Remote Control Installation Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page ccvii)*.

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Remote Control Installation Guide..... 9

Audience..... 9

Versions..... 9

Terms used in this guide..... 9

Chapter 2. Overview of the Remote Control system..... 10

How to use the guide..... 12

Remote Control operating requirements..... 12

A Basic installation..... 13

Installation with support for firewall and NAT traversal..... 14

Installation with support for remote control sessions over the internet..... 15

Server requirements..... 16

Server environment guidelines..... 18

Controller requirements..... 23

Target requirements..... 24

Gateway requirements..... 25

Broker requirements..... 26

Chapter 3. Get started..... 28

Chapter 4. Install the Remote Control components..... 29

Obtain the installation files..... 29

Install the server..... 29

Set up the database..... 30

Installing by using the server installer..... 36

Installing on WebSphere Application Server version 8.5.5: deploying the war file..... 44

Installing from the BigFix console..... 55

Install the target..... 55

Installing Windows Target..... 55

Installing the Linux™ target 76

Install the BigFix® Remote Control Target for macOS..... 76

Run a target custom installation..... 78

Install the controller..... 84

Installing the controller on a Windows™ system..... 84
Installing the Linux™ controller..... 85
Install the BigFix® Remote Control Controller for macOS..... 86
Installing the controller in other supported operating systems..... 87
Installing a preconfigured controller component..... 87
Install the command-line tools..... 90
Installing the cli tools on a Windows system..... 90
Installing the CLI tools in Linux™ 92
Install gateway support..... 93
Installing Windows gateway support..... 93
Installing Linux™ gateway support 94
Install broker support..... 95
Installing Windows broker support 95
Installing Linux broker support 95
Install Web Session Manager support..... 96
Chapter 5. Utility for extracting the component installation files..... 97
Extract the installation files by using the additional setup utility 98
Chapter 6. Enable secure target registration..... 99
Enable secure target authentication in the server..... 99
Enabling secure registration when you install the server..... 99
Enabling secure target registration after you install the server..... 99
Add a token for secure target registration..... 100
Adding a token on a Windows system..... 101
Add a token on a Linux system..... 103
Chapter 7. Install the driver for smart card authentication..... 104
Installing the virtual smart card reader driver by using the installer..... 104
Adding or removing the smart card reader driver by using the installer..... 104
Installing the smart card reader driver by running a silent installation..... 105
Installing the virtual smart card reader driver when you upgrade the target 106
Installing the driver and certificate by using a Fixlet 106
Installing the certificates by using a Fixlet..... 107
Downloading the certificates 107

Chapter 8. Manage the component services..... 109

Starting, stopping, or restarting the Windows™ components.....109

Starting, stopping, or restarting the Linux™ components..... 109

Chapter 9. Enabling email..... 111

Chapter 10. Configure LDAP 112

Setting up LDAP synchronization..... 112

Verifying connection information.....114

Configuring connection credentials.....115

Setting connection security.....116

SASL (Simple Authentication and Security Layer) 116

SSL (Secure Socket Layer) 117

Setting user authentication properties.....118

Authenticating the user.....118

Searching for the users directory entry.....120

Importing Active Directory Groups..... 121

Testing the Connection.....123

Verifying that the groups are imported.....124

Sample LDAP Configuration File.....124

Chapter 11. Configure Microsoft Entra ID.....130

Setting up Microsoft Entra ID synchronization.....130

Verifying connection information.....132

Configuring connection credentials.....133

Setting user authentication properties.....133

Authenticating the user.....133

Searching for the users.....134

Importing Groups..... 134

Testing the Connection.....135

Verifying that the groups are imported.....135

Migrating from LDAP to Microsoft Entra ID..... 135

Sample Microsoft Entra ID Configuration File..... 136

Chapter 12. Federal information processing standard (FIPS) compliance in Remote Control..... 139

Enable FIPS compliance on the server..... 139

Enabling FIPS compliance on a server installation with a stand-alone Open Liberty Application Server..... 140
Enabling FIPS compliance on an automated server installation 140
Enabling FIPS compliance on the controller..... 144
Enable FIPS compliance on the target..... 145
Enabling FIPS compliance on a Windows™ target..... 145
Enabling FIPS compliance in Linux® or UNIX® based operating systems..... 146
Enabling FIPS compliance on the gateway..... 146
Enabling FIPS compliance on the broker..... 147
Chapter 13. NIST SP800-131A compliance in Remote Control..... 148
Enable NIST SP800-131A compliance on the server..... 148
Enabling NIST SP800-131A compliance during the server installation 149
Enabling NIST SP800-131A compliance on a server with a stand-alone WebSphere Application Server..... 149
Enabling NIST SP800-131A compliance after you install the server 150
Creating a certificate for an MS SQL database when NIST SP800-131A is enabled 152
Enabling NIST SP800-131A compliance on the controller 155
Enabling NIST SP800-131A compliance in the stand-alone controller..... 155
Enable NIST SP800-131A compliance on the target..... 156
Enabling NIST SP800-131A compliance in a Windows® target..... 156
Enabling NIST SP800-131A compliance on Linux® or UNIX® based targets..... 157
Enabling NIST SP800-131A compliance on the gateway..... 157
Enabling NIST SP800-131A compliance on the broker..... 158
Enabling NIST SP800-131A compliance on the CLI tools..... 158
Enabling NIST SP800-131A compliance when you install the Windows cli tools..... 158
Enabling NIST SP800-131A compliance on the cli on Linux® or UNIX® based targets..... 158
Chapter 14. Verifying the server installation..... 159
Chapter 15. Recover from installation errors..... 160
Recovery steps..... 160
Errors during installation..... 160
Not enough memory..... 160
DB2® connection error when database options are verified..... 161
Oracle pre-checks..... 161
libstdc++.so.5 error when installing the server using the installation program..... 162

Errors after installation....162
Out of memory error....163
Database connection authorization failure....164
Application welcome page does not display....165
DB2® connection error when database options are verified....165
Targets cannot contact the server 166
Errors when you use Oracle as the database....167
Errors when trying to connect to the Microsoft® SQL database in FIPS compliancy mode....168
Chapter 16. Uninstall the components....169
Uninstall the server....169
Uninstalling the server by using the installer....169
Uninstalling the server application in IBM® Websphere Application Server....169
Uninstalling the server using Add or Remove programs....170
Uninstalling the target on Windows™ systems....170
Uninstalling the target on Linux® systems....170
Chapter 17. Upgrade from previous versions....172
Upgrade to Version 10 from earlier versions....172
Upgrade the gateway component....172
Upgrade the broker component....173
Upgrade the server component....173
Upgrade the target component....175
Upgrade the controller component....175
Chapter 18. Maintaining the target installation....177
Appendix A. Properties that can be set in the target configuration....178
Appendix B. AV Exclusions on Windows, Linux and MAC....203
Appendix C. Support....206
Notices....ccvii
Index....a

Chapter 1. Remote Control Installation Guide

By using Remote Control you can remotely support and control thousands of PCs and servers, on an enterprise scale, from a central location or directly, in peer to peer mode.

Use the Remote Control administration web interface, to view and control a remote desktop, including its keyboard and mouse, anywhere on your network. You can also chat, transfer files, remotely guide the users, administer the policies to be applied to different users and target groups, and much more. These features can help provide more efficient and effective analysis of user problems from the administrators desktop, without the added cost of dispatching a technician or relying on user descriptions over the phone. Use Remote Control to deliver better support, more flexibility, and richer security, by using robust features that include enhanced central logging and video capture of the sessions and full data stream encryption.

Audience

This guide is for administrators and IT managers who want to install and administer Remote Control. It details the system requirements for each of the components and provides installation instructions that allow you to deploy the program in your environment. It also includes information about configuring and maintaining Remote Control.

