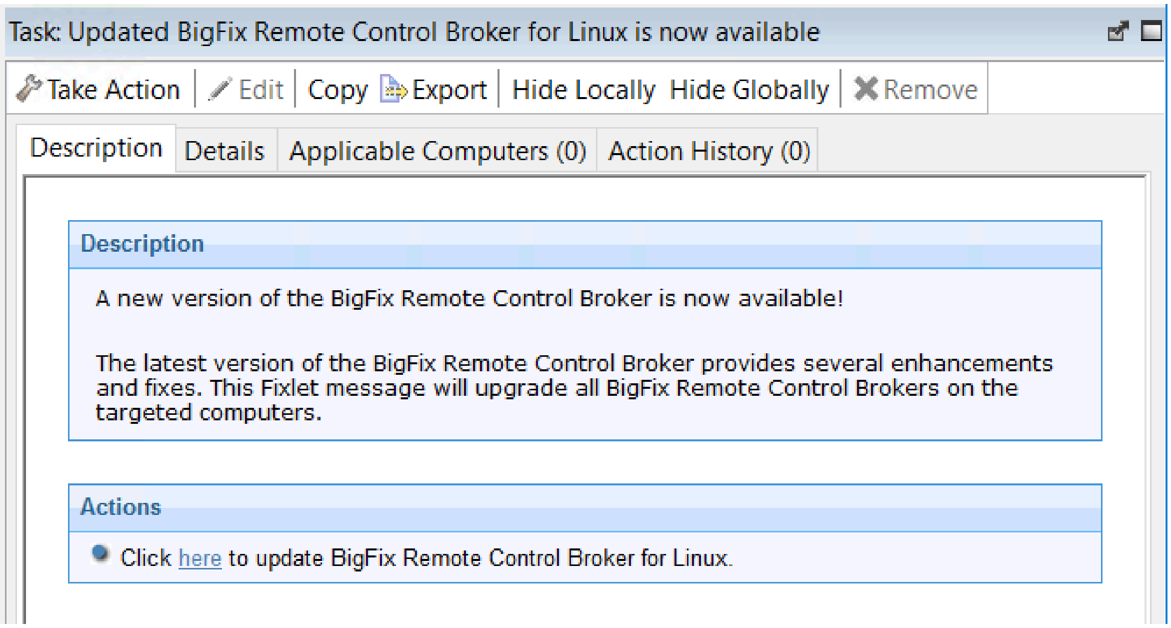
The summary screen shows the progress of the task.

The gateway support on the selected targets is upgraded to the version of the chosen update.

Updating the Linux® broker support

You can use the Linux tasks to update the broker software, on a Linux® computer. These tasks apply any new enhancements and fixes that are included in the chosen version to the broker configuration that is already installed. To initiate this task, complete the following steps:

1. Click **Updates > Linux** in the navigation tree.
2. Select the Fixlet that is relevant to the version of broker that you want to upgrade to.
   For example, **Updated Remote Control Broker for Linux is now available (Version 10.x.x)**.
3. In the **Task** window, review the description and follow the instructions in the Actions box to initiate the task.



A new version of the BigFix Remote Control Broker is now available!

The latest version of the BigFix Remote Control Broker provides several enhancements and fixes. This Fixlet message will upgrade all BigFix Remote Control Brokers on the targeted computers.

● Click here to update BigFix Remote Control Broker for Linux.

4. In the **Take Action** window on the Target tab, select the relevant option for determining which targets to install the broker update on.
5. Click **OK**.

The summary screen shows the progress of the task.

The broker software on the selected targets is upgraded to the version of the chosen update.

Download the Remote Control server component

You can run a Fixlet to download the Remote Control server installer file to a specific location on selected computers.

Downloading the Remote Control server installer file for Windows

Download the Remote Control server installer file for Windows by running a Fixlet in the BigFix® console.

To download the `trc_server_setup.exe` file, complete the following steps:

1. In the navigation tree click **Deployment > Windows**.
2. Select the **Download Remote Control Server for Windows** task.
3. Review the information in the **Description** tab.
4. Follow the instructions in the **Actions** field to download the installer file.
5. Enter a location to save the installer file to and click **OK**.

The `trc_server_setup.exe` file is downloaded to the selected computers. For more information about installing the server, see the *BigFix® Remote Control Installation Guide*.

Downloading the Remote Control server installer file for Linux

Download the Remote Control server installer file for Linux by running a fixlet in the BigFix® console.

To download the `trc_server_setup.bin` file, complete the following steps.

1. In the navigation tree click **Deployment > Linux** .
2. Select the **Download Remote Control Server for Linux** task.
3. Review the information in the **Description** tab.
4. Follow the instructions in the **Actions** field to download the installer file.
5. Enter a location to save the installer file to and click **OK**.

The `trc_server_setup.bin` file is downloaded to the selected computers. For more information about installing the server, see the *BigFix® Remote Control Installation Guide*.

Start a remote control session

The Remote Control controller and target components can be used to establish remote connections between each other to monitor or control the target system.

There are two types of remote control session: a peer-to-peer session that is made directly between the target and controller and a managed session that is initiated from the Remote Control server. For more information about the types of session, see Definition of terms that are used in Remote Control *(on page 8)*.

For more information about how to end a remote control session, see the *BigFix® Remote Control Controller User's Guide*.

Start a peer-to-peer session

There are two ways to start a peer-to-peer remote control session between a controller and a target.

- From the BigFix® console
- By using the controller component

Starting a peer-to-peer session from the BigFix® console

Use the BigFix® console to start a peer-to-peer session directly from the console. Use the menu option that displays when you right-click the target computer that you want to start a session with.

Note:

1. To start a remote control session from the BigFix® console, you must install the controller component on the same computer as the console is installed on. However, when the controller is deployed, only the current user who is logged on to the controlling computer, has the rights to see the menu item

to start a session. The menu item is not visible to other users. For more information, see Frequently asked questions *(on page 108)* .

2. For the menu item to be enabled, the **Remote Control Installation and Security Options** Analysis must be active for the selected computer. The Analysis must be reporting that the Remote Control target is active.

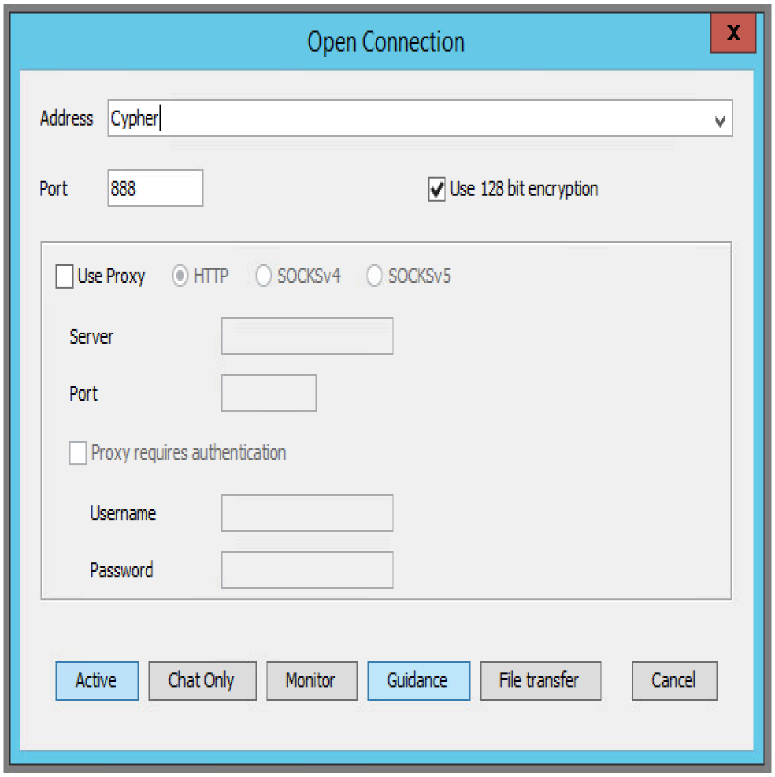
To start a peer-to-peer session, complete the following steps:

1. From the list of target computers, right-click the target that you want to start a remote control session with.
2. Select **Remote Control**.

   Note:

   a. This action can be carried out on any section of the console in which the list of computers is displayed.
   b. If an earlier version of the controller is installed, you might see IBM® Endpoint Manager for Remote Control as the menu item instead.

3. The Open connection window is displayed with the IP address or URL of the target that you want to connect to.



Open Connection

Address: Cypher

Port: 888

☑ Use 128 bit encryption

☐ Use Proxy ● HTTP ○ SOCKSv4 ○ SOCKSv5

Server:

Port:

☐ Proxy requires authentication

Username:

Password:

4. Select **Use proxy** if you are using a proxy. Select the relevant protocol and information.

   Server

The host name or IP address of the proxy server.

Port

The port that is required for the proxy server.

Proxy requires authentication

Select this option to authenticate with the proxy server. Provide a valid user name and password for authentication.

5. Select the session type.
   For more information about the session types that can be established, see the *BigFix® Remote Control Controller User's Guide*.

   Note:

   a. If a login window is displayed, enter a valid Windows operating system ID and password to continue.
   b. A user acceptance window might be displayed on the target, depending on the policies set on the target. The target user can accept or reject the session.

When the session is accepted and started, the policies values that are set locally on the target determine what actions can be carried out during the session. For more information about peer-to-peer sessions and the functions available in the controller UI, see the *BigFix® Remote Control Controller User's Guide*.

Starting a peer-to-peer session by using the controller

You can start a peer-to-peer session from any computers that you deploy the controller component on.

To start a peer-to-peer session by using the controller component, complete the following steps:

1. Start the controller

   Windows® systems

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

   Linux® systems

   To start the controller, locate the Remote Control controller application from the operating system application interface or run the following command:

   ```
   java jar /opt/bigfix/trc/controller/TRCConsole.jar
   ```

2. Follow from step 3 *(on page 55)* in Starting a peer-to-peer session from the BigFix console *(on page 54)* to start the session.

When the session is accepted and started, the policies values that are set locally on the target determine what actions can be carried out during the session. For more information about peer-to-peer sessions and the functions available in the controller UI, see the *BigFix® Remote Control Controller User's Guide*.

Start a server initiated remote control session

To start a remote control session initiated from the Remote Control server UI, the server component must be installed and running. For more information about creating and running server installation configurations tasks, see Creating Remote Control server installation tasks *(on page 58)*.

Note: The server can be installed also by using the installation files. For more information, see the *BigFix® Remote Control Installation Guide*.

After the server component is installed, use the *BigFix® Remote Control Controller User's Guide* for details about how to access and log on to the server UI. Remote control sessions that are initiated from the Remote Control server require permissions links to be set up. The links are made between the groups that the controller user and the target are members of. These permissions links determine what policies are effective for the session. For information about creating user and target groups, creating permissions links, and how policies are resolved for a remote control session, see the *BigFix® Remote Control Administrator's Guide*.

After you install the server and create the relevant groups and permissions links, you can start a remote control session by using the Remote Control server UI. For more information, see the *BigFix® Remote Control Controller User's Guide*.

Respond to warnings

During the discovery process, if issues are found that interfere with the normal operation of the Remote Control components, a **Warnings** node is displayed in the Remote Control navigation tree.

Note: If no issues are found during the discovery process, this node is not displayed in the navigation panel.

This node displays relevant Fixlets that you can use to resolve the issues on any applicable computers. When the Remote Control target software is installed, a default firewall rule is created to open the inbound Remote Control port. If the target operating system is blocking this port, use a Fixlet to add a rule to enable inbound TCP connections for Remote Control.

Note: The SUSE firewall Fixlet is not relevant when the firewall is started manually, it is only relevant when the firewall is in automatic mode.

Manage target and server configurations

Remote Control provides two wizards that you can use to create tasks to install Remote Control server or target configurations. These tasks can be run on all, or specific, servers, or targets.

Creating Remote Control server installation tasks

With the Remote Control **Server Installer Wizard**, you can create an installation task to install a remote control server.

Run the task on a Windows™® system or Linux™ (Red Hat and SUSE) systems to install a fully functional, self-contained Remote Control server with either of the following component setups:

- Remote Control server with WebSphere® Application Server Liberty Profile version and a Derby database.
- Remote Control server with WebSphere® Application Server Liberty Profile version and one of the following databases:
    - IBM DB2 11.5 Virtual Processor Core (VPC).
    - Oracle 11g, 12c, and 19c.

      When you use an Oracle database, if you are using the Oracle 11g drivers, set oracle.increment.keys.off=1 in the trc.properties file. Restart the server service.
    - Microsoft SQL server 2008, 2012, 2014, 2016, 2017, 2019, and 2022.

      You must use a JDBC driver whose version is higher than 6.3. Older versions do not support TLS1.2 or JRE8.