Versions

The guide includes the functions introduced in Remote Control V10, © Copyright HCL Ltd. 2025.

Terms used in this guide

The following terms are all Remote Control terms, but are used throughout the guide without being labeled every time with Remote Control:

- Controller always means Remote Control Controller application
- Target always means Remote Control Target
- Server always means Remote Control Server
- Broker always means Remote Control Broker
- Managed mode refers to installations where a server has been deployed and the targets are configured to register and report status to the server.

Chapter 2. Overview of the Remote Control system

The Remote Control system enables remote control through three core components—Target, Controller, and Server—with optional managed-mode services (CLI tools, Gateway, Broker) for secure or external connectivity. Targets can operate in peer-to-peer or managed mode, while the Server centralizes policies, authentication, auditing, and session launch.

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 Open Liberty® server, or install it by using the installer package along with an embedded version of Open Liberty®. The server listens for HTTP or HTTPS connections by default. When it is installed with the embedded Open Liberty® option, Open Liberty® it listens on ports 80 and 443. When it is deployed on top of an existing Open Liberty® 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 from an LDAPv3 server, such as Active Directory or Tivoli Directory Server. This deployment scenario has the same networking characteristics as peer-to-peer. Therefore, direct TCP connectivity is required between all the controllers and all the targets. However,

the Remote Control server provides a method of centralized, and finer, policy control, where targets can have different policies that are determined by the user who is trying to start the remote control session. The Server also provides for centralized audit and storage of full session automatic recordings. In this scenario, the controller is not a stand-alone application, but is started as a Java™ Web Start application from the Remote Control server's web interface to start the remote control session.

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

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

The following components can be used only in managed mode:

Remote Control CLI tools

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

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

Remote Control Gateway

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

Remote Control Broker

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

How to use the guide

The process of getting Remote Control up and running varies, depending on your network environment and the management granularity you want to achieve. The installation guide focuses on three types of deployments:

Peer to peer

Is the simplest scenario and therefore ideal for small deployments. All targets are in network sight of the controllers and there is no requirement to centrally manage the controller policies.

Intranet managed

Are most appropriate in a complex network infrastructure that requires the deployment of gateways to traverse firewalls, or there is a requirement for strict policy control and centralized auditing.

Managed

With support for internet sessions where at least one broker must be installed in an internet-facing computer so that it is visible to targets outside the controller's network sight.

For the sake of readability and generality, the installation guide assumes the following restrictions:

- Each Remote Control server must have access to one of the supported database servers. The database can be located locally on the server computer or remotely on a separate server. The supported database systems are DB2, Oracle, and MS SQL. It is also possible to install the server by using the embedded Derby database that is provided by the installer. However, this configuration is not supported for production deployments.
- In managed environments, each controller can make an HTTP or HTTPS connection to the Remote Control server.
- In managed environments, each Remote Control target computer in the network must be able to make an HTTP or HTTPS connection to a server, a gateway, or a broker on the specified ports.

If your network configuration does not match any of the scenarios in that chapter, contact a support technician for more options.

The initial deployment of a minimal managed Remote Control system (server and a few targets) can take approximately 1 hour to complete.

Several steps in the Remote Control installation depend on the completion of prior steps. For this reason, it is recommended that you follow the guide in the order presented.

Remote Control operating requirements

Remote Control runs efficiently by using minimal server, network, and client resources. The requirements for the client programs are not stringent. The hardware that is required by the server and the target depends on the number of computers that are administered and the frequency that is defined for their status updates.

A Basic installation

The most basic installation requires the Remote Control target and controller components. Use the two components to start a peer to peer remote control session, for which the policies are defined only at target level.

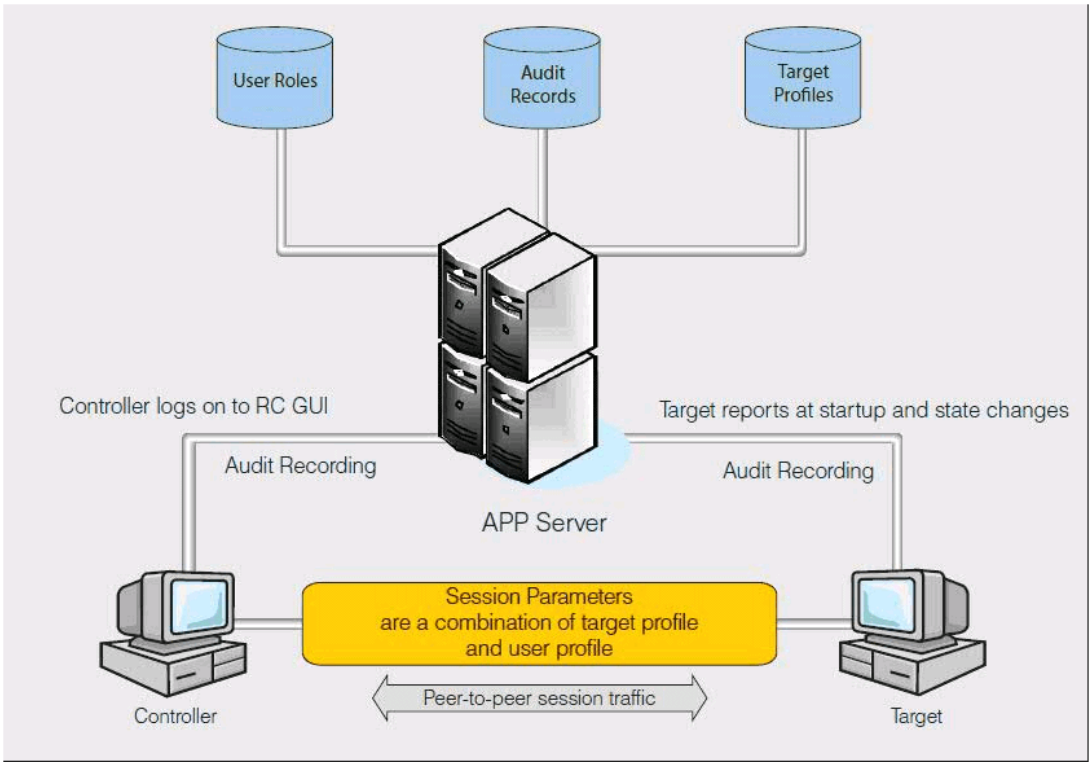
The port to be used for target to controller communication is configurable at installation time. The default is port 888.

Such an installation provides basic audit information. This information is accessible from the BigFix® console. It is also stored in the application event log, in a Windows operating system, or system log, in a Linux operating system. However, if centralized auditing and management of users and computers is required, install the server component.

The server component provides a single interface where controller users can easily search for targets. They can also organize the targets that are most frequently accessed and view their session history. For an administrator, a managed environment provides the following extra capability.

- Centralized management of users and targets: Users can be organized into groups with similar profiles. They can be organized manually, by using the Remote Control server interface, or by importing users and groups from LDAP or from Microsoft Entra ID. Similarly, targets can be organized into groups manually or by setting target membership rules to automatically assign a target to a specific group. For more information about target membership rules, see the *BigFix® Remote Control Administrator's Guide*.
- Centralized policy management: When a session is started from the server interface, the permissions that are set for the session are derived from the target and controller properties. Provides more flexibility to define different levels of access, against a single target, for different users in your organization.
- Centralized auditing and recording repository: Administrators can use the Remote Control server interface to browse and examine audit information. They can also view recordings that are associated with a specific remote control session. Administrators can search the existing session history. For example, by user ID or computer name.
- Access request management: Administrators can grant temporary access, or increase the level of access, to a target or group of targets. Temporary access can be granted to Remote Control registered and unregistered users.
- Reporting capabilities

Figure 1. Basic installation environment

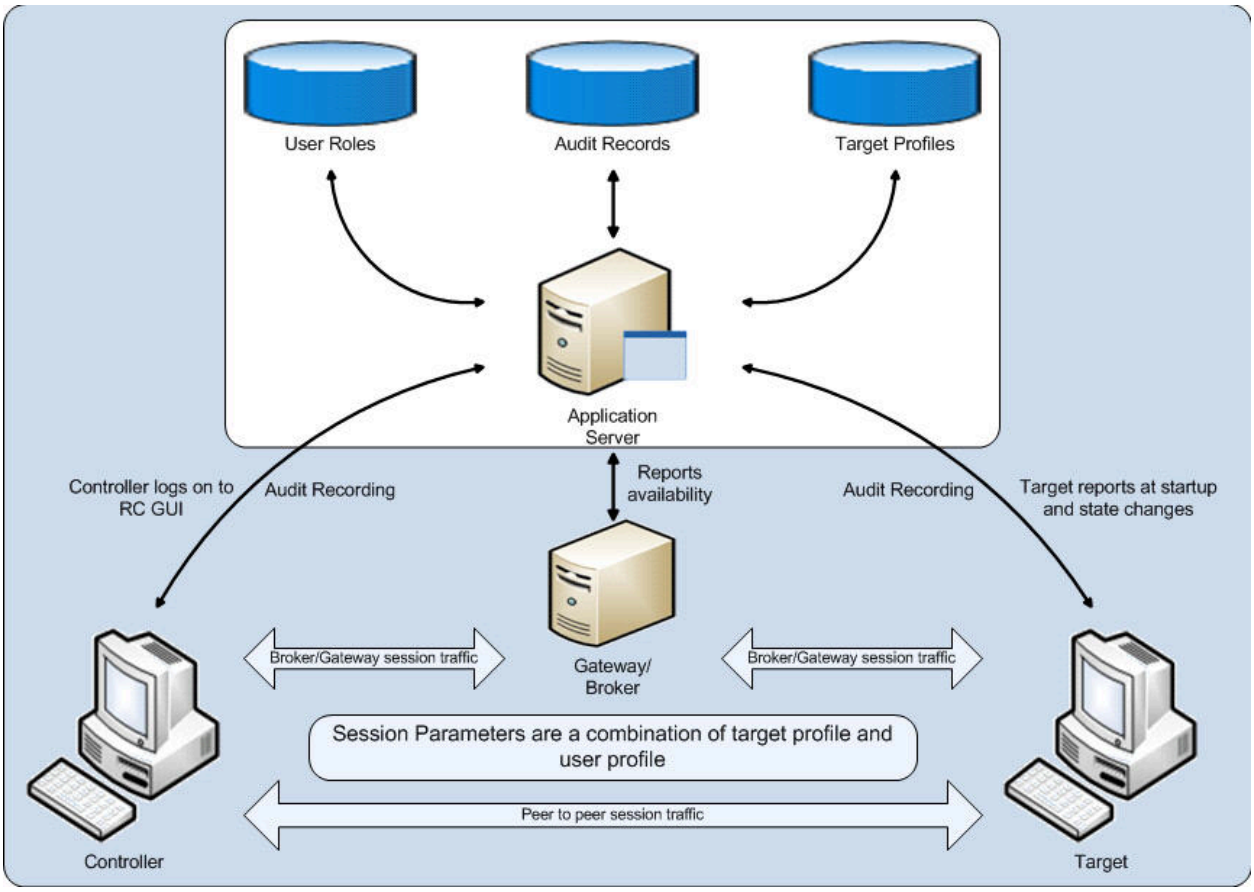


Note: It is not necessary to install the controller component in a managed environment. Remote control sessions are launched in-context from the Remote Control server interface. You can also configure the target components, in a managed environment, to accept peer to peer remote control requests from a stand-alone controller component. For more information about installing the target, see Install the target *(on page 55)*.

Installation with support for firewall and NAT traversal

In some environments, it is not possible to open a port in a firewall to enable controller to target, or target to server communication for all endpoints. It is more appropriate to enable traffic from, or traffic to a single computer that acts as a gateway to traverse the firewall.

The gateway component can be strategically installed in your network to enable traffic between targets and controllers, or targets and servers that are in different networks. This component can also be used as a proxy server to forward the target's status update to the remote control server.



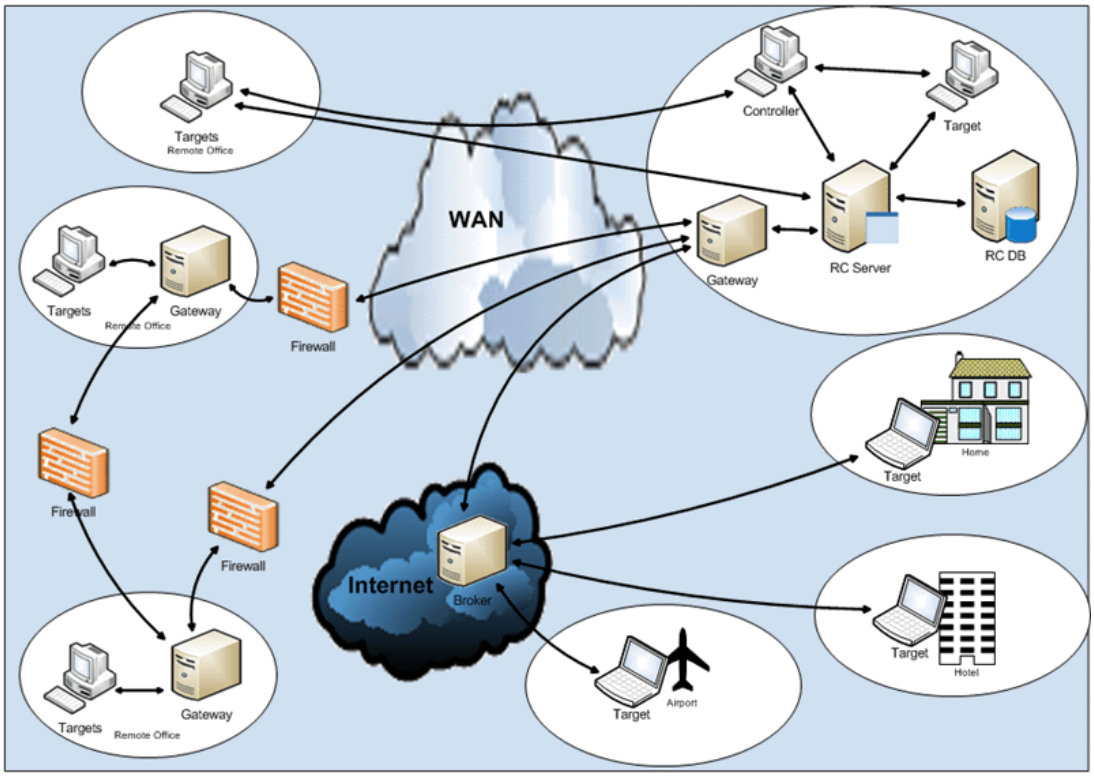
Installation with support for remote control sessions over the internet

Sometimes the target that requires support is out of network sight in an internet location. For example, in a hotel or an airport lounge.

Use the broker component to enable remote control sessions to these computers by bridging the target and controller communication. The broker must be placed in the DMZ and a gateway is required to provide secure communication to the server in the intranet.

In this scenario, the controller user can start a broker connection and obtain a connection code from the server. The user who requires assistance enters the connection code by using the appropriate menu option in the target UI. When the session details are validated by the server, the session is connected.

Figure 2. Sample deployment environment



Server requirements

The hardware that is required by the server component depends on the number of computers that are administered and the frequency that is defined for their status updates.

The distributed architecture of Remote Control allows a single server to support hundreds of thousands of computers.