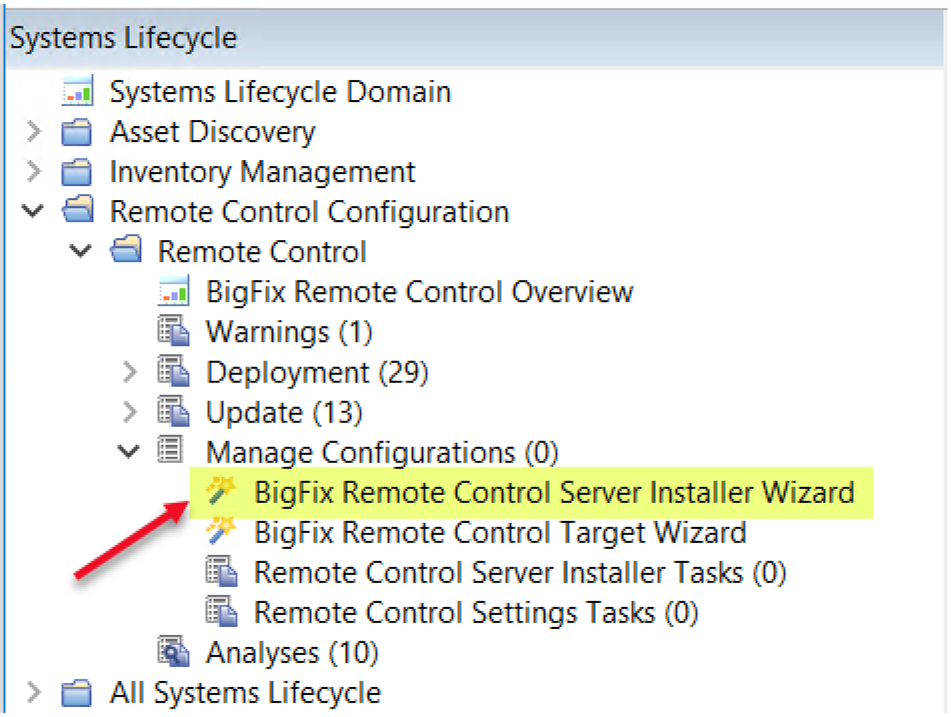
      When you use an MS SQL database, Windows™ authentication is not supported. You cannot log on with a domain user. You must use mixed mode authentication and create an SQL user to connect to the database.

Note:

1. If you choose the DB2®, MS SQL or Oracle database options, you must install the database and create a database instance before you run the server installation task.
2. If you are using DB2® 9.7 GA version, you must upgrade to DB2® 9.7 fix pack 1 due to a DB2® issue where NULL values are returned in generated key values.

To access the **Remote Control Server Installer Wizard**, complete the following steps:

1. In the Remote Control navigation tree, select **Manage Configurations > Remote Control Server Installer Wizard**.



Systems Lifecycle

- Systems Lifecycle Domain
- Asset Discovery
- Inventory Management
- Remote Control Configuration
    - Remote Control
        - BigFix Remote Control Overview
        - Warnings (1)
        - Deployment (29)
        - Update (13)
        - Manage Configurations (0)
            - BigFix Remote Control Server Installer Wizard
            - BigFix Remote Control Target Wizard
            - Remote Control Server Installer Tasks (0)
            - Remote Control Settings Tasks (0)
        - Analyses (10)
- All Systems Lifecycle

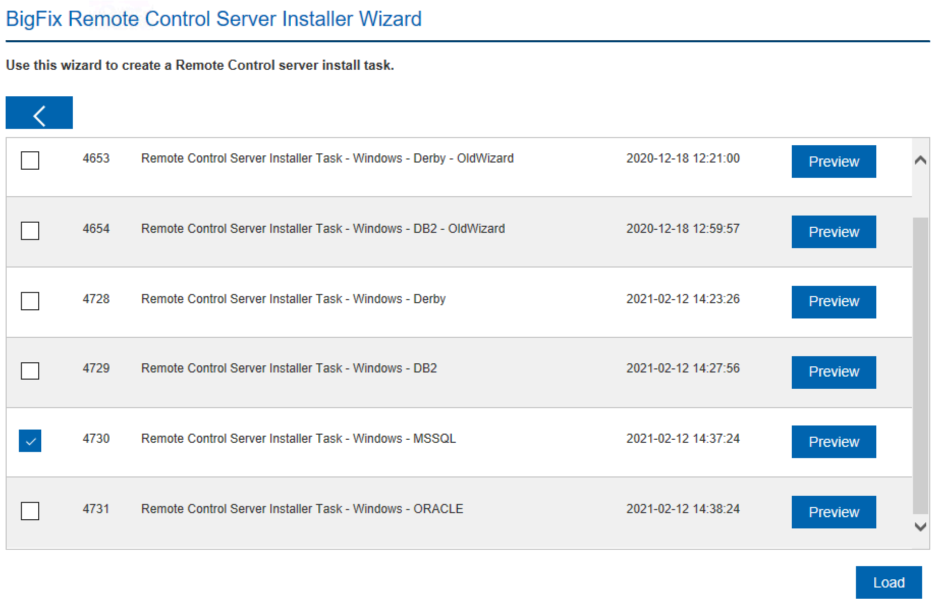
2. Set your configuration values by using one of the following options.

Load Settings from Existing Task

The wizard initially displays server configuration default values that you can change to your own requirements. To load previously saved settings, complete the following steps.

a. Click **Load Settings from Existing Task**.

b. On the **Wizard Fixlets** screen, select the task.


BigFix Remote Control Server Installer Wizard

Use this wizard to create a Remote Control server install task.

☐	4653	Remote Control Server Installer Task - Windows - Derby - OldWizard	2020-12-18 12:21:00	Preview
☐	4654	Remote Control Server Installer Task - Windows - DB2 - OldWizard	2020-12-18 12:59:57	Preview
☐	4728	Remote Control Server Installer Task - Windows - Derby	2021-02-12 14:23:26	Preview
☐	4729	Remote Control Server Installer Task - Windows - DB2	2021-02-12 14:27:56	Preview
☑	4730	Remote Control Server Installer Task - Windows - MSSQL	2021-02-12 14:37:24	Preview
☐	4731	Remote Control Server Installer Task - Windows - ORACLE	2021-02-12 14:38:24	Preview

c. Click **Load Wizard with Fixlet**. The configuration values are loaded into the wizard.

d. Follow the steps in Create a new configuration task *(on page 60)* to create a new configuration task.

Reset to default values

You can use this feature to clear any selections that are made and return the values in the wizard to the default configuration values.

Create a new configuration task

Follow the steps that are relevant to the database that you are using.

- Derby installation. For more information, see Creating a default server configuration *(on page 60)*
- DB2®. For more information, see Creating a DB2 server configuration *(on page 63)*
- MSSQL. For more information, see Creating an MS SQL server configuration *(on page 66)*
- Oracle. For more information, see Creating an Oracle server configuration *(on page 69)*

Creating a default server configuration

Use a default server configuration to install and use the embedded Derby database that is included as part of the Remote Control installation. The database is installed locally. To create a default installation task, complete the following steps:

1. Select the relevant operating system.
2. Enter the installation directory for the Remote Control server to be installed to or accept the default that is given.

Note: WebSphere® Application Server cannot be installed in a directory whose name contains non-English-language characters. This installation installs an embedded version of WebSphere® Application Server. Therefore, you must choose a destination for the installation files that does not contain any non-English-language characters.

3. Select **Derby** and enter the relevant database parameter values.

   Name of the database to use

   Specify the name for the database to be used with Remote Control server or accept the default that is given.

4. Enter the server installation parameter values.

   HTTPS as Default for Target URL

   Select this option for the target to use the HTTPS server URL to communicate with the server. The **enforce.secure.endpoint.callhome** and **enforce.secure.endpoint.upload** properties in the `trc.properties` file are also set to *true*. If not selected, the HTTP URL is used. Regardless of your selection, the **enforce.secure.web.access**, **enforce.secure.weblogon**, and **enforce.secure.alllogon** properties that enable HTTPS logon and access to the web portal, are all set to *True* by default. For more information about these properties, see the *BigFix® Remote Control Administrator's Guide*.The check box is selected by default on a new installation.

   Note: For HTTPS, you must use a fully qualified domain name in the **Address of the Websphere server** field.

   Use secure registration tokens to register targets

   Select this option to enable the secure target registration feature. This feature prevents unauthorized targets from registering with the Remote Control server. Ensure that the **HTTPS as Default for Target URL** option is also selected. For more information about secure registration, see Enable secure target registration. *(on page 103)*.

   Address of the WebSphere® server

   The fully qualified name for the Remote Control server. For example, `trcserver.example.com`.

   Note: Enter the fully qualified name. This name is used to create the URL in the `trc.properties` file that is passed to the target when it contacts the server for the first time. If the fully qualified name is incorrect, the target might be unable to contact the server successfully when it is next due to contact it.

   Web path of URL

   Specify the web path for the server URL, `http://trcserver.example.com/webpath`. For example, `trc`. `http://trcserver.example.com/trc`

HTTP port

Specify a port for the server. Default is 80.

HTTPS port

Specify a port if you are using SSL. Default is 443.

Administrator email

Specify an administrator email address. For example, `admin@company.com`

Note: To use the email function within the Remote Control server, a mail server must be installed. For more information about enabling email, see the *BigFix® Remote Control Installation Guide*.

Enable FIPS

Select to enable FIPS compliance on the server. For more information about enabling FIPS compliance, see the *BigFix® Remote Control Installation Guide*.

Enable TLS 1.3 Support

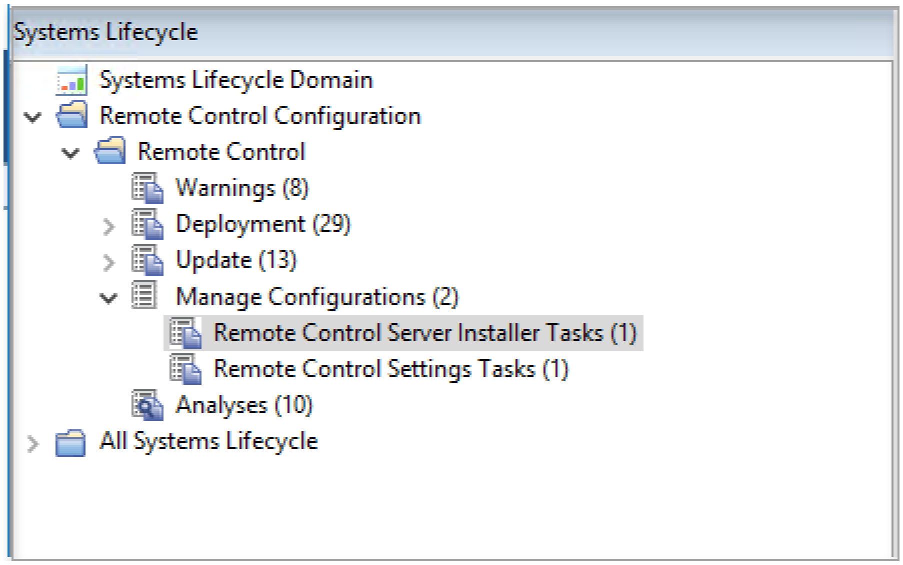
Select this option to enable the TLS 1.3 support. For more information about enabling TLS 1.3, see the *BigFix® Remote Control Installation Guide*.

Adjust some advanced web parameters

Select this option to set extra port values.

5. Save the configuration by completing the following steps:
   a. Click **Create Server Installation Task**
   b. Complete the relevant information for your task and click **OK**.

Your task is displayed in the list panel of the **Remote Control Server Installer Tasks** subnode.


Systems Lifecycle
Systems Lifecycle Domain
Remote Control Configuration
Remote Control
Warnings (8)
Deployment (29)
Update (13)
Manage Configurations (2)
Remote Control Server Installer Tasks (1)
Remote Control Settings Tasks (1)
Analyses (10)
All Systems Lifecycle

Creating a DB2® server configuration

You can create a server installation configuration that uses a DB2® database. You must install the database, either locally or remotely, and create a database instance before you install the Remote Control server.

Ensure that you set up the database before you create the task. For more information about setting up the database, see the *BigFix® Remote Control Installation Guide* and the chapter that describes Setting up the database.

To create a DB2® server configuration task, complete the following steps:

1. Select the relevant operating system.
2. Enter the installation directory for the Remote Control server to be installed to or accept the default that is given.
3. Select the relevant DB2® version and enter the relevant database parameters.

    Database server address

    The IP address or host name of your database server.

    Note: 127.0.0.1 can be used when DB2® is installed locally. If you install DB2® on a remote system, type the IP address of the remote system.

    Port on which to connect to the database

    Port on which DB2® is installed.

    Note:

    a. On Windows™® systems, the default port is 50000. On Linux™ systems, the default port is 50001.
    b. A remote DB2® installation is limited to type four connections. A local installation can use type two or four. For type two connections, set the port value to 0.

    Name of the Database to use

    Specify the name for the database to be used with the Remote Control server or accept the default that is given.

    Database Administrator Userid

    Specify the Administrator user ID that is used for logging on to the database. The user ID must have admin access to the database.

    Database Administrator Password

    Specify the Administrator password for connecting to the database.

    Path to the JDBC drivers

Specify the path to the DB2® JAR files, `db2jcc.jar`, and `db2jcc_license.jar`

Path to db2profile script

Specify the path to the db2profile for the DB2® instance. For example, `/home/db2inst1/sqllib/db2profile`

Note: This field is available only when you install in a Linux™ operating system and if you select to create the database.

Path to the DB2® libraries

Specify the path to the DB2® libraries. For example, `/home/db2inst1/sqllib/lib32`

Note: This field is available only when you install in a Linux™ operating system and if you select to create the database.

If Local, create the database

If DB2® is installed locally (127.0.0.1), you can select to create a blank database during the installation. You can also select to drop an existing local database and create a new database.

Note: Do not select create database or drop database if you are using a remote database.

If Local, drop an existing database

If DB2® is installed locally (127.0.0.1), you can select to drop the database and create a new one.

Note: Do not drop the database if you are using a remote database.

New database location (Drive name) / (Path name)

Specify the path where the database can be installed. If the installation is local and you select to create the database, the admin user who is specified must have the appropriate authority. On a Windows™ system, use the db2admin user, and on a Linux™ system, the user must be a member of the group db2grp1.

Note:

Linux™ systems

Specify a directory that the admin User ID has read and write permissions for.

Windows™ systems

Specify a drive letter.

4. Enter the server installation parameter values.

HTTPS as Default for Target URL

Select this option for the target to use the HTTPS server URL to communicate with the server. The **enforce.secure.endpoint.callhome** and **enforce.secure.endpoint.upload** properties in the `trc.properties` file are also set to *true*. If not selected, the HTTP URL is used. Regardless of your selection, the **enforce.secure.web.access**, **enforce.secure.weblogon**, and **enforce.secure.alllogon** properties that enable HTTPS logon and access to the web portal, are all set to *True* by default. For more information about these properties, see the *BigFix® Remote Control Administrator's Guide*.The check box is selected by default on a new installation.

Note: For HTTPS, you must use a fully qualified domain name in the **Address of the Websphere server** field.

Use secure registration tokens to register targets

Select this option to enable the secure target registration feature. This feature prevents unauthorized targets from registering with the Remote Control server. Ensure that the **HTTPS as Default for Target URL** option is also selected. For more information about secure registration, see Enable secure target registration. *(on page 103)*.

Address of the WebSphere® server

The fully qualified name for the Remote Control server. For example, `trcserver.example.com`.

Note: Enter the fully qualified name. This name is used to create the URL in the `trc.properties` file that is passed to the target when it contacts the server for the first time. If the fully qualified name is incorrect, the target might be unable to contact the server successfully when it is next due to contact it.

Web path of URL

Specify the web path for the server URL, `http://trcserver.example.com/`*`webpath`*. For example, `trc`. `http://trcserver.example.com/trc`

HTTP port

Specify a port for the server. Default is 80.

HTTPS port

Specify a port if you are using SSL. Default is 443.

Administrator email

Specify an administrator email address. For example, `admin@company.com`

> **Note:** To use the email function within the Remote Control server, a mail server must be installed. For more information about enabling email, see the *BigFix® Remote Control Installation Guide*.

Enable FIPS

Select to enable FIPS compliance on the server. For more information about enabling FIPS compliance, see the *BigFix® Remote Control Installation Guide*.

Enable TLS 1.3 Support

Select this option to enable the TLS 1.3 support. For more information about enabling TLS 1.3, see the *BigFix® Remote Control Installation Guide*.

Adjust some advanced web parameters

Select this option to set extra port values.

5. Save the configuration by completing the following steps:
    a. Click **Create Server Installation Task**
    b. Complete the relevant information for your task and click **OK**.

Creating an MS SQL server configuration

You can create a server installation configuration to use an MS SQL database. You must install the database, either locally or remotely, and create a database instance before you install the Remote Control server.

To create an MS SQL server configuration task, complete the following steps:

1. Select the relevant operating system.
2. Enter the installation directory for the Remote Control server to be installed to or accept the default that is given.
3. Select the relevant MS SQL version and enter the relevant database parameters.

Database server address

The IP address or host name of your database server.

> **Note:** 127.0.0.1 can be used when MS SQL is installed locally on a Windows™ system only.

Port on which to connect to the database

Port on which MS SQL is installed.

Name of the Database to use

Specify the name for the database to be used with the Remote Control server or accept the default that is given.

Database Administrator Userid

Specify the Administrator user ID used for logging on to the database. The user ID must have admin access to the database.

Database Administrator Password

Specify the Administrator password for connecting to the database.

Path to the JDBC drivers

Specify the path to the MS JDBC Java files. The `mssql-jdbc-X.X.X.jre8.jar` file must be used depending on the version of MS SQL database that you are using.

If Local, create the database

If MS SQL is installed locally, you can select to create a blank database during the installation.

If Local, drop an existing database

If MS SQL is installed locally, you can select to drop the database and create a new one. Do not select drop the database if you are using a remote database.

New database location (the directory must exist)

Specify the database installation path. If the installation is local and you select to create the database the Admin user must have appropriate authority to do so.

Linux™ systems.

Specify a directory that the admin User ID has read and write permissions for.

Windows™ systems.

Specify an existing directory.

4. Enter the server installation parameter values.

HTTPS as Default for Target URL

Select this option for the target to use the HTTPS server URL to communicate with the server. The **enforce.secure.endpoint.callhome** and **enforce.secure.endpoint.upload** properties in the `trc.properties` file are also set to *true*. If not selected, the HTTP URL is used. Regardless of your selection, the **enforce.secure.web.access**, **enforce.secure.weblogon**, and **enforce.secure.alllogon** properties that enable HTTPS logon and access to the web portal, are all set to *True* by default. For more information about these properties, see the *BigFix® Remote Control Administrator's Guide*.The check box is selected by default on a new installation.

Note: For HTTPS, you must use a fully qualified domain name in the **Address of the Websphere server** field.

Use secure registration tokens to register targets

Select this option to enable the secure target registration feature. This feature prevents unauthorized targets from registering with the Remote Control server. Ensure that the **HTTPS as**

Default for Target URL option is also selected. For more information about secure registration, see Enable secure target registration. *(on page 103)*.

Address of the WebSphere® server

The fully qualified name for the Remote Control server. For example, `trcserver.example.com`.

> **Note:** Enter the fully qualified name. This name is used to create the URL in the `trc.properties` file that is passed to the target when it contacts the server for the first time. If the fully qualified name is incorrect, the target might be unable to contact the server successfully when it is next due to contact it.

Web path of URL

Specify the web path for the server URL, `http://trcserver.example.com/webpath`. For example, `trc`. `http://trcserver.example.com/trc`

HTTP port

Specify a port for the server. Default is 80.

HTTPS port

Specify a port if you are using SSL. Default is 443.

Administrator email

Specify an administrator email address. For example, `admin@company.com`

> **Note:** To use the email function within the Remote Control server, a mail server must be installed. For more information about enabling email, see the *BigFix® Remote Control Installation Guide*.

Enable FIPS

Select to enable FIPS compliance on the server. For more information about enabling FIPS compliance, see the *BigFix® Remote Control Installation Guide*.

Enable TLS 1.3 Support

Select this option to enable the TLS 1.3 support. For more information about enabling TLS 1.3, see the *BigFix® Remote Control Installation Guide*.

Adjust some advanced web parameters

Select this option to set extra port values.

5. Save the configuration by completing the following steps:
    a. Click **Create Server Installation Task**
    b. Complete the relevant information for your task and click **OK**.

Creating an Oracle server configuration

You can create a server installation configuration to use an Oracle database. You must install the database, either locally or remotely, and create a database instance before you install the Remote Control server.

To create an Oracle server configuration task, complete the following steps:

1. Select the relevant operating system.
2. Enter the installation directory for the Remote Control server to be installed to or accept the default that is given.
3. Select the relevant Oracle version and enter the relevant database parameters.

   Database server address

   The IP address or host name of your database server. 127.0.0.1 can be used when Oracle is installed locally. If you install Oracle on a remote system, type in the IP address of the remote system.

   Port on which to connect to the database

   Port on which Oracle is installed.

   Name of the Database to use

   Specify a name for the database. The name is the SID name on the server, not the one in `tnsnames.ora`. For example, `TRCDB`.

   Database Administrator Userid

   Specify the administrator user ID that is used for logging on to the database. The user ID must have admin access to the database.

   Note: For an Oracle installation, a user that is called **asset** must exist. This user ID can be used here or use an existing or new user.

   Database Administrator Password

   Specify the Administrator password for connecting to the database.

   Path to the JDBC drivers

   Specify the path to the oracle Java™ JDBC library. The location can be obtained from the Oracle server installation or downloaded from the Oracle website. For example, `c:\oracle\ora92\jdbc\lib\ojdbc14.jar`

4. Enter the server installation parameter values.

   HTTPS as Default for Target URL

   Select this option for the target to use the HTTPS server URL to communicate with the server. The **enforce.secure.endpoint.callhome** and **enforce.secure.endpoint.upload** properties in the `trc.properties` file are also set to *true*. If not selected, the HTTP URL is used. Regardless of your selection, the **enforce.secure.web.access**, **enforce.secure.weblogon**, and

enforce.secure.alllogon properties that enable HTTPS logon and access to the web portal, are all set to *True* by default. For more information about these properties, see the *BigFix® Remote Control Administrator's Guide*.The check box is selected by default on a new installation.

Note: For HTTPS, you must use a fully qualified domain name in the **Address of the Websphere server** field.

Use secure registration tokens to register targets

Select this option to enable the secure target registration feature. This feature prevents unauthorized targets from registering with the Remote Control server. Ensure that the **HTTPS as Default for Target URL** option is also selected. For more information about secure registration, see Enable secure target registration. *(on page 103)*.

Address of the WebSphere® server

The fully qualified name for the Remote Control server. For example, `trcserver.example.com`.

Note: Enter the fully qualified name. This name is used to create the URL in the `trc.properties` file that is passed to the target when it contacts the server for the first time. If the fully qualified name is incorrect, the target might be unable to contact the server successfully when it is next due to contact it.

Web path of URL

Specify the web path for the server URL, `http://trcserver.example.com/`*`webpath`*. For example, `trc`. `http://trcserver.example.com/trc`

HTTP port

Specify a port for the server. Default is 80.

HTTPS port

Specify a port if you are using SSL. Default is 443.

Administrator email

Specify an administrator email address. For example, `admin@company.com`

Note: To use the email function within the Remote Control server, a mail server must be installed. For more information about enabling email, see the *BigFix® Remote Control Installation Guide*.

Enable FIPS

Select to enable FIPS compliance on the server. For more information about enabling FIPS compliance, see the *BigFix® Remote Control Installation Guide*.

Enable TLS 1.3 Support

Select this option to enable the TLS 1.3 support. For more information about enabling TLS 1.3, see the *BigFix® Remote Control Installation Guide*.

Adjust some advanced web parameters

Select this option to set extra port values.

5. Save the configuration by completing the following steps:
    a. Click **Create Server Installation Task**
    b. Complete the relevant information for your task and click **OK**.

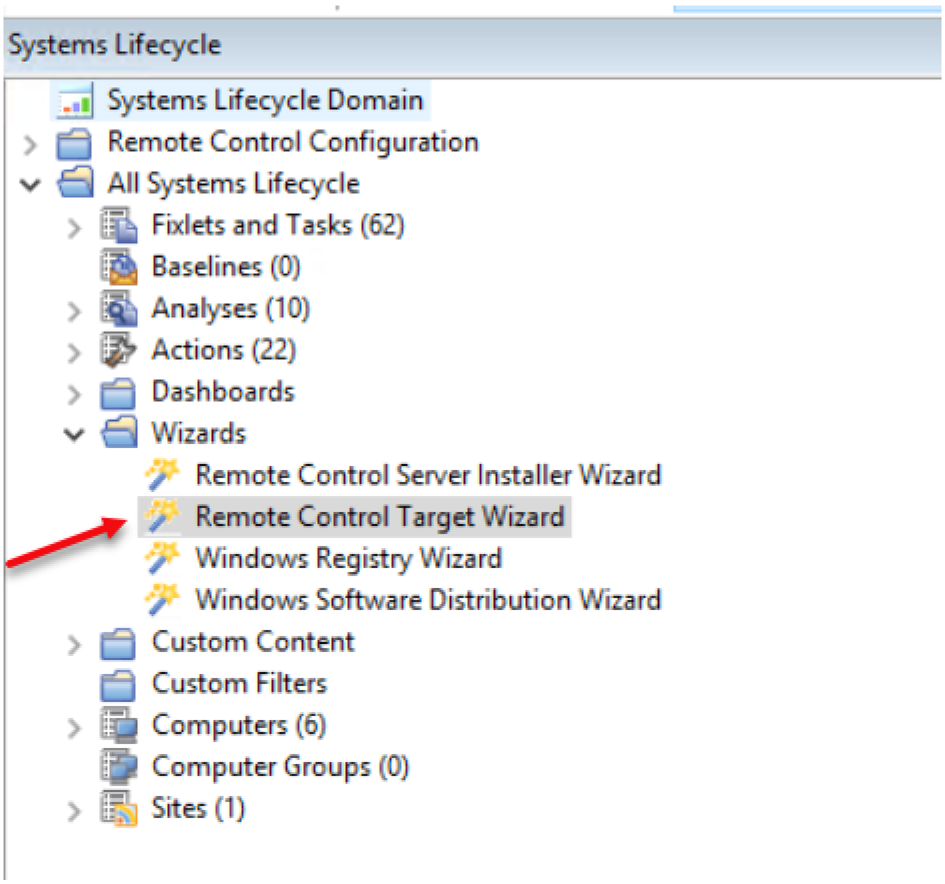
Creating Remote Control target configuration tasks

Use the Remote Control Target wizard to create a set of target configuration parameters.

Run a task to apply the parameters to all targets or selected targets that have the Remote Control target software already installed. The configurations determine what types of session the targets can take part in and the actions that can be carried out by the controller user during a remote control session. For more information about the options, see the *BigFix® Remote Control Installation Guide*. To create a configuration task, complete the following steps:

Note: The configuration values set here are only in effect when a peer-to-peer session is requested with a target. If a remote control session is started from the Remote Control server, the session policies are passed to the target from the server.

In the Remote Control navigation tree, select **Manage Configurations > Remote Control Target Wizard**.