The computer on which you install the Remote Control server must have the minimum following capabilities:

Minimum Hardware requirements

- 1 Quad core or two dual core processors. 2.40 GHz with supported OS.
- A minimum of 4 GB of memory.
- A minimum of 2 GB of storage or hard disk space to install, and an average of 2 MB per client in the database.
- A minimum screen resolution of 800 by 600 pixels is required when you run an automated server installation.
- Adequate space for storing session video recordings. Recordings are stored on the hard disk and their size can vary depending on the duration and screen activity of the session. On average a 5-minutes session, 8-bits mode, can use about 2 MB of space. In true color 24-bit mode, recordings can take more space.
- A network card that supports TCP/IP.
- A supported browser.

Supported browsers

Verified browsers are:

- Mozilla Firefox
- Chrome
- Safari
- Edge

Operating system support

The following operating systems are supported.

- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ Server 2022
- Windows™ Server 2025
- Red Hat Enterprise Linux™ 7.0 or later
- Red Hat Enterprise Linux™ 8.0 or later
- Red Hat Enterprise Linux™ 9.0 or later
- SUSE Linux™ Enterprise Server 15

Supported Architectures

- Intel™ IA®-32 (also known as x86, x86-32)
- Intel™ 64 or AMD64 (also known as x64, x86-64, EM64T)

Note:

- IA®-64 (also known as Itanium™) processors are not supported.
- 32-bit support is for Windows™ only.

Supported databases

The following databases are supported.

- IBM DB2 11.5 Virtual Processor Core (VPC), IBM DB2 12.1.
- 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 2016, 2017, 2019, 2022, and 2025.

You must use a JDBC driver whose version is higher than or equal to 13.4. Older versions do not support TLS1.2 or JRE25.

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.

- Azure SQL managed Instance for Microsoft SQL Server 2022 database

Note: You must use JDBC drivers which support at least Java 25.

Note: Oracle is not supported when FIPS is enabled.

Derby Version 10.13 is included with the Remote Control server and is installed locally when you select the Derby option during the installation.

Note: Install Derby only for proof of concept configurations. Derby is not supported in production environments.

When you install the server by using the installer, a WebSphere Application Server Liberty Profile version is also installed.

Server environment guidelines

In addition to system requirements, you must also determine which type of server installation to use in your environment. Use the following information as a guide.

Table 1. Remote Control server installation types

Note: Server installation types 1 and 2 are available only when you use Windows® or Linux® operating systems.

Note: Server installation type 1 must be used only in Proof of Concept or test deployments.

The following sections provide guidance and recommendations based on environment size.

Small environment guidelines

For environments containing up to 5K targets, you can use server installation types 1, proof of concept only, or 2 in Server environment guidelines *(on page 18)*.

Also, consider the following extra requirements.

- Processors: 1 Quad core or 2 dual core processors, 2.40 GHz, with supported OS.
- Memory: 4 GB RAM.
- Storage. For more information, see Server requirements *(on page 16)*.
- Heartbeat configuration

Table 2. Heartbeat configuration properties: suggested values for a small environment

Property in `trc.properties`	Value
heartbeat.timeout	60 **Note:** If there are performance issues, set the value to 1440, which is 24 hours. For example, when there is heavy usage of reports, especially with Derby. Default is 60, which is 1 hour.
heartbeat.retry	10
heartbeat.delay	20
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

Note: Installation type 1 is suitable for demonstrations or pilot projects. Installation type 2 can give better performance, which might be preferred for production systems in these environments.

Medium environment guidelines

For environments containing from 5K to 75K targets, you can use server installation types 2 or 3 in Server environment guidelines *(on page 18)*. In terms of performance, installation type 2 is suitable. However, with installation type 3 you can also use the admin functions of the installed Open Liberty Application Server.

Also, consider the following extra requirements.

- Processors: 1 Quad core or 2 dual core processors, 2.40 GHz.
- Memory: 8 GB RAM.
- Storage: RAID 5 - 6 HDD. DB2, Oracle, or MS SQL 64 bit or 32 bit.
- Heartbeat configuration -

Table 3. Heartbeat configuration properties: suggested values for a medium environment

Property in `trc.properties`	Value
heartbeat.timeout	1440 **Note:** If there are specific groups of computers where more regular updates are needed, a smaller heartbeat timeout setting can be applied as a group attribute for those specific groups of targets. For details of setting this attribute at group level, see the chapter that explains how to create a target group in the *BigFix® Remote Control Administrator's Guide*.
heartbeat.retry	10 **Note:** In an environment that contains target numbers nearer to 75 K, set this value to 20 to help with performance.
heartbeat.delay	20 **Note:** In an environment that contains target numbers nearer to 75 K, set this value to 40 to help with performance.
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

Note: In this type of environment, ensure that the target deployment is done in stages. A staged deployment can avoid overload in the server when the targets try to register with the server. Give the **RegistrationDelay** target property a value that distributes the target computer registration evenly through the staged deployment. Distribute the target registration to avoid too many computers trying to register at the one time.

Large environment guidelines

For environments containing up to 250K targets, you can use server installation type 3 described in Server environment guidelines *(on page 18)*.

Note: 250K targets include a maximum number of 60K targets running in Unattended mode.

Also, consider the following extra requirements:

- End-to-end network latency below 50 ms across the whole environment (Server, Database, Broker, Targets).
- **Log Level** = `ERROR` on the Server. Higher log verbosity significantly increases I/O and reduces the supported total.
- Heartbeat configuration as defined in the Heartbeat configuration table, including **rc.unattended.heartbeat.interval.minutes** = `2` and **heartbeat.timeout** = `1440`.
- The Server runs on real physical hardware matching the specifications listed below. Performance can degrade on virtualized servers; an additional sizing margin is recommended in that case.

To host Open Liberty Application Server

- Processors: 2 Quad core processors. 2.40 GHz with supported OS.
- Memory: 16 GB RAM.
- Storage: Very fast SSD disks.
- Heartbeat configuration: See the table below.

Table 4. Heartbeat configuration properties: suggested values for a large environment

Property in `trc.properties`	**Value**
heartbeat.timeout[1]	1440
heartbeat.retry	60
heartbeat.delay	60
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0
rc.unattended.heartbeat.interval.minutes[2]	2

1. **Note:** If there are specific groups of computers where more regular updates are needed, a smaller heartbeat timeout setting can be applied as a group attribute for those specific groups of targets. For details of setting this attribute at group level, see the chapter that explains how to create a target group in the *BigFix® Remote Control Administrator's Guide*.

2. **Note:** Heartbeat interval, in minutes, used by Unattended-mode targets. Defined in the Unattended Target section of `trc.properties`. This value is part of the scalability baseline: lowering it increases Server overhead and reduces the supported total.

To host the database

- Processors: 4 Quad core processors, 2.40 GHz.
- Memory: As recommended by the database supplier.
- Storage: Very fast SSD disks (146 GB).

Note: The database administrator must tune the database for appropriate performance.

Additional guidelines for large reports

The following guidelines must also be considered when you use large reports, as some performance degradation can be experienced.

- Ensure that the **All targets** report is not the default home page report.
- Ensure staged deployment of the targets to avoid overload in the server when they try to register.

  Note: Give the **RegistrationDelay** target property a value that distributes the target computer registration evenly through the staged deployment. Distribute the target registration to avoid too many computers trying to register at the one time.

Note for LDAP: If you configure LDAP and LDAP synchronization is enabled, set a reasonable frequency for the synchronization. If your LDAP configuration is set up to import many users and groups, set the frequency to 24 hours. For more information about configuring LDAP, see Configure LDAP *(on page 112)*.

Note for Microsoft Entra ID: If you configure Microsoft Entra ID and Microsoft Entra ID synchronization is enabled, set a reasonable frequency for the synchronization. If your Microsoft Entra ID configuration is set up to import many users and groups, set the frequency to 24 hours. For more information, see Configure Microsoft Entra ID *(on page 130)*.

Controller requirements

The Controller is a Java™ based application that can run on the following operating systems with the listed prerequisites.

Operating system support

The following operating systems are supported:

- Windows™ 10
- Windows™ 11
- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ Server 2022
- Windows™ Server 2025
- Red Hat Enterprise Linux™ 7.0 or later
- Red Hat Enterprise Linux™ 8.0 or later
- Red Hat Enterprise Linux™ 9.0 or later
- SUSE Linux™ Enterprise Server 15 or later
- macOS 14.x Sonoma
- macOS 15.x Sequoia
- macOS 26.x Tahoe

Supported architectures

- Intel™ IA®-32 (also known as x86, x86-32)
- Intel™ 64 or AMD64 (also known as x64, x86-64, EM64T)
- Apple Silicon

Note:

- IA®-64 (also known as Itanium™) processors are not supported.
- 32-bit support is for Windows™ only.

Pre-requisites

- Oracle Java™ SE Runtime Environment 8 or IBM® Java™ SE Runtime Environment 8.

Note: Oracle Java™ is not supported in FIPS or NIST SP800-131a mode. You must use the IBM® Java™ in this mode.

Target requirements

Minimum requirements

The computer on which you install the Remote Control target must have at least the following specifications:

- At least a 1 GHz Intel™® or AMD processor.
- A minimum of 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit).
- A minimum of 50 MB hard disk space.
- Adequate space for storing session video recordings. Recordings are stored on the hard disk and their size can vary depending on the duration and screen activity of the session. On average a 5-minutes session, 8-bits mode, can use about 2 MB of space. In true color 24-bit mode, recordings can take more space.
- The maximum display resolution per display is 7680 pixels by 4320 pixels.
- The maximum number of displays is 8 by 8.

Network requirements

Before you install the Remote Control, ensure that the below network requirements are met:

- Incoming TCP connections to the Target port 888 (or any other port that is configured for the Remote Control sessions) must be allowed in the firewall rules.
- Traffic on the locahost loopback address 127.0.0.1 between `trc_base`, `trc_gui`, `trc_dsp` and `trc_ft` on ports between 49152 - 65535 must be allowed.

Note: Antivirus or Intrusion Detection System software might also block this traffic.

Operating system support

The following operating systems are supported:

- Windows™ 10
- Windows™ 11
- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ Server 2022
- Windows™ Server 2025
- Red Hat Enterprise Linux™ 7.0 or later
- Red Hat Enterprise Linux™ 8.0 or later (XORG Only)
- Red Hat Enterprise Linux™ 9.0 or later (XORG Only)
- SUSE Linux™ Enterprise Server 15 or later
- macOS 14.x Sonoma
- macOS 15.x Sequoia
- macOS 26.x Tahoe

Note: On macOS 11.1, ensure the monitor screen resolution is set to one of the following: 1280 x 768, 1280 x 800, 1280 x 1024, 1360 x 768, 1440 x 900, 1600 x 900, 1680 x 1050, 1920 x 1080, or 2880 x 1800. This is because, the following screen resolutions can result in a black screen on the Controller during a remote session: 1400 x 1050, 1768 x 992.

Supported architectures

- Intel™ IA®-32 (also known as x86, x86-32)
- Intel™ 64 or AMD64 (also known as x64, x86-64, EM64T)
- Apple Silicon

Note:

- IA®-64 (also known as Itanium™) processors are not supported.
- 32-bit support is for Windows™ only.

Gateway requirements

The computer on which you install the Remote Control gateway must have the minimum following items or specification:

1. At least a 1 GHz Intel® or AMD processor.
2. A minimum of 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
3. A minimum of 50 MB hard disk space.

Operating system support

The following operating systems are supported:

- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ Server 2022
- Windows™ Server 2025
- Red Hat Enterprise Linux™ 7.0 or later
- Red Hat Enterprise Linux™ 8.0 or later
- Red Hat Enterprise Linux™ 9.0 or later
- SUSE Linux™ Enterprise Server 15

Supported Architectures

- Intel™ IA-32 (also known as x86, x86-32)
- Intel™ 64 or AMD64 (also known as x64, x86-64, EM64T)

Note:

- IA-64 (also known as Itanium™) processors are not supported.
- 32-bit support is for Windows™ only.

Broker requirements

The hardware needed by the Remote Control Broker depends on how the Broker is used: for On-Demand sessions only, or to serve a population of Unattended-mode targets.

Scope and assumptions

The figures provided on this page are valid only under the following conditions:

- Sessions are established from the standalone Controller application. No validated figures are available when sessions are established from the Web Controller.
- The Broker runs on real physical hardware matching the specifications listed below. **Performance can degrade on virtualized servers; an additional sizing margin is recommended in that case.**
- Broker performance is driven mainly by the number of available CPU cores. Adding cores improves throughput more than adding RAM, provided the minimum RAM listed for the target population is met.

Reference environment configuration

The figures on this page were measured with the Remote Control environment configured as follows. The same configuration is assumed when applying the Broker sizing in a real deployment; significant deviations from these values can change the supported workload.

Table 5. Reference environment configuration

Property	Value	Location	Purpose
rc.unattended.heartbeat.interval.minutes	2 mins	trc.properties (Server)	Heartbeat interval used by Unattended-mode targets.
heartbeat.timeout	1440 mins	trc.properties (Server)	Time after which a target is marked offline if no heartbeat is received.
LogLevel	ERROR	trc.properties (Server)	Server log verbosity. Keep I/O overhead under control.
LogLevel	1	trc_broker.properties (Broker)	Broker log verbosity. Default is 2; lower to 1 to keep I/O overhead under control.

When the broker is used for On-Demand sessions only:

- Processor: at least 1 GHz, on a supported operating system.
- Memory: 4 GB RAM (32-bit) or 8 GB RAM (64-bit) minimum.
- Disk: 120 MB minimum.
- Additional disk space for session video recordings. Recordings are stored temporarily; size depends on session length and on-screen activity. As a reference, a 5-minute session at 8-bit color uses about 2 MB; 24-bit true color recordings require more space.

When the broker is used for Unattended Targets up to 10000 - 16000 targets:

- Processor: two Quad core processors at 2.40 GHz, on a supported operating system.
- Memory: 4 GB RAM (32-bit) or 8 GB RAM (64-bit) minimum.
- Disk: 1 GB minimum.
- Additional disk space for session video recordings. Recordings are stored temporarily; size depends on session length and on-screen activity. As a reference, a 5-minute session at 8-bit color uses about 2 MB; 24-bit true color recordings require more space.
- Up to 10K Unattended targets set **rc.unattended.heartbeat.interval.minutes** = 2 (default).
- Up to 16K Unattended targets set **rc.unattended.heartbeat.interval.minutes** = 4.

Operating system support

The following operating systems are supported:

- Windows™ Server 2016
- Windows™ Server 2019
- Windows™ Server 2022
- Windows™ Server 2025
- Red Hat Enterprise Linux™ 7.0 or later
- Red Hat Enterprise Linux™ 8.0 or later
- Red Hat Enterprise Linux™ 9.0 or later
- SUSE Linux™ Enterprise Server 15 or later

Supported Architectures

- Intel™ 64 or AMD™64 (also known as x64, x86-64, EM64T)

Note: IA-64 (also known as Itanium™) processors are not supported.