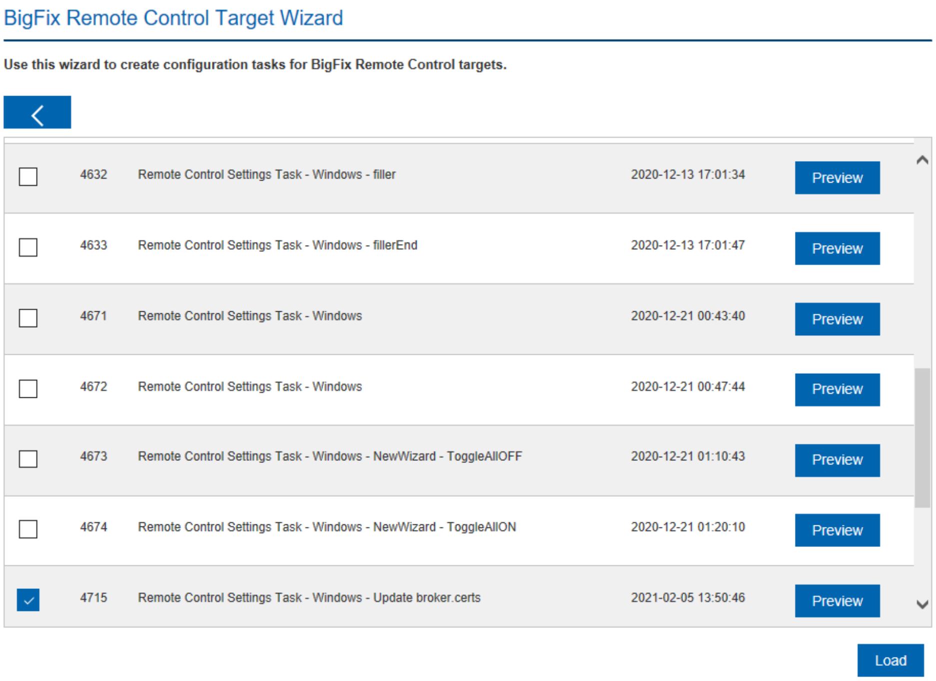


1. Select the relevant operating system.
2. Set your configuration values.

   Load settings from an existing task

   Use this feature to load previously created configuration settings.

   a. Click **Load settings from an existing task**.
   b. On the **Wizard Fixlets** panel, select the task.



BigFix Remote Control Target Wizard

Use this wizard to create configuration tasks for BigFix Remote Control targets.

□	4632	Remote Control Settings Task - Windows - filler	2020-12-13 17:01:34	Preview
□	4633	Remote Control Settings Task - Windows - fillerEnd	2020-12-13 17:01:47	Preview
□	4671	Remote Control Settings Task - Windows	2020-12-21 00:43:40	Preview
□	4672	Remote Control Settings Task - Windows	2020-12-21 00:47:44	Preview
□	4673	Remote Control Settings Task - Windows - NewWizard - ToggleAllOFF	2020-12-21 01:10:43	Preview
□	4674	Remote Control Settings Task - Windows - NewWizard - ToggleAllON	2020-12-21 01:20:10	Preview
☑	4715	Remote Control Settings Task - Windows - Update broker.certs	2021-02-05 13:50:46	Preview

Click **Load Wizard with Fixlet**. The configuration values are loaded into the wizard.

Reset to default values

Use this feature to clear any selections that are made and return the values in the wizard to the default configuration values.

Selecting configuration values

The wizard is loaded with default configuration values that you can change to your own requirements by selecting or clearing the relevant options.

Note: Depending on the selected operating system, all or some of the following properties are displayed.

Table 1. Installation option descriptions

Installation option	Target property	Default Value	Description
Server URL	ServerURL	blank	For the target to register with the server and take part in remote control sessions that are started from the server, provide the Remote Control server url in the format: `http://servername/trc`, where *servername* is the fully qualified name of theRemote Control server. For example, `http://trcserver.example.com/trc`.

Installation option	Target property	Default Value	Description
			Note: ◦ For the targets to take part only in remote control sessions that are started from the server, if you provide a server url, select **never** for **Allow peer-to-peer mode**. ◦ *If the Remote Control server has been installed with a custom URL which is not ending with /trc (e.g. https://my.rcserver/trccustom), you need to specify the ServerURL with the /trc at the end (e.g. https://my.rcserver/trc) so that the field is correctly validated then once that the Fixlet has been generated you need to manually edit the URL in the ActionScript. For example the line "ServerURL"="https://my.rcserver/trc" will be replaced with the line "ServerURL"="https://my.rcserver/trccustom".*
Proxy URL	ProxyURL	blank	Host name or IP address for a proxy server, if you are using one.
Broker List	BrokerList	blank	The list of host names or IP addresses of the brokers and their ports, that you want the target to connect to. Enter in the following format, **hostname1:port,hostname2:port,hostname3:port.**
Trusted certificates for Broker connections		n/a	Select this option to configure the truststore that is used for verifying broker certificates. To add a certificate, complete the following steps. a. Open the certificate file in a text editor. b. Select the certificate and copy it to the clipboard. **Note:** You must select everything and include the BEGIN CERTIFICATE and END CERTIFICATE lines. c. Click **Save**.
Register target in group	GroupLabel	blank	Enter a target group name that the target is made a member of when the configuration is applied. This target group must exist in the Remote Control database. **Note:** The **GroupLabel** property can be used only if the target is not already registered with the server. If the target is already registered, it is not assigned to the target group. The **allow.target.group.override**

Installation option	Target property	Default Value	Description
			property in the `trc.properties` file on the server must be set to true for the **GroupLabel** property value to be applied.
Remote Control port	PortToListen	888	Specify the TCP port that the target listens on.
Allow peer-to-peer mode	AllowP2P	Never	Used to enable peer-to-peer mode. **Never** A peer-to-peer session cannot be established between a controller and this target. If a **ServerURL** is provided, the targets can take part only in remote control sessions that are initiated from the server. **Only if server is unreachable.** A peer-to-peer session can be established between a controller user and this target only when the Remote Control server is down or unreachable. **Always** A peer-to-peer session can be established between a controller user and this target. **Note:** If this option is selected and a server url is provided, the targets can take part in both peer-to-peer sessions and sessions that are initiated from the server.
FIPS compliance	FIPSCompliance	not selected	Select this option to enable the use of a FIPS-certified cryptographic provider for all cryptographic functions. For more information about enabling FIPS compliance, see the *BigFix® Remote Control Installation Guide*. **Note:** If you enable FIPS compliance on the target, also enable FIPS compliance on the controller components that are installed. Only the IBM® Java™ Run-time Environment (JRE) is supported in FIPS-compliant mode and the JRE is installed when you install the controller software. To enable FIPS compliance on the controller, complete the following steps.

Installation option	Target property	Default Value	Description

			a. Edit the `trc_controller.cfg` file on the system that the controller is installed on.
			Windows® systems
			`[controller installation dir]\trc_controller.cfg`
			where *[controller installation dir]* is the directory that the controller is installed in.
			Linux® systems
			`opt/bigfix/trc/controller/trc_controller.cfg`
			b. Set the **fips.compliance** property to true and save the file.

Enable NIST SP800-131A compliance (Enables FIPS)	SP800131A-Compliance	not selected	Select this option to enforce NIST SP800-131A-compliant algorithms and key strengths for all cryptographic functions. For more information about enabling NIST SP800-131A compliance, see the *BigFix® Remote Control Installation Guide*. **Note:** If you enable NIST SP800-131A compliance on the target, also enable NIST SP800-131A compliance on the controller components that are installed. Only the IBM® Java™ Run-time Environment (JRE) is supported in NIST SP800-131A compliant mode and the JRE is installed when you install the controller software. To enable NIST SP800-131A compliance on the controller, complete the following steps. a. Edit the `trc_controller.cfg` file on the system that the controller is installed on. **Windows® systems** `[controller installation dir]\trc_controller.cfg` where *[controller installation dir]* is the directory that the controller is installed in. **Linux® systems**

Installation option	Target property	Default Value	Description
			`opt/bigfix/trc/controller/trc_controller.cfg` b. Set the **sp800131A.compliance** property to true and save the file.
Disable IPv6	Disable IPv6	not selected	Prevent the target from using IPv6 addresses.
Disable IPv4	Disable IPv4	not selected	Prevent the target from using IPv4 addresses.
Accessibility	Accessibility	not selected	Select this option to enable the accessibility UI. Available when you select **Windows** as the operating system.
Log Level	LogLevel	2	The log level determines the types of entries and how much information is added to the log file. Default value is 2. 0 - Logging is set to a minimal level. 1 - Logging is set to **ERROR** level. 2 - Logging is set to **INFO** level. 4 - Logging is set to **DEBUG** level. **Note:** Use Log Level = 4 only by request from HCL support.
Log Rollover	LogRollover	Daily	Controls the period after which a new log file is started. This period must be shorter than the LogRotation period, therefore not all combinations are valid. LogRollover cannot be disabled. Default value is Daily. **Hourly** Start a new log file on the hour. Recommended if the log is written to frequently or when you use a log level higher than 2.

Installation option	Target property	Default Value	Description
			Daily Start a new log file every day.
Log Rotation	LogRotation	Weekly	Controls the period after which an older log file is overwritten. Log rotation can be disabled. Default value is Weekly. **Daily** Overwrite log files after 1 day. When LogRollover is set to Hourly, the suffix that is added to the log file name is 00H to 23H. **Weekly** Overwrite log files after 1 week. When LogRollover is set to Hourly, the suffix that is added to the log file name specifies the day and hour. Value can be Mon-00H to Sun-23H. When LogRollover is set to Daily, the suffix that is added to the log file name specifies the day. The value can be Mon to Sun. **Monthly** Overwrite log files after 1 month. 01-00H to 31-23H. When LogRollover is set to Hourly, the suffix that is added to the log file name specifies the numeric day of the month and the hour. Value can be 01-00H to 31-23H. When LogRollover is set to Daily, the suffix that is added to the log file name specifies the numeric day of the month. The value can be 01 - 31. **Disabled** LogRotation is disabled. When LogRollover is set to hourly, the suffix that is added to the log file name specifies the current date and time. Value can be YYYY-MM-DD-hh. When LogRollover is set to Daily, the suffix that is added to the log file name specifies the current date. The value can be YYYY-MM-DD.

Table 2. Session option descriptions.

User options	Target property	Default Value	Description
Allow monitor mode	AllowMonitor	selected	Determines whether the target can take part in monitor peer-to-peer sessions. For details of the different types of remote control session that can be established, see the *BigFix® Remote Control Controller User's Guide*. **selected** The target can take part in monitor peer-to-peer sessions. The Monitor option is available for selection in the session type list in the controller window. The Open connection window also lists a Monitor option. **not selected** The target cannot take part in monitor peer-to-peer sessions. The Monitor option is not available in the session type list in the controller window.
Allow guidance mode	AllowGuidance	selected	Determines whether the target can take part in guidance peer-to-peer sessions. **selected** The target can take part in guidance peer-to-peer sessions. The Guidance option is available in the session type list in the controller window. The Open connection window also lists a Guidance option. **not selected** The target cannot take part in guidance peer-to-peer sessions. The Guidance option is not available in the session type list in the controller window.
Allow active mode	AllowActive	selected	Determines whether the target can take part in active peer-to-peer sessions. **selected** The target can take part in active peer-to-peer sessions. The Active option is available in the session type list in the controller window. The Open connection window also lists an Active option. **not selected** The target cannot take part in active peer-to-peer sessions. The Active option is not available in the session type list in the controller window.
Disable chat	DisableChat	not selected	Determines the ability to start a chat session with the target and also chat to the controller user during a peer-to-peer session. **selected**

User options	Target property	Default Value	Description
			If **Chat Only** is chosen as the connection type on the open connection screen, the session is refused. During the session, the chat icon is not available in the controller window. **not selected** A Chat Only session can be initiated from the open connection window. During the session, the chat icon is available in the controller window.
Disable file transfer to Controller	DisableFile-Pull	not selected	Determines the ability to transfer files from the target to the controller during the session. **selected** Files can be transferred from the target to the controller. **not selected** Files cannot be transferred from the target to the controller.
Disable file transfer to Target	DisableFile-Push	not selected	Determines the ability to transfer files from the controller to the target during the session. **selected** Files can be transferred from the controller to the target. **not selected** Files cannot be transferred from the controller to the target.
Disable clipboard transfer	DisableClip-board	not selected	Determines the availability of the clipboard transfer menu. Use the menu to transfer the clipboard content between the controller and target during a remote control session. **selected** The clipboard transfer menu is available during the session to transfer the clipboard content to and from the target. **not selected** The clipboard transfer menu is not available during the session.
Allow local recording	Allow-Recording	selected	The controller user can make and save a local recording of the session in the controlling system. **selected** The record option is available in the controller window. **not selected**

User options	Target property	Default Value	Description
			The record option is not available in the controller window.
Allow collaboration	AllowCollaboration	selected	Use this property to allow more than one controller to join a session. Determines the availability of the collaboration icon on the controller window. **selected** The collaboration icon is available in the controller window. **not selected** The collaboration icon is not available in the controller window.
Allow handover	AllowHandover	selected	The master controller, in a collaboration session, can hand over control of the session to a new controller. Determines the availability of the **Handover** button on the collaboration control panel. **selected** The **Handover** button is displayed in the collaboration control panel. **not selected** The **Handover** button is not displayed in the collaboration control panel.
Allows requests to disconnect session	AllowForceDisconnect	not selected	Determines whether a **Disconnect session** button is available in the message window that is displayed when you attempt to connect to the target. You can use the **Disconnect session** option to disconnect the current session. **selected** The disconnect button is displayed in the message window. **not selected** The disconnect button is not displayed in the message window.
Disconnect grace time	ForceDisconnectTimeout	45	Number of seconds you must wait for the current controller to respond to the prompt to disconnect the current session. If they do not respond in the time that is given, they are automatically disconnected from the session. The timer takes effect only when **AllowForceDisconnect** and **CheckUserLogin** are set to Yes. The default value is 45.
Connect at logon	AutoWinLogon	selected	Determines whether a session can be started when no users are logged on at the target. **selected** Session is started with the target.