Chapter 3. Get started

Now that you understand the terms and components available in Remote Control, you can identify which components you need to install:

Table 6. Determining which components to install

Requirements	Target	Controller	Server	Gateway	Broker
I want others to remotely connect to this computer.	Yes	Yes			
I want to remotely connect to other computers by using the Remote Control console or by starting the standalone controller.	Yes	Yes			
To centrally manage users and targets, and their policies.	Yes	Optional *	Yes		
To maintain a central audit and recording repository.	Yes	Optional *	Yes		
Traverse firewalls in your company infrastructure	Yes	Optional *	Yes	Yes	
Connect to targets outside your company network.	Yes	Optional *	Yes	Yes **	Yes

* In a managed environment, the controller user starts remote control sessions from the Remote Control server interface. Starting sessions this way does not require the controller component to be installed separately. The Remote Control server interface starts a Java Web Start controller console, in context.

** A gateway is not strictly required in a broker deployment but it does increase security.

Chapter 4. Install the Remote Control components

The Remote Control components can be installed in two ways. If you have access to the BigFix® console, use a deployment fixlet to install the components.

For more information, see the *BigFix® Remote Control Console User's Guide*. Alternatively use the component installation files.

You can obtain the installation files in various ways. Choose the appropriate method for obtaining the files. There is no specific order in which the different components must be installed.

Obtain the installation files

The installation files for installing the Remote Control components can be obtained in various ways.

HCL License & Delivery Portal

To install the Remote Control components, download the images from My HCLSoftware.

Note: IBM Passport Advantage® and Fix Central® were replaced by FlexNet Operations®. Now FlexNet Operations® has been replaced by My HCLSoftware®.

Downloading the files from the server UI

If you install the Remote Control server, you can download the installation files for the target, controller, and cli components. The controller installation file is for the standard controller. For the FIPS-compliant controller installation file, use the additional setup utility.

1. Click **Tools > Downloads**.
2. Select **Agent Downloads**.
3. Select the relevant component file.

Install the server

Remote Control server supports the following installation types:

Table 7. Server installation types

Automated installation - For more information, see Installing by using the server installer *(on page 36)*	**Manual Installation - For more information, see Installing on WebSphere Application Server version 8.5.5: deploying the war file *(on page 44)***
Available on Windows® operating system and Linux operating system.	Available on any operating system that WebSphere Application Server 8.5 supports.
Derby is installed as embedded or uses existing supported database. Local or remote.	Database must be created or an existing supported database can be used.

Table 7. Server installation types (continued)

Automated installation - For more information, see Installing by using the server installer *(on page 36)*	Manual Installation - For more information, see Installing on WebSphere Application Server version 8.5.5: deploying the war file *(on page 44)*
All embedded components are installed locally on the same computer.	The database can be installed on a separate computer.

Note: The embedded Derby database is not supported in production.

Set up the database

Before you set up the database, install the database software and create the instance where the database for Remote Control is held.

Setting up DB2®

To perform the database setup for DB2® complete the following steps. If you are using a Windows® operating system, begin from step 2 *(on page 30)*. If you are using Linux® operating system begin from step 1 *(on page 30)*:

1. To verify that DB2® and the instance are ready for remote connectivity using TCP/IP complete the following steps:
    a. Run `db2 get database manager configuration` and verify that the value of **svcename** is a valid port.

    ```
    for example 50000


    or a reference mapped to a valid port
    for example,db2c_db2inst1.
    ```

    b. Ensure that the configured port is not used by other processes in the system, or blocked by a firewall that sits between the Application Server host and the DB2® server.

    c. Use the `db2stop` command to stop the DB2® instance.

    Set **DB2COMM** to tcpip with the command

    ```
    db2set DB2COMM=tcpip
    ```

    Run db2start to start the DB2® instance again.

    The DB2® server is now ready for accessing over the network.
2. Create the database that Remote Control will use by running the following command as the instance owner:

Note: Not necessary when the database is local.

```
db2 create db databasename using codeset UTF-8 territory requiredtrerritory
```

where *databasename* is the name required for the database. This database name must be the name that was referenced in any configuration settings. For example, TRCDB.

requiredterritory is the required territory. For example, GB for Great Britain.

3. Verify the privileges that a specific user, for the database, needs to have.
   Do not use the **db2inst1** user as the user configured to access the Remote Control database. Create a new specific user for DB2® that has the database owner privileges.

With the blank database created and ready to use, the next step is to set up the Open Liberty® server, see Setting up the application server *(on page 45)*. It is possible to verify that the database is set up properly by using a DB2® client to connect to the database from another host. For more details see the DB2® Infocenter.

Setting up Oracle

To set up Oracle to use with Remote Control, create the database and then set up the database permissions.

Creating the database

Run the Oracle database configuration assistant to create the database.

To create the Oracle database that will be used for Remote Control, complete the following steps:

1. Run the Oracle database configuration assistant.

   Windows® systems

   For example, Select **Start > All Programs > Oracle > Configuration and Migration Tools > Database Configuration Assistant**.

   UNIX®-based systems

   Enter the command dbca from the `$ORACLE_HOME/bin` directory.

2. Click **Next** on the welcome screen.
3. **Step 1**: Select **Create a Database**. Click **Next**.
4. **Step 2**: Select **General Purpose** for the template. Click **Next**.
5. **Step 3**:
   a. Specify a name for the database. For example, TRCDB.
   b. Specify an SID to be used to reference the database. For example, TRCDB.

   Click **Next**.

6. **Step 4**: Select the database management option that you require. For example, **Use Database Control for Database Management**. Click **Next**.
7. **Step 5**: Specify a password for the database and confirm the password. For example, `dboracle`. Click **Next**.
8. **Step 6**: Specify where the database will be stored. For example, `File System`. Click **Next**.
9. **Step 7**: Specify locations for the database files. For example, `Use Database File Locations from Template`. Click **Next**.
10. **Step 8**: Select the recovery options for the database. Click **Next**.
11. **Step 9**: On the Database Content window, click **Next**.
12. **Step 10**: On the Initialization Parameters screen select the **Character Sets** tab.
    a. Select the required Database Character Set
    b. Click **Next**.
13. When you are using Oracle 11g, the following two steps are also required.
    a. Security Settings, accept the enhanced 11g default security settings.
    b. Automatic Maintenance Tasks, enable automatic maintenance tasks.
14. **Step 11**: On the Database Storage window click **Next**.
15. **Step 12**: Select the required Creation Options. Click **Finish**.
16. On the Confirmation screen, click **OK** to start the database creation.

    Note: This may take some time as it goes through the different stages.

17. Click **Exit** when the database creation is complete.

The Oracle database that will be used for Remote Control is created.

Setting up database permissions

When you have created the Oracle database that will be used for Remote Control you will need to configure its permissions.

To configure the database permissions complete the following steps:

1. Run Oracle SQL*Plus.

   Windows® systems

   For example: Click **Start > Programs > Oracle-OraHomeName > Application Development > SQL Plus**.

   Alternatively, enter the following command at a command prompt.

   sqlplusw

   Log on using the database user name and password and click **OK**. See your database system administrator if you do not have this.

   For example:

Username - system

Password - dboracle

Linux® systems

Open a UNIX® or a Windows® terminal and enter the SQL*Plus command:

sqlplus *username* / *password* *@connect_identifier*

username and *password* are the database credentials required to connect to the database.

connect_identifier is the connection required for your specific database.

For example, @TRCDB as SYSDBA

@//servername:port/DatabaseSID as SYSDBA

servername is the server name or IP address of the system where your Oracle installation is located.

port is the port of the system where your Oracle installation is located.

DatabaseSID is the SID defined for the database you created.

The SQL*Plus executable is installed in `$ORACLE_HOME/bin`, which is included in your operating system PATH environment variable. You may need to change directory to the `$ORACLE_HOME/bin` directory to start SQL*Plus.

2.

After SQL*Plus has started and connected to the database you can create the required users and grant permissions. There are two methods for creating users and granting permissions. Choose the appropriate method for creating the users.

Create one user ID in Oracle which will also be used to log on to Remote Control.

Create a single user. The user must be called Asset. This user ID is used by Remote Control to create and log on to the database, and use the database.

Issue the following commands to create the user ASSET.

a. connect SYS/PASSWORD@DATABASE AS SYSDBA;

   where *PASSWORD* is the default Oracle user password.

   and *DATABASE* is the database name that was defined when creating the database. For example, TRCBD.

b. CREATE USER ASSET IDENTIFIED BY PASSWORD DEFAULT TABLESPACE users TEMPORARY TABLESPACE temp;

Note: PASSWORD can be changed to whatever you require, for the user ASSET.

c. GRANT UNLIMITED TABLESPACE TO ASSET;
d. GRANT CONNECT TO ASSET;
e. GRANT CREATE INDEXTYPE TO ASSET;
f. GRANT CREATE SEQUENCE TO ASSET;
g. GRANT CREATE TABLE TO ASSET;
h. GRANT CREATE TRIGGER TO ASSET;
i. GRANT CREATE INDEXTYPE TO ASSET;
j. GRANT CREATE PROCEDURE TO ASSET;
k. GRANT CREATE VIEW TO ASSET;
l. GRANT ANALYZE ANY TO ASSET;

Create a separate user ID to log on to Remote Control

Create 2 users. User 1 must be called Asset. This user has no specific permissions and is used only as a schema name. User 2 is the main user and can be called anything you require. This user is used by Remote Control to create and logon to the database, and use the database. Use the assistant tool to create user TRCDBU.

Complete the following steps to create the required permissions for user TRCDBU.

a. GRANT UNLIMITED TABLESPACE TO ASSET;
b. GRANT UNLIMITED TABLESPACE TO TRCDBU;
c. GRANT ALTER ANY INDEX TO TRCDBU ;
d. GRANT ALTER ANY INDEXTYPE TO TRCDBU ;
e. GRANT ALTER ANY PROCEDURE TO TRCDBU ;
f. GRANT ALTER ANY SEQUENCE TO TRCDBU ;
g. GRANT ALTER ANY TABLE TO TRCDBU ;
h. GRANT ALTER ANY TRIGGER TO TRCDBU ;
i. GRANT COMMENT ANY TABLE TO TRCDBU ;
j. GRANT CREATE ANY INDEX TO TRCDBU ;
k. GRANT CREATE ANY INDEXTYPE TO TRCDBU ;
l. GRANT CREATE ANY SEQUENCE TO TRCDBU ;
m. GRANT CREATE ANY TABLE TO TRCDBU ;
n. GRANT CREATE ANY TRIGGER TO TRCDBU ;
o. GRANT CREATE INDEXTYPE TO TRCDBU ;
p. GRANT CREATE PROCEDURE TO TRCDBU ;
q. GRANT CREATE SEQUENCE TO TRCDBU ;
r. GRANT CREATE TABLE TO TRCDBU ;
s. GRANT CREATE TRIGGER TO TRCDBU ;
t. GRANT CREATE VIEW TO TRCDBU ;
u. GRANT DELETE ANY TABLE TO TRCDBU ;

v. GRANT INSERT ANY TABLE TO TRCDBU;
w. GRANT DROP ANY INDEX TO TRCDBU ;
x. GRANT DROP ANY INDEXTYPE TO TRCDBU ;
y. GRANT DROP ANY PROCEDURE TO TRCDBU ;
z. GRANT DROP ANY SEQUENCE TO TRCDBU ;
aa. GRANT DROP ANY TABLE TO TRCDBU ;
ab. GRANT DROP ANY TRIGGER TO TRCDBU ;
ac. GRANT EXECUTE ANY INDEXTYPE TO TRCDBU ;
ad. GRANT EXECUTE ANY LIBRARY TO TRCDBU ;
ae. GRANT EXECUTE ANY TYPE TO TRCDBU ;
af. GRANT SELECT ANY SEQUENCE TO TRCDBU ;
ag. GRANT SELECT ANY TABLE TO TRCDBU ;
ah. GRANT UNLIMITED TABLESPACE TO TRCDBU ;
ai. GRANT UPDATE ANY TABLE TO TRCDBU;
aj. GRANT ANALYZE ANY TO TRCDBU;

Setting up MSSQL

To set up MS SQL to use with Remote Control, create the database and then set up the database permissions.

Creating the database

Use the MS SQL management studio to complete the following steps:

1. Click **Connect**.
2. Right-click the **server tree** and click **properties**.
3. Select **security**.
4. Ensure that SQL server and authentication mode is selected.
5. Expand the **server tree**.
6. Right-click **databases**.
7. Select **Create New Database**.
8. Enter a name for the database. For example, TRCDB. Click **OK**.

The default owner of the database is user *sa*, the system administrator. Create a new user, to be the owner of the database being used with Remote Control.

Database permissions

The default system administrator is the owner of the database and therefore has the required permissions for using the database. If you have created a new user, they also have the required permissions if they have been assigned as the owner of the database.

Installing by using the server installer

The Remote Control server installer can be used on Windows™ operating systems, Red Hat Linux™ operating systems, and SUSE Linux™ operating systems. A fully functional self-contained server with either of the following component setup is installed.

- 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), IBM DB2 12.1.
  - 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 2016, 2017, 2019, 2022, and 2025.

    You must use a JDBC driver whose version is higher than or equal to 13.4. Older versions do not support TLS1.2 or JRE25.

    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.
  - Azure SQL managed Instance for Microsoft SQL Server 2022 database

For more information about the supported versions of the installed components, see Server requirements *(on page 16)*

Note: Click **Cancel** at any time to end the installation.

Approximate installation time

- Specifying options in the installer: 5 - 10 minutes.
- Installation of the software: 5 minutes.

1. A minimum screen resolution of 1024 by 768 pixels is recommended when you are using the installer.
2. On a Linux™ operating system, you must install **libstdc++.so.5** when you are installing and configuring the operating system. If this package is not installed, you can install package **compat-libstdc++-33**, which contains **libstdc++.so.5**.

Note:

- Console mode installation is not supported.
- During the file copy phase of the server installation:

- A backup copy of any existing installation is saved. This feature is useful if a problem occurs with the installation when you are upgrading.
- The following directory is deleted if it exists:

  `[INSTALLDIR]/trcserver.bak`.
- The current server installation in `[INSTALLDIR]/wlp/usr/servers/trcserver` is then renamed or moved to `[INSTALLDIR]/trcserver.bak`.

You can access the backup directory to restore or recover anything from the previous installation.

To install the Remote Control server application, complete the following steps:

1. Run the server installation file relevant to your operating system.

   Windows™ systems

   `trc_server_setup.exe`

   Linux™ systems

   `trc_server_setup.bin`

   To obtain the installation file see Obtain the installation files *(on page 29)*.
2. Choose the language and click **OK**.
3. At the **Introduction** window click **Next**.
4. Click to accept both the IBM® and non-IBM® terms, click **Next**.
5. Accept the default location or click **Choose** to define a location for the installation files, click **Next**.

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

6. Select the database, click **Next**.

   Note: Derby is embedded in the application and is installed locally when you select Derby. To use DB2® or Oracle, you must install them and create a database instance before you install Remote Control.

7. Enter the options for your selected database and click **Next**.

   Derby

a. Specify a name for the database, click **Next**. For example, `TRCDB`.

Note: If you are using an existing database, you can choose to drop the database.

DB2®

Database server

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

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.

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.

If you select **create database**, the user ID must have administrator access for DB2®.

Administrator password

Specify the Administrator password for connecting to the database.

Database Name

Specify a name for the database. For example, `TRCDB`.

Note: If you are using a remote database, type the name of the database that was created on the remote system.

Directory path to db2jcc.jar file

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

Note: If you are using a remote database share the drive, on the remote system, that the DB2® JAR files are in. Enter the shared drive location.

Create 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.

Path for database install

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.