User options	Target property	Default Value	Description
			not selected Session is not started and the following message is displayed. `Session rejected because there is no user logged to confirm the session`
Run pre-session script	RunPreScript	not selected	Determines whether a user-defined script is run before the remote control session starts. The script is run just after the session is allowed but before the controller user has access to the target. The outcome of running the script and the continuation of the session is determined by the value that is set for **Proceed on pre/post-script failure**. **selected** When a remote control session is requested, the defined script is run before the controller user has access to the target. **not selected** No script is run before the session. For more information about setting up pre and post session scripts, see the *BigFix® Remote Control Administrator's Guide*.
Run post-session script	RunPostScript	not selected	Determines whether a user-defined script is run after the remote control session finishes. **selected** When a remote control session ends, the user-defined script is run. **not selected** No script is run after the session. For more information about setting up pre and post session scripts, see the *BigFix® Remote Control Administrator's Guide*.
Proceed on pre/post-script failure	ProceedOnScriptFail	not selected	Action to take if the pre-script or post-script execution fails. A positive value or 0 is considered a successful run of the pre-script or post-session script. A negative value, a script that is not found, or not finished running within 3 minutes is considered a failure. **selected** If the pre-script or post-script run fails, the session continues. **not selected** If the pre-script or post-script run fails, the session does not continue and ends.
Reset console	Workaround-W2K3RDP	Not selected	Automatically reset the console after a Remote Desktop console session. When a Remote Desktop user uses the **/admin** or **/console** option to start a Remote Desktop session with a Windows® Server 2003 system and a user starts a remote control session with this target before, during or after the Remote Desktop session, remote control is unable to capture the

User options	Target property	Default Value	Description
after RDP console session			display. The result is that a gray screen is shown in the controller. This issue is a limitation in Windows® Server 2003 operating systems. Therefore, this property introduces a workaround that will reset the Windows® session either after each Remote Desktop session ends, or before a remote control session starts, depending on the value selected. **0** The workaround is disabled. This value is the default value. **1** Reset the session automatically when a remote control session is started. **Note:** The Windows® session takes a couple of minutes to initialize and the controller sees a blank desktop until the initialization is complete. A message informs the controller user that the session is being reset and it might take a few minutes. **2** Reset the session automatically when the Remote Desktop user logs out.
Follow Active Session	FollowActiveSession	Not selected	If selected, the controller connects to the active session in the target, even if this session is a Remote Desktop session. This feature is available in Remote Control v9.1.2 IF0002 and later versions and is supported on the following Microsoft™ Windows™ operating system versions: ◦ Microsoft™ Windows™ Vista ◦ Microsoft™ Windows™ 7 ◦ Microsoft™ Windows™ 8 ◦ Microsoft™ Windows™ 8.1 ◦ Microsoft™ Windows™ 10 This feature is not supported on any server edition of Microsoft™ Windows™.

Table 3. User acceptance option descriptions

User options	Target property	Default Value	Description
Confirm incom-	Confirm-	selected	Determines whether the acceptance window is displayed on the target, when a remote control session is requested. **selected**

User options	Target property	Default Value	Description
ing connections	TakeOver		The user acceptance window is displayed and the target user can accept or refuse the session. **not selected** The user acceptance window is not displayed and the session is established.
Confirm mode changes	ConfirmModeChange	selected	Determines whether the user acceptance window is displayed when the controller user selects a different session mode from the session mode list on the controller window. **selected** The user acceptance window is displayed each time a session mode change is requested and the target user must accept or refuse the request. **not selected** The user acceptance window is not displayed and the session mode is changed automatically.
Confirm file transfers	ConfirmFileTransfer	selected	Determines whether the user acceptance window is displayed when the controller user selects to transfer files between the target and the controller. **selected** The acceptance window is displayed in the following two cases. The target user must accept or refuse the file transfer. ◦ The controller user selects **pull file** from the file transfer menu on the controller window. The target user must select the file that is to be transferred after they accept the request. ◦ The controller user selects **send file to controller** from the **Actions** menu in the target window. **Not selected** The acceptance window is not displayed and files are transferred automatically from the target to the controller system when requested.
Confirm system information	ConfirmSysInfo	selected	Determines whether the user acceptance window is displayed when the controller user requests to view the target system information. **selected** When the controller user clicks **System information** in the controller window, the user acceptance window is displayed. The target user must accept or refuse the request. If the target user clicks accept, the target system information is displayed in a separate window on the controller system. If they click refuse, a message is displayed on the controller and the system information is not displayed. **not selected**

User options	Target property	Default Value	Description
			The target system information is displayed automatically when the controller user clicks the system information icon.
Confirm recording	ConfirmRecording	selected	Determines whether the user acceptance window is displayed when the controller user clicks the record icon on the controller window. **selected** When the controller user clicks the record icon on the controller window, a message window is displayed. If the target user clicks **Accept**, the controller user can select a directory to save the recording to. If the target user clicks **Refuse**, a recording refused message is displayed to the controller. **Note:** After the target user accepts the request for recording, if the controller user stops and restarts local recording, the acceptance window is not displayed. **not selected** When the controller user clicks the record icon on the controller window, the message window is not displayed. The controller user can select a directory to save the recording to.
Confirm collaboration	ConfirmCollaboration	selected	Determines whether the user acceptance window is displayed when another controller user requests to join a collaboration session with a target. **selected** When the controller user tries to join the collaboration session, the user acceptance window is displayed. The target user must accept or refuse the request to allow the additional controller to join the session. If the target user clicks accept, the additional controller joins the collaboration session. If they click refuse, a message is displayed on the controller system and the additional controller cannot join the collaboration session. **not selected** The additional controller automatically joins the collaboration session when they try to connect to the master controller of the session.
Acceptance grace time	AcceptanceGraceTime	45	Sets the number of seconds to wait for the target user to respond before a session starts or times out, used with **Confirm incoming connections**. ◦ Acceptable values 0 - 60. If set to 0, the target user is not asked to respond to the session request. **Note:** If **Confirm incoming connections** is selected, **Acceptance grace time** must be set to a value >0 to provide the target user with enough time to respond.

User options	Target property	Default Value	Description
Proceed on acceptance timeout	AcceptanceProceed	not selected	Action to take if the user acceptance window timeout lapses. The target user did not click accept or refuse within the number of seconds defined for **Acceptance grace time**. **selected** Session is established. **not selected** Session is not established.
Hide windows (Deprecated)	HideWindows	not selected	**Note:** The "Allow to show/hide selected windows during the session" feature has been deprecated for all versions above Windows 7. Determines whether the **Hide windows** check box is displayed on the user acceptance window when **Confirm incoming connections** is also selected. **selected** The **Hide windows** check box is displayed on the user acceptance window. **not selected** The **Hide windows** check box is not visible on the user acceptance window.

Table 4. security option descriptions

Security options	Target property	Default Value	Description
Authenticate using system logon	CheckUserLogin	selected	Determines whether the login window is displayed when a session type is selected on the **Open Connection** window. **Yes** The logon window is displayed and the controller user must log on with a valid Windows™ operating system ID and password. If the logon credentials are invalid, the target refuses the session. **No** The logon window is not displayed and the peer-to-peer session is established.
Authorized	CheckUserGroup	see description	Default value is: **Windows® systems** `BUILTIN\Administrators`

Security options	Target property	Default Value	Description

user group			**Linux® systems**
			`wheel`
			When **Authorized user group** has a value set, the user name that is used for authentication must be a member of one of the groups that are listed. If the user is not a member, the session is refused. Multiple groups must be separated with a semicolon. For example, `wheel;trcusers`
			Note: By default, on Windows® systems, only the Administrator user is granted access. On Linux® systems, by default no users are granted access. To resolve this issue, complete one of the following steps.
			a. To also grant administrator rights to the users, add them as members to the Administrators group on Windows® systems or the wheel group on Linux® systems.
			b. For users with no administrator rights, complete the following steps
			i. Create a group or use an existing group. For example, the following command can be run as root:
			`groupadd trcusers`
			.
			ii. Add the users to this group. For example, the following command can be run as root to add **bsmith** to **trcusers**:
			`usermod -a -G trcusers <bsmith>`
			iii. Add the group to the list in the **Authorized user group** field.

Audit to system log	AuditToSystem	selected	Determines whether the actions that are carried out during remote control sessions are logged to the application event log on the target. This file can be used for audit purposes. **selected** Entries are logged in the application event log of the target corresponding to each action that is carried out during the session. **not selected** No entries are logged to the application event log.
Save chat messages	AutoSaveChat	not selected	Determines whether the chat text, entered during a chat session, can be saved. **selected** The chat text is saved as an html file. The file is `chat-`*`username`*`-`*`date`*`.html`, where *username* is the display name of the logged on user on the controller ma-

Security options	Target property	Default Value	Description
			chine in a peer-to-peer session. In managed mode *username* is the display name for the controller user that is on the server. The date is in the format *YYYYMMDD*. The file is saved in the working directory of the target. The location of the working directory is defined by the target property **WorkingDir**. For example, on Windows™ systems, the file is saved to `c:\ProgramData\BigFix\Remote Control`. On Linux systems, the file is saved to `/var/opt/bigfix/trc/target/`. **not selected** The chat text is not saved to a file.
Enable system access for file transfer	EnableFileTransferSystemAccess	not selected	Determines whether the file transfer session allows for target file system access using System privileges (Windows) or root privileges (Linux). This option is valid for peer to peer sessions only. **selected** The file transfer session uses System privileges (Windows) or root privileges (Linux) on the target file system. **not selected** The file transfer session uses the privileges of the logged on user on the target file system.
Lock target on disconnect	SessionDisconnect	not selected	Determines whether the target computer is automatically locked when the remote control session ends.Allowed value: *lock*. When you set the value to *lock*, the target computer is automatically locked at the end of the session. If the property is blank or set to another value, the target computer is not automatically locked at the end of the session.
Allow privacy	AllowPrivacy	selected	Determines whether a controller user can lock the local input and screen of the target when in a remote control session. Determines the visibility of the **Enable Privacy** option on the controller window. **selected** The **Enable Privacy** option is available in the **Perform Action in target** menu in the controller window. **not selected** The **Enable Privacy** option is not available in the **Perform Action in target** menu in the controller window.

Security options	Target property	Default Value	Description
Allow input lock	AllowInputLock	selected	This property works with **Allow privacy** and on its own. You can use **Allow input lock** to lock the target users mouse and keyboard during a remote control session. **selected** The **lock target input** menu item is enabled, in the **Perform action in target** menu in the controller window. Select **lock target input** to lock the target users mouse and keyboard during a remote control session. The target screen is still visible to the target user. **not selected** The lock target input menu item is not enabled in the **Perform action in target** menu in the controller window. **Note:** If the option to **Enable Privacy** is selected during a session, the remote user input is automatically locked. It is not possible to enable privacy without also locking the input.
Enable privacy	EnablePrivacy	not selected	Determines whether the local input and screen are locked for all sessions. Therefore, the target user cannot input or do anything on the target while in a remote control session. **selected** The target screen is blanked out by the privacy bitmap when the session starts, preventing the target user from interacting with the screen while in the session. The target desktop is still visible to the controller user in the controller window. **not selected** The target screen is not blanked out when the session is started and the target user can interact with the screen.
Enable input lock	EnableInputLock	not selected	This property works with **Enable privacy**. When privacy mode is enabled, use **Enable input lock** to determine whether the target user can view their screen or not, during a remote control session. **selected** The target screen is visible to the target user during the session, while in privacy mode but their mouse and keyboard control is locked. **not selected** The target screen is not visible to the target user. The privacy bitmap is displayed on the target during the session. The target users mouse and keyboard input is also disabled.

Security options	Target property	Default Value	Description
			Note: Enable privacy must be selected for **Enable input lock** to take effect.
Disable-PanicKey	Disable-PanicKey	not selected	Determines whether the Pause Break key can be used by the target user to automatically end the remote control session. **selected** The target user cannot use the Pause Break key to automatically end the remote control session. **not selected** The target user can use the Pause Break key to automatically end the remote control session.
Enable on-screen session notification	Enable-OSSN	not selected	Determines whether a semi-transparent overlay is displayed on the target computer to indicate that a remote control session is in progress. Use this property when privacy is a concern so that the user is clearly notified when somebody can remotely view or control their computer. **selected** The semi-transparent overlay is displayed on the target screen with the text **Remote Control** and what type of remote control session is in progress. `For example, Remote Control - Active Mode.` The overlay does not intercept keyboard or mouse actions, therefore the user is still able to interact with their screen. **not selected** No overlay is displayed on the target computer. **Note:** This policy is only supported on targets that have a Windows® operating system installed.
Disable GUI	Disable-GUI	not selected	Determines the appearance of the target GUI when the remote control session is starting and also during the session. **Note:** This option works only when the target is installed in peer-to-peer mode and the **Managed** target property is set to No. This option is ignored when applied to any targets that were installed by using the Remote Control server mode when a server URL was supplied. **selected**

Security options	Target property	Default Value	Description
			The target GUI is not visible on the target and the target user is not aware that the session is started. The Remote Control target icon is not visible in the Windows® system tray. **not selected** The target GUI is displayed on the target as the session is starting and is available to the target user during the remote control session.

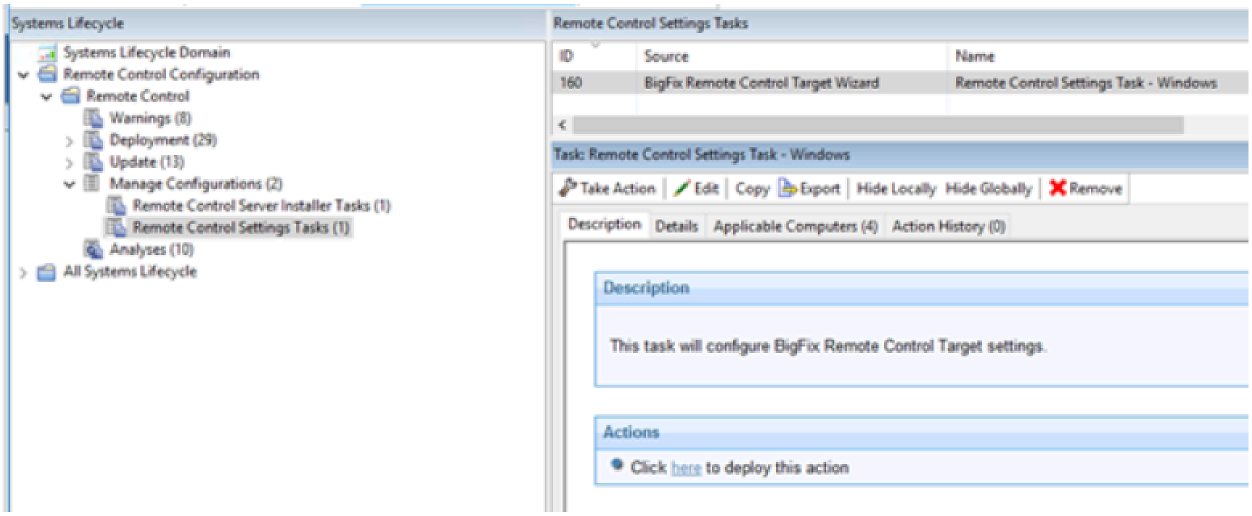
Table 5. performance option descriptions

Security options	Target property	Default Value	Description
Inactivity timeout	IdleTimeout	360	Number of seconds to wait until the connection ends if there is no session activity. Set this value to 0 to disable the timer so that the session does not end automatically. The minimum timeout value is 60 seconds. For values 1 - 59, the session times out after 60 seconds of inactivity. **Note:** The inactivity timeout value applies to Active session mode only. The session does not end automatically when other session modes are used. The default value is 360.
Enable high quality colors	EnableTrueColor	not selected	Determines whether the target desktop is displayed in high-quality colors in the controller window at the start of a session. Used together with **Lock color quality**. **selected** The target desktop is displayed in true color 24-bit mode at the start of the session. Partial screen updates are also enabled. **not selected** The target desktop is displayed in 8-bit color mode at the start of the session. Partial screen updates are also enabled. This value is the default value.
Lock color	LockColorDepth	not se-	Determines whether the color quality that a remote control session is started with can be changed during the session. Used together with **Enable high quality colors**.

Security options	Target property	Default Value	Description
quality		lected	**selected** The initial color quality, for the remote control session, is locked and cannot be changed during the session. The **Performance settings** icon is disabled in the controller window. The controller user cannot change settings to improve the session performance if their network is slow. **not selected** The color quality can be changed during the session. The **Performance settings** icon is enabled in the controller window.
Remove desktop	RemoveBackground	not selected	Determines whether a desktop background image can be removed from view during a remote control session. **selected** The desktop background image, on the target, is not visible during a remote control session. **not selected** The desktop background image, on the target, is visible during a remote control session.
Stop screen saver updates	NoScreenSaver	not selected	Stops the target from sending screen updates when it detects that the screen saver is active. **selected** While the screen saver is active on the target system, the target stops transmitting screen updates. A simulated screen saver is displayed on the controller computer so that the controller user knows that a screen saver is active on the remote screen. The controller user can close the screen saver by pressing a key or moving the mouse. **not selected** No simulated screen saver is displayed in the session window. The target screen is displayed as normal and the target continues to transmit screen updates.

3. Click **Create Configuration Task**. Type the relevant information for your task and click **OK**

Your task is displayed in the list panel of the Remote Control Settings Tasks subnode.



ID	Source	Name
160	BigFix Remote Control Target Wizard	Remote Control Settings Task - Windows

Description

This task will configure BigFix Remote Control Target settings.

Actions

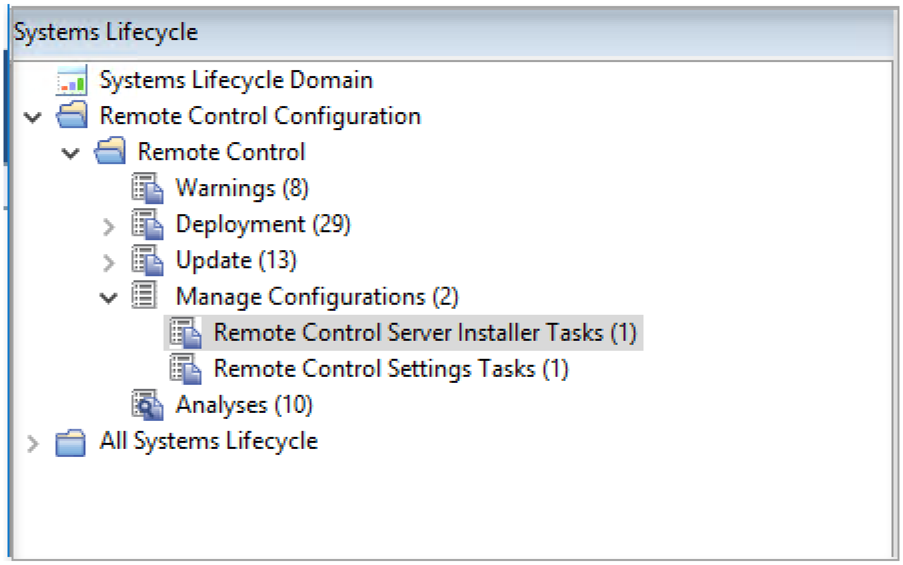
- Click here to deploy this action

Run Remote Control tasks

After you create server and target configuration tasks, run the tasks to install the Remote Control server software or change the configuration of already installed targets.

Running server installer tasks

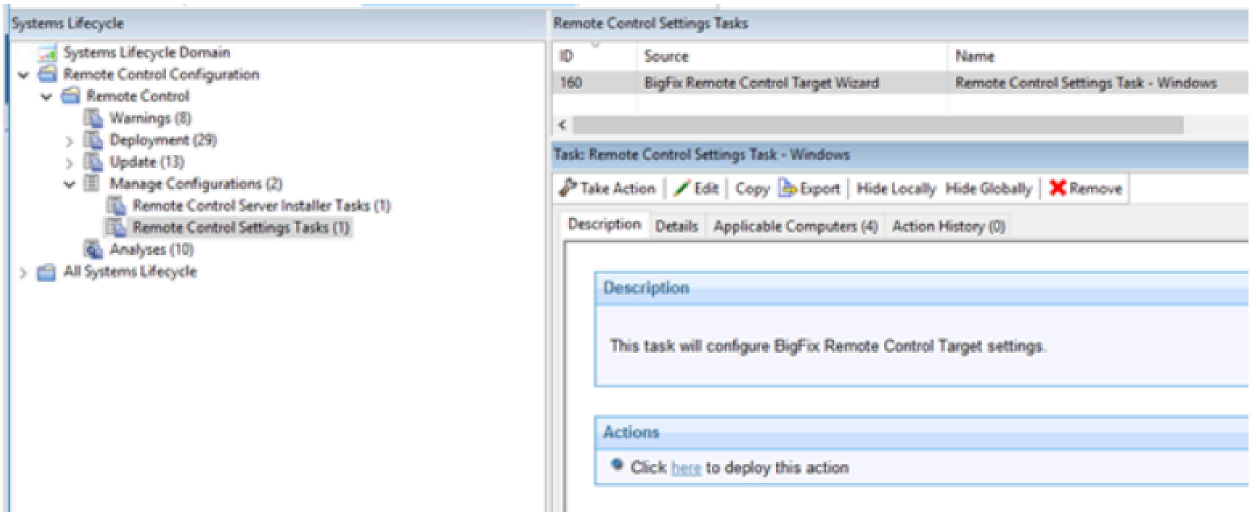
Use the **Remote Control Server Installer Tasks** subnode to run the tasks that you created by using the **Remote Control Server Installer Wizard**. Select the required task. Select the **Description** tab and review the description. If you are using a DB2, MS SQL, or Oracle database, you must enter the database password. Follow the instructions in the Actions box to initiate the task. These tasks install the Remote Control server software on your selected computers.


Systems Lifecycle
Systems Lifecycle Domain
Remote Control Configuration
Remote Control
Warnings (8)
Deployment (29)
Update (13)
Manage Configurations (2)
Remote Control Server Installer Tasks (1)
Remote Control Settings Tasks (1)
Analyses (10)
All Systems Lifecycle

Note: If the server installer fails, the task fails and an exit code is displayed.

Running target configuration tasks

Use the **Remote Control Settings Tasks** subnode to run the configuration tasks that you created by using the **Remote Control Target Wizard**. Select the task. In the **Task** window, review the description, and follow the instructions in the Actions box to initiate the task.



ID	Source	Name
160	BigFix Remote Control Target Wizard	Remote Control Settings Task - Windows

Task: Remote Control Settings Task - Windows

Description

This task will configure BigFix Remote Control Target settings.

Actions

- Click here to deploy this action

Analyses

The **Analyses** subnode provides a set of analyses that gather installation, user, and audit information. This data provides a history of remote control connection events that took place on the computers in your environment that have the controller or target components installed. These analyses are activated globally therefore any computers in your environment, that the analysis is relevant for, report their values.

Retrieving target installation and security data

The **Remote Control Installation and Security Options** analysis is used for gathering information about the installation and security property values from targets in your environment. The returned values provide information about the targets. For example, if they are allowed to take part in peer-to-peer sessions or if they can take part in remote control sessions that are initiated from an Remote Control server. For property value definitions, see step 2 *(on page 72)* .

If the analysis is active, the computers that this analysis was relevant for and the values of the installation and security options, are displayed in the **Results** tab. You can expand the **Applicable Computers** entry and filter the data further by **Retrieved Properties**. This feature can be useful in many ways. For example, to determine which targets can take part in peer-to-peer remote control sessions or to view the version of target software that is installed on the various Remote Control targets.

For example, to view a list of targets that are running a specific version of Remote Control target software, expand **Applicable Computers** > **By Retrieved Properties** > **By Remote Control Target Version** and select a specific version from the list. A list of relevant targets is displayed.

Retrieving audit events data

The **Remote Control Controller Logs** analysis is used for gathering the audit events from any computers in your environment that have the Remote Control controller component installed. The information is retrieved and updated every 6 hours. This information can be used for auditing purposes and also for monitoring session activity carried out by the controller user.

If the analysis is active, the list of computers that this analysis is relevant for is displayed in the **Results** tab. Double-click a computer to see summary data for the selected computer. The data includes a section for the controller log entries that are retrieved by the **Remote Control Controller Logs** analysis. You can also expand the **Applicable Computers** entry and filter the data further by specific retrieved properties.

Note: If the controller component is actively in a remote control session while the analysis tries to gather data from it, an error is reported. The error is reported in the analysis results stating that the file is in use.

Retrieve user, session, and performance data

The **Remote Control User, Session, and Performance Options** analysis is used for gathering user interaction, session behavior, and performance property values from targets in your environment. Use the properties to determine what actions the controller user can carry out during a remote control session with this target. For property value definitions, see step 2 *(on page 72)*.

If the analysis is active, the computers that this analysis was relevant for and the values of the user interaction properties are displayed in the Results tab. You can expand the **Applicable Computers** entry and filter the data further by specific retrieved properties.

Retrieve session connection data

The **Remote Control Target Log (Start/Stop)** analysis is used for gathering the audit events from any computers in your environment that have the Remote Control target component installed.

The information is retrieved and updated every 6 hours. The information that is returned by this analysis is useful for viewing remote control session usage activity on specific targets. Only the session connection, start, and stop events that are returned for each session. If you require information about the remote control session activity, use the **Remote Control Target Log** analysis.

Note: This analysis is only valid for Windows™ targets.

If the analysis is active, the Results tab lists the computers that this analysis was relevant for. Double-click a computer to see summary data for the selected computer that includes a section for the target log start stop entries. You can also expand the Applicable Computers entry and filter the data further by specific retrieved properties.

Retrieve session activity data

The **Remote Control Target Logs** analysis is used for gathering the audit events from any computers in your environment that have the Remote Control target component installed. The information is retrieved and updated every 6 hours. This information is useful for auditing purposes. Details of the actions that were carried out during a remote control session are displayed. For example, a change in session type or a file transfer. The controller user in the session is also displayed.

If the analysis is active, the computers that this analysis was relevant for are displayed in the **Results** tab. Double-click a computer to see summary data for the selected computer. The data includes a section for the target log entries that are retrieved by the **Remote Control Target Logs** analysis. You can also expand the **Applicable Computers** entry and filter the data further by specific retrieved properties.

Note: To view the complete information for the reason codes, use the web reports feature to display the output. For more information about web reports, see Viewing web reports *(on page 107)*.