Oracle

Database server

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

Port on which Oracle is installed.

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.

Administrator password

Specify the administrator password for connecting to the database.

Database Name

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

Directory path to the oracle Java JDBC library

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`

MSSQL

Database server

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

Port on which MS SQL is installed.

Administrator Userid

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

Administrator password

Specify the administrator password for connecting to the database.

Database Name

Specify a name for the database. For example, `TRCDB`.

Directory path to the MS JDBC Java files

Specify the path to the MS JDBC Java files. The `mssql-jdbc-X.X.X.jre11.jar` file must be used depending on the version of MS SQL database that you are using.

If installed on the same server, select to create database

If MS SQL is installed locally, you can select to create the database.

Drop the database if installed locally

Select if you already have an existing database with the name that is entered for **Database Name** that you do not want to use.

If local, select path where to create the database

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.

8. Specify the web server parameters then click **Next**.

Force targets to use HTTPS

Select this option for the target software to communicate with the server by using the HTTPS URL. The **enforce.secure.endpoint.callhome** and **enforce.secure.endpoint.upload** properties in the `trc.properties` file are also set to *true*. The check box is selected by default on a new installation.

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*.

Note: If you are using HTTPS, you must use a fully qualified domain name for the server name.

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. The check box is selected by default on a new installation. Ensure that the **Force targets to use HTTPS** option is also selected. For more information about secure registration, see Enable secure target registration *(on page 99)*.

Upload data to server

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

Note: You must make sure that you enter the fully qualified name. The name is used for creating the URL in the `trc.properties` file that is passed to the target after it contacts the server for the first time. If the fully qualified name is incorrect, the target might not be able 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. For example, `/trc`.

Server port on Webserver (default 80)

Specify a port for the server.

SSL Port (default 443)

Specify a port for SSL.

Administrator email

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

Note: To use the email function, you must install a mail server. Edit the `trc.properties` file after you install the Remote Control server. For more information about editing the properties files, see the *BigFix® Remote Control Administrator's Guide*

Enable FIPS

Select this option to enable FIPS compliance on the server. For more information about enabling FIPS compliance, see Federal information processing standard (FIPS) compliance in Remote Control *(on page 139)* .

Enable NIST SP800-131A Compliance (Enables FIPS)

Select this option to enable NIST SP800-131A compliance on the server. For more information about enabling NIST SP800-131A compliance, see NIST SP800-131A compliance in Remote Control *(on page 148)*.

9. Select options for your SSL certificate and click **Next**. The certificate configuration is stored in the `ssl.xml` file.

Use an auto generated certificate store

Select this option to use a self-signed certificate that is generated by the installer.

Note: If the following options are not enabled, click **Use an auto generated certificate store** to enable them.

Overwrite an existing certificate store.

If a self-signed certificate store is already saved, the new certificate overwrites the saved certificate store. This option is the default option.

Password for a new or a previously generated certificate store.

Type a new password for the self-signed certificate. If you do not select to overwrite, type the password for your existing auto generated certificate store.

If left blank, the default password **TrCWebAS** is saved as the password. The password must have a minimum of 6 characters.

Select an existing certificate store

Select this option to use an existing certificate store that is already saved.

Select existing certificate store location.

Click **Choose** to browse to the relevant certificate store. Select the certificate store. The file extension can be `.jks` or `.p12`.

Note: If FIPS is enabled then only a `.p12` keystore can be used for security reasons.

When you use an existing certificate store, it is not copied to the installation directory during installation. The server software instance points to the location of the certificate store that you provide. Therefore, you must make sure that you save the certificate store to an adequate location on the server before you start the server installation. The certificate store must be stored in a location that does not get deleted. Therefore, do not save the file in the *`[installdir]`*`\wlp` directory or any of its subdirectories. Do not delete the certificate store at the end of the installation.

If you select a previously saved auto-generated certificate store from the server installation directory, a warning is displayed. Choose **Copy file** to copy the file to a location that is not deleted during the installation. If the file is not copied successfully, you must manually copy the certificate store file to another location. Click **Choose** and select the new location of the file.

Click **Restore Default** to reset the field value to its original value.

Enter the certificate store password.

Type a password for the certificate store.

10. Select options to configure Single-Sign-On (SSO) and click **Next**. The SSO configuration is stored in the `sso.xml` file.

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.

11. Select a location for the product icons to be displayed.
    If you select Other, click **Choose** to specify a location.

    Note: Product icons do not work when you are using Linux™.

12. In the **Summary** pane, click **Install**.
13. If you selected to enable SSO, a pane that is labeled as **Important** is displayed. Take note of the URL and information and click **Next**.
14. Click **DONE** to complete the installation.

The Remote Control server software is installed including a set of properties files. These files can be edited to configure your environment.

Note:

1. It is important to make sure that the **URL** property in the `trc.properties` file contains the correct URL for the Remote Control server. This property is used when targets contact the server and for determining the server during a remote target installation. If the URL property value is not correct, the remote targets are not able to contact the server successfully. Therefore, you might have problems when you start remote control sessions with the targets.
2. If the IP address of the server changes at any time, make sure that you update the URL property in `trc.properties`. Restart the server service because the targets try to contact to the old IP address until the change to the property is made.

Installing on WebSphere Application Server version 8.5.5: deploying the war file

As described in the prerequisites section, a database needs to be created for Remote Control. After the database is created, add it to the WebSphere® data sources.

Setting up the application server

It is necessary to create the WebSphere profile in a folder that does not include any spaces in its path. Otherwise, unrecoverable issues might occur when you deploy the application war file.

Use the **WebSphere Integrated Solution Console** to configure the application server.

To access the Integrated Solution Console, complete the following steps:

1. In your browser type

   ```
   https://[server : port]/ibm/console
   where server is the IPaddress or name for the application server machine
   for example localhost or 192.0.2.0
   and port is the port that the server is listening on.
   ```

   The default port for the WebSphere Application Server admin console is 9060.
2. Log on with the ID and password that you defined when you installed WebSphere.

DB2® configuration

Creating DB2 database authentication data

Creating authentication data for connecting to an Remote Control DB2 database

Credentials to use for the database connection need to be established and added as a new entry to the JAAS-J2C authentication data.

To create an entry complete the following steps:

1. Click **Security > Global Security**.
2. On the right of the screen, expand **Java™ Authentication and Authorization Services** .
3. Click **J2C authentication data**.
4. Click **New** to add a new entry.
5. Supply the following information:

   Alias

   Specify a name for the authentication alias.

   Userid

   Type the user ID that was defined when DB2® was installed. Can be one of the following users.

- The user who has permissions to access the TRCDB database, if a specific user was created.
- The DB2® owner instance, **db2admin** in a Windows® system and **db2inst1** in UNIX® / Linux® system.

Password

Type the password that you defined when you installed DB2®.

6. Click **OK**.
7. Click **Save**.

Verifying the Websphere variables

The JDBC Provider uses WebSphere® environment variables to define the paths to the JDBC driver JAR files.

- db2jcc.jar
- db2jcc-javax.jar
- db2jcc-license_cu.jar
- db2jcc4.jar. If available.

Verify that the correct values are defined by completing the following steps:

1. Select **Environment / WebSphere® Variables**.
2. Click **DB2UNIVERSAL_JDBC_DRIVER_PATH** and verify that this points to the DB2® libraries.

Local DB2® database

If you have installed the DB2® database locally the files are located in

Windows® systems

```
\Program Files\ibm\sqllib\java
```

Linux® systems

```
/opt/ibm/db2/VERSION/java
 where VERSION is the DB2 version number
for example: /opt/ibm/db2/V8.1/java
```

Remote DB2® database

If you are using a remote DB2® database you must copy the jar files from the remote system to a location on your local system and put the path to the local files here.

3. Click **OK**.
4. Click **Save**.

Creating