Enable smart card authentication in the target

To support smart card authentication in the BigFix® Remote Control Target you must install the virtual smart card reader driver and related certificates on the target. You can install the driver and certificates after you install the target by running a Fixlet® in the BigFix® console. You can also install the certificates by using Active Directory Group Policy.

The device driver for the IBM® virtual smart card reader is required to enable the use of smart cards for remote authentication, or to perform an action on the target computer. During a remote control session, the target creates a virtual card reader. The controller user selects a physical card reader on their system to connect it to the virtual card reader so that the target system can access the smart card. During the session, when Windows™ makes a request to the virtual card reader, the target redirects the request to the physical card reader on the controller system. For more information about using the smart card feature during a session see, the *BigFix® Remote Control Controller User's Guide*.

Note: The device driver for the IBM® virtual smart card reader is supported only in Windows™ 7 or later and Windows™ Server 2008 R2 or later.

Determining whether smart card support is enabled

To enable smart card support on your targets, multiple prerequisites must be met. Check which of your computers need action by using an Analysis.

To see the status of your computers, complete the following steps:

1. Go to the **Remote Control- Virtual Smart Card Reader Driver Status** analysis in the **Remote Control** site.
2. Review the information in the **Description** tab.
3. Review the information in the **Results** tab.

If smart card support is enabled, the **Driver Installed** value reports the version of the driver installed, and the following properties display a YES value:

- **Trusted Publisher SHA1 Installed**
- **Trusted Publisher SHA256 Installed**
- **Root CA SHA1 Installed**
- **Root CA SHA256 Installed**

The **KB2921916 Installed** and **KB3033929 Installed** properties can display the value YES or N/A, depending on the version of Windows operating system installed on the target.

Note: If *<error>* is displayed in the **KB2921916 Installed** and **KB3033929 Installed** columns, you must ensure that you are subscribed to the Patches for Windows™ site. Enable the Patches for Windows™ site in the **License Overview** section of the BigFix® console.

Installing the virtual smart card reader driver and certificates by running a Fixlet

Install the device driver for virtual smart card reader together with the certificates by running a Fixlet in the BigFix® console.

You can install the driver and certificates by running a Fixlet after you install the target. To install the driver and certificates, complete the following steps:

1. In the **Remote Control** site, click the **Deployment** node.
2. Select the **Install Remote Control Virtual Smart Card Reader Driver version 10.0.0.23 and certificates** task.
3. Review the information in the **Description** tab.
4. Follow the instructions in the **Actions** field to install the driver.

The device driver and certificates that are required for smart card authentication are installed. During a remote control session, when the controller user selects a physical card reader on their system, the target can now create a virtual card reader.

Note: If an error is reported when you run the Fixlet, use the `VSCDriverInstall.log` file in the target installation directory for debugging purposes.

Removing the virtual smart card reader driver and certificates by running a Fixlet®

Remove the device driver for the IBM® virtual smart card reader together with the certificates by running a Fixlet® in the BigFix® console.

To remove the driver and certificates complete the following steps:

1. In the **Remote Control** site, click the **Deployment** node.
2. Select the **Uninstall Virtual Smart Card Reader Driver for Remote Control** task.
3. Review the information in the **Description** tab.
4. Follow the instructions in the **Actions** field to remove the driver and certificates.

The device driver and Trusted Publisher certificates that are required for smart card authentication are removed from the selected computers. The smart card feature is no longer available on the selected computers.

Note: If an error is reported when you run the Fixlet®, use the `VSCDriverUninstall.log` file in the target installation directory for debugging purposes.

Installing the certificates by running a Fixlet®

Use a Fixlet® to install the certificates that are required by the device driver for the virtual smart card reader.

You can install the certificates together with the driver by running a Fixlet®. However, if the results of the **Remote Control - Virtual Smart Card Reader Driver Status** analysis show that the device driver is installed on your computer, but there are no certificates, you can install the certificates by running a Fixlet®. To install the certificates, complete the following steps:

1. In the **Remote Control** site, click the **Deployment** node.
2. Select the **Install Remote Control Certificates for the Virtual Smart Card Reader Driver version 10.0.0.23** task.
3. Review the information in the **Description** tab.
4. Follow the instructions in the **Actions** field to install the driver.

The certificates that are required for smart card authentication are installed. For more information about the **Remote Control - Virtual Smart Card Reader Driver Status** analysis, see Determining whether smart card support is enabled *(on page 96)*.

Note: If an error is reported when you run the Fixlet®, use the `VSCCertsInstall.log` file in the target installation directory for debugging purposes.

Downloading the certificates for the virtual smart card reader

You can download the certificates that are required by the device driver for the virtual smart card reader and install them manually. For example, by using Active Directory Group Policy.

You can download the certificates in multiple ways. Choose the method for downloading the certificates.

- Download the files from the Remote Control site in the BigFix® console:
  1. Click the **Deployment** node and select the **Install Remote Control Virtual Smart Card Reader Driver version 10.0.0.23 and certificates** task.
  2. Select the **Description** tab.
  3. Follow the instructions in the **Description** field to download the certificates.
  4. Save the `vsc_certs_1020.zip` file.
  5. Extract the certificate files from the `.zip` file.
- Extract the certificate files from the installation media:

1. Access the image files. For more information about the image file, see Obtain the installation files.
2. Download the `BigFix_Rem_Cntrl_V10xx_Image_1.zip` file, where *10xx* is relevant to the version that is installed.
3. Extract the certificate files from the `\Windows` directory of the `.zip` file.

When you install the certificates, you must install the `HCL_America_Inc-sha256.crt` file to the Trusted Publishers store. Install the `TrustedRoot.crt` and `DigiCertCA-sha256.crt` files to the Trusted Root Certificate Authorities store.

Configure single sign-on (SSO) on the server

Remote Control V9.1.3 introduced support for SAML 2.0 authentication on the Remote Control server.

You can configure Single Sign-On (SSO) in multiple ways.

- During the Remote Control server installation.
- After you install the server.

After you configure SSO and access the remote control server, you are redirected to the SAML Identity Provider logon page to log on. The remote control server UI logon page is no longer displayed. However, the admin user ID must be able to log on to the remote control server without using SSO. Type the following URL in your browser to log on with the admin user ID when SSO is enabled. `https://[serverurl]/trc/altLogon.do`, where *[serverurl]* is the URL of your remote control server.

Configuring the server for single sign-on during installation

During the installation of the Remote Control server, you can configure support for SAML V2.0 authentication.

Download the server installation file by running a Fixlet®. For more information, see Download the Remote Control server component *(on page 53)*.

1. Follow the installation steps in the **Installing by using the server installer** chapter in the *BigFix® Remote Control Installation Guide*.
2. During the installation, select your configuration options on the SSO configuration window.

   Enable SSO

   Select this option to enable Single-Sign-On (SSO). To continue with the configuration, you must get the SAML metadata XML file from the Identity Provider (IdP) and which hash algorithm they are using: SHA-1 or SHA-256.

   Metadata XML file

   Click **Choose** and select the SAML metadata XML file that you obtained from the IdP.

   Algorithm used to sign SAML messages

Select the signature algorithm (SHA-1 or SHA-256) to use to sign messages in communications between the Identity Provider (IdP) and this Service Provider (SP) which is the BigFix® Remote Control Server.

Advanced parameters (optional)

Type in further configuration options, by adding attribute names in a space-separated list, in the following format: *[keyword]*="*[keyword-value]*". Where *[keyword]* is the attribute name and *[keyword-value]* is the attribute value.

Force regeneration of SAML data. (you must re-register with the IdP)

The first time that you enable SSO, a new default SAML certificate keystore is created. For future upgrades, you can select the regeneration option to create a new default certificate keystore. The current keystore is deleted and the new one is saved. When you select this option, you must reestablish the connection between the SP and the IdP after the server restarts.

3. Complete the installation. After you click **Install** on the **Summary** window in the installation program, the **Important** window is displayed. Take note of the URL and information on the **Important** window. After the server starts, type the URL in your browser to download the SP metadata. You must provide the metadata to the IdP to establish federation between them.

Configuring the server for single sign-on after installation

After you install the Remote Control server, you can configure it to support SAML 2.0 authentication.

You must create a keystore with a single self-signed certificate (or CA signed certificate) before you start the configuration. Select a **Key Size** of 2048 and select sha256 for the **Signature Algorithm**. The keystore file can be a `.p12` or `.jks` file. Do not save the file to the server installation directory because that might conflict with the server self-signed certificate. Set a long validity period for the keystore. For more information about creating a keystore file, see Creating a self signed certificate.

Note: SSO support in Remote Control is done through the WebSphere Liberty samlWebSso20 feature. By default, the **NameID** that is returned by the Identity Provider to our service must contain an email field in the following format.

```
URI: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
```

You can configure a Liberty server as a SAML web browser Single-Sign-On (SSO) service provider by enabling the samlWeb-2.0 feature in Liberty.

To configure the Remote Control server, complete the following steps:

1. Create an `sso.xml` file in the following directory:

Windows™ operating system

```
C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver
```

Linux™ operating system

`/opt/BigFix/TRC/server/wlp/usr/servers/trcserver`

2. Add the following content to the `sso.xml` file:

```
<server>
<featureManager> }}
<feature>samlWeb-2.0</feature>}}
</featureManager> }}
<samlWebSso20 id="defaultSP" keyStoreRef="samlKeyStore" httpsRequired="true"
signatureMethodAlgorithm="SHA256" spHostAndPort="https://[hostname:port]"/>
<keyStore id="samlKeyStore" location="[samlKey.file]"
password="[yourkeystorepassword]" type="[filetype]"/>
</server>
```

[hostname:port]

Defines the host name and SSL port of your remote control server. For example, https://example.com:443/.

[samlKey.file]

Defines the path to your keystore file. For example, `c:\trc\samlKey.jks`.

[yourkeystorepassword]

Defines the password for your keystore file. For example, password="mypassword".

[filetype]

Defines the file type of your keystore file. For a `.p12` file, set type to PKCS12. For a `.jks` file, set type to JKS.

The **keyStore** *id* value must match the **keyStoreRef** value in the **<samlWebSso20>** element.

You can add more configuration parameters. For more information, see SAML Web SSO 2.0 Authentication (samlWebSso20)

In a default configuration, the following values are used:

AssertionConsumerService URL

`https://`**`<hostname>`**`:`**`<sslport>`**`/ibm/saml20/defaultSP/acs`.

Service Provider (SP) metadata URL

`https://`**`<hostname>`**`:`**`<sslport>`**`/ibm/saml20/defaultSP/samlmetadata`

Where **<hostname>** is the host name of your Remote Control server and **<sslport>** is the SSL Port value. For example, 443.

3. Edit the `application.xml` file in the following directory:

Windows™ operating system

`C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver`

Linux™ operating system

`/opt/BigFix/TRC/server/wlp/usr/servers/trcserver`

Add the following **<application-bnd>** statement to the file.

```
<server>
 <application   context-root="/trc" type="ear" id="trcserver"
 location="TRCAPP.ear" name="trcserver"  autoStart="true" >
 <application-bnd>
  <security-role name="any-authenticated">
  <special-subject type="ALL_AUTHENTICATED_USERS" />
  </security-role>
 </application-bnd>
 </application>
 <application   context-root="/" type="ear" id="trcredir"
 location="REDIR.ear" name="trcredir"  autoStart="true" />
 <applicationMonitor updateTrigger="disabled" dropinsEnabled="false" />
</server>
```

4. Get the SAML metadata XML file from the Identity Provider (IdP).
   How this file is obtained varies, depending on the IdP. Rename the file to `idpMetadata.xml` and copy it to the following directory on the server:

   Windows™ operating system

   `C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver\resources\security`

   Linux™ operating system

   `/opt/BigFix/TRC/server/wlp/usr/servers/trcserver/resources/security`

5. Edit the `common.properties` file and set **sso.enabled** to *True*.
   The file is in the following directory:

   Windows™ systems

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

   Where *[installdir]* is the directory in which the Remote Control server is installed.

   Linux™ systems

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

   Where *[installdir]* is the directory in which the Remote Control server is installed.

6. Restart the Remote Control server.
7. After the server restarts, type the following URL into your browser to download the metadata for this service provider (SP) which is the BigFix® Remote Control Server: `https://<hostname>:<sslport>/ibm/saml20/defaultSP/samlmetadata`, where *<hostname>* is the host name of your remote control server and *<sslport>* is the SSL port of the server. Provide the metadata to the SAML identity provider to establish federation between this SP and Identity Provider (IdP).

When you access the Remote Control server application, and you did not previously log on, you are redirected to the IdP. If you did previously log on by using the same IdP, you are automatically logged on to the Remote Control server application.

Note: After you enable SAML 2.0 authentication, if you reinstall or upgrade your server, the `sso.xml` file must be copied to a temporary directory before you start. Replace the `sso.xml` file that is installed during the upgrade with the backed-up file. Also, ensure that **sso.enabled** is set to *True* in the `common.properties` file.

Enable secure target registration.

To prevent unauthorized targets from registering with the Remote Control server, you can enable the secure registration feature and use tokens to authenticate the target.

After you install the server, create a registration token on the server and distribute it when you install the target. The token is used to restrict new target registrations, or restrict updates to existing target details when you reinstall a target. After the target registers, the server sends an endpoint token to the target to replace the token that was used when it registered. The target uses the endpoint token to authenticate with the server each time it contacts the server.

New Installation scenario

The following scenario covers a new installation of server and targets.

- Create a server installer task and select **Use secure registration tokens to register targets**. Ensure that **HTTPS as Default for Target URL** is also selected. Run the task. For more information about creating a server installer task, see Creating Remote Control server installation tasks *(on page 58)*.
- Create a secure registration token in the server UI.
  1. Click **Admin > Create Secure Registration Token**.
  2. Supply the following information for the token. The default time period starts from the current date and time until 23:59 on the next day.

        - Description for token. Enter a description for the token.
        - Starting on. Click the calendar pull-down and select a date that the token is valid from. Enter a start time or keep the default time.
        - Ending on. Click the calendar pull-down and select a date that the token is valid to. Enter an end time or keep the default time.
    3. Click **Submit**. Before you leave the page, you must copy the registration token. Keep the token secure and confidential.
- Run the relevant target deployment task and enter the registration token. For more information, see Deploying the Windows target *(on page 17)* or Deploying the Linux target *(on page 28)*.

Upgrade scenario

The following scenario covers an upgrade of the server and targets.

- Create a server configuration task. Do not select **Use secure registration tokens to register targets**. Select **Migrate values from the existing properties files**. Run the task. For more information about creating a server installer task, see Creating Remote Control server installation tasks *(on page 58)*.
- Create a secure registration token in the server UI.
    1. Click **Admin > Create Secure Registration Token**.
    2. Supply the following information for the token. The default time period starts from the current date and time until 23:59 on the next day.
        - Description for token. Enter a description for the token.
        - Starting on. Click the calendar pull-down and select a date that the token is valid from. Enter a start time or keep the default time.
        - Ending on. Click the calendar pull-down and select a date that the token is valid to. Enter an end time or keep the default time.
    3. Click **Submit**. Before you leave the page, you must copy the registration token. Keep the token secure and confidential.
- To upgrade the target, run the update task that is relevant to your operating system. For more information, see Updating the Windows target *(on page 44)* or Updating the Linux target *(on page 48)*.
- Run the **Set Secure Registration Token for Remote Control Targets** task and enter the registration token. For more information, see Distributing a secure registration token to targets *(on page 105)*.
- Enable the secure registration feature in the server UI.
    1. In the server UI select **Admin > Edit properties file**.
    2. Select `trc.properties` from the list.
    3. Set **rc.enforce.secure.registration** to true. Ensure that the **enforce.secure.endpoint.callhome** and **enforce.secure.endpoint.upload** properties are also set to true.
    4. Click **Submit**.
    5. Click **Admin > Reset Application**

Distributing a secure registration token to targets

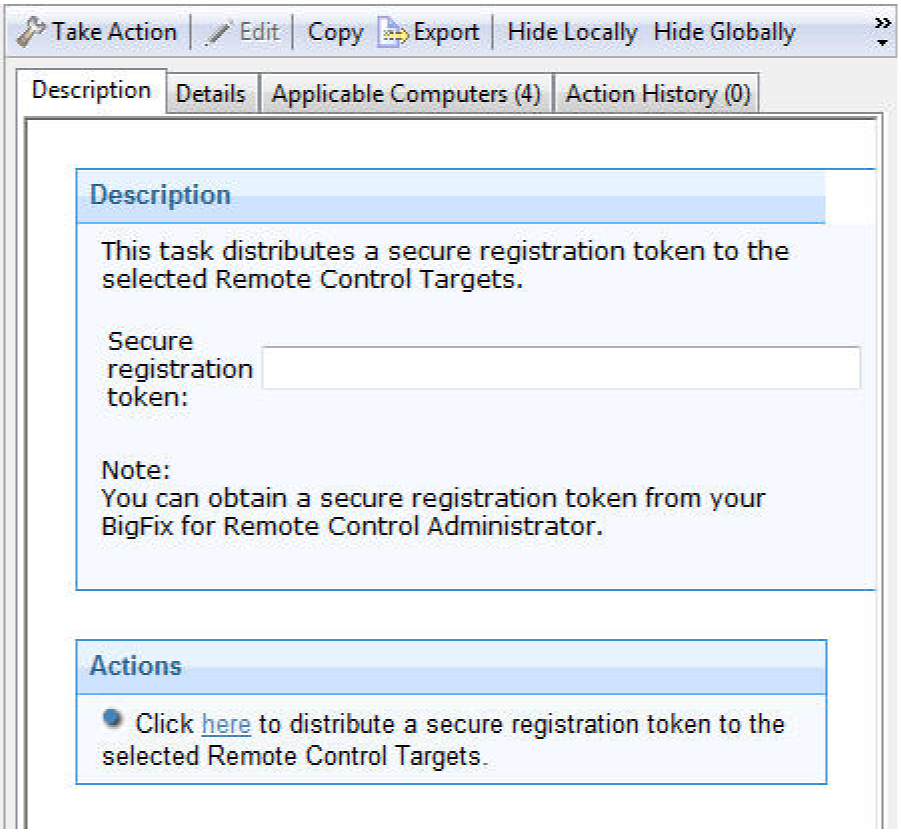
Use the **Set Secure Registration Token for Remote Control Targets** task to distribute a secure registration token to selected targets. The targets can use the token to securely register with the Remote Control server.

To run the task, you must have a valid secure registration token. For more information about creating a token, see **Creating a secure registration token** in the *BigFix® Remote Control Administrator's Guide*.

For secure target registration, the feature must also be enabled in the Remote Control server. The **rc.enforce.secure.registration** property in the `trc.properties` file must be set to true. Ensure that the **enforce.secure.endpoint.callhome** and **enforce.secure.endpoint.upload** properties are also set to true. For more information about enabling secure registration on the server, see **Enable secure target authentication in the server** in the *BigFix® Remote Control Installation Guide*.

To distribute the secure registration token, complete the following steps:

1. Within the **Systems Lifecycle** domain, expand **Remote Control configuration > Remote Control**.
2. Select **Update**.
3. In the **Update** pane, select the **Set Secure Registration Token for Remote Control Targets** task.
4. In the **Task** pane, review the description. Enter the secure registration token. Follow the instructions in the **Actions** box to start the task.



Description

This task distributes a secure registration token to the selected Remote Control Targets.

Secure registration token:

Note:
You can obtain a secure registration token from your BigFix for Remote Control Administrator.

Actions

● Click here to distribute a secure registration token to the selected Remote Control Targets.

5. In the **Take Action** pane on the **Target** tab, select the relevant option for determining which computers to distribute the secure registration token to.

The next time that the target contacts the server, it sends the secure registration token. If the secure authentication feature is enabled on the server, the server validates the token. If the token is valid, the target is registered and the server sends back an endpoint token to the target.

Chapter 6. Viewing web reports

Remote Control offers a report available in the **Web Reports** component of the application. The web report was formulated to provide log data that is gathered from the controller and target logs relevant to specific targets. The data can be used for auditing purposes and for monitoring remote control activity on specific computers in your environment.

To access the Remote Control web report, complete the following steps:

1. Click **Tools > Launch Web Reports**
2. Enter your **Web Reports** user name and password.
   If you do not know your user name or password, check with your administrator. After you log on, the main web reports page opens in a new browser window.
3. Select **Systems Lifecycle** to see a list of reports that includes the Remote Control report.
   The Remote Control Events entry is displayed in the reports list under the **Report List** menu.
4. Click **Remote Control Events**.
5. Enter the computer name of the target whose information you want to view and click **View Events**.

Any log data that was gathered from the controller and target logs, for the specified target is displayed in the relevant sections, showing the remote control events.

Appendix A. Frequently asked questions

1. The target software is installed on a target, but why is there is no menu option to start a remote control session when you right-click the computer in the BigFix® console?

   To start a remote control session by using this method, make sure that the following conditions are met.

   - The controller component is also installed on the system that the BigFix® console is installed on.
   - For the menu item to be visible, the **Remote Control Installation and Security Options** analysis must be active for the selected computer and reporting that the Remote Control target is active.
   - When the controller is deployed, only the current user who is logged on to the computer that you are deploying to has the rights to see the menu item; it is not visible to other users. The following registry key can also be created:

     Key name: `HKEY_CURRENT_USER\Software\BigFix\Enterprise Console\Settings \ComputerListContextMenuExtensions\TivoliRC`

     With the following values:

     ```
     ComputerApplicabilityRelevance (REG_SZ) = value of results (current computer, property 1 of
      fixlet 4 of bes site whose (name of it starts with "BigFix Remote Control")) = "True"
     ```

     ```
     MaxComputerSetSize (REG_DWORD) = 1
     ```

     ```
     MenuDisplayName (REG_SZ) = &BigFix Remote Control
     ```

     ```
     ShellCommandRelevance (REG_SZ) = "%22C:\Program Files\BigFix\Remote
      Control\Controller\jre\bin\javaw.exe%22 -jar %22C:\Program Files\BigFix\Remote
      Control\Controller TRCConsole.jar%22 --host " & ip address of current computer as string
     ```

2. I have deployed the target software in peer-to-peer mode. I now want the target to register with my Remote Control server. How can I get it to connect to the server?

   Use the Remote Control Target wizard to create a configuration task and specify the server URL of the required server. Run the task on the selected target to reconfigure it so that it can contact the server. For more information about creating the tasks, see Creating Remote Control target configuration tasks *(on page 71)*.

3. Where can I find more information about using Remote Control?

   Information about installing, using, and administering Remote Control can be found in the Remote Control documentation in HCL Knowledge Center.

4. Extra Remote Control function is available when you have the Remote Control server component installed; where can I obtain the server component from?

You can create a server installation task by using the **Remote Control Server Installer Wizard** to create an Remote Control server configuration. For more information about creating a server task, see Creating Remote Control server installation tasks *(on page 58)*.

You can also install a server that points to an already installed WebSphere Application Server instance that uses an already installed DB2®, MS SQL, or Oracle database. For more information about installing the server, see the *BigFix® Remote Control Installation Guide* and the section that displays, Installing the server.

5. How can I determine which type of server installation would be suit my environment?

    For guidelines to consider when you plan your installation, see the *BigFix® Remote Control Installation Guide*.

6. How do I troubleshoot Broker and Gateway upgrade fixlets fail with MSI error code 1638?

    For more details and instructions, see Broker and Gateway upgrade fixlets fail.

Appendix B. 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.

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

analyses
94
application log
96
remote control controller logs
95
remote control installation and security options
94
remote control target log (start/stop)
95
remote control user, session and performance options
95

audit events
retrieving data
95

B

broker
updates
Linux
52
windows
47

C

cli
updates
linux
50
windows
46

cli tools
deployment
linux
33
windows
23
uninstallation
linux
34
windows
24

controller
deployment
linux
32
macOS
42
windows
21
uninstall
macOS
43
uninstallation
linux
32
windows
22
updates
linux
49
windows
45

controller logs
retrieving data
95

D

dashboards
12
Remote Control overview
13

data
gathering
94

db2
server installation configurations
58, 63

definitions
8

Deploying Linux broker support
from the console
37
Deploying Windows broker support
from the console
26
deployment
cli tools
linux
33
windows
23
controller
linux
32
macOS
42
windows
21
gateway support
linux
35
windows
25
linux
28
macOS
39
overview
16
target
linux
28
macOS
39
windows
17
windows
17
deployment data
viewing
13
derby
server installation configurations
58, 60
download
linux server installer
54
server component
53
windows server installer
53

F

firewall rules
57
frequently asked questions
108

G

gateway
updates
Linux
51
windows
46
gateway support
deployment
linux
35
windows
25
uninstallation
linux
36
windows
26

I

IEM console
components
9
dashboards
12
overview
9

M

managed mode session
starting
57
managing target and server configurations
57
MS SQL
server installation configurations
66
mssql
server installation configurations
58

O

oracle
server installation configurations
58, 69
Overview
6

P

peer-to-peer session
controller initiated
56
M console initiated
54

R

Remote Control
using
16
Remote Control
overview
13
remote control server installer tasks
executing
93
remote control session
console initiated
54
peer to peer
54
starting
54
using the
Remote Control
server
57
Remote Control settings tasks
94
response
warnings
57

S

SAML 2.0
99
secure target registration
enabling
103
server
download linux installer
54
download windows installer
53
Server
SAML 2.0 support
99
server installation configurations
creating
58
db2
58, 60, 63
derby
58
MS SQL
66
mssql
58
oracle
58, 69
server installation tasks
creating
58
running
93
session activity data
retrieving
96

session connection data
retrieving
95
single sign on
server configuration
after installation
100
smart card
driver installation
96
smart card reader driver
Fixlet installation
97
removal Fixlet
97
smartcard
certificate
installation Fixlet
98
certificates
downloading
98
sso
server installer
99
starting a remote control session
54

T

target
deployment
linux
28
macOS
39
windows
17
smart card driver
96
uninstall
macOS
41
uninstallation
linux
31
windows
20
updates
linux
48
windows
44
target configuration task
creating
71
executing
94
target data
installation
94
properties
94
security
94
target installation data
retrieving
94
target properties
configuring
71
retrieving data
94
target security data
retrieving
94
target user data
retrieving
95
tasks
executing
93

U

uninstall
controller
macOS

43
target
macOS
41
uninstallation
cli tools
linux
34
windows
24
controller
linux
32
windows
22
gateway support
linux
36
windows
26
target
linux
31
windows
20
Uninstalling Linux broker support
from the console
38
Uninstalling Windows broker support
from the console
27
updates
broker
Linux
52
windows
47
cli
linux
50
windows
46
component
44
controller
linux
49
windows
45
gateway
Linux
51
windows
46
linux
48
target
linux
48
windows
44
windows
44
using
Remote Control
16
V
viewing web reports
107
W
warnings
57
web reports
viewing
107
wizard
server installation configuration
58
target configuration
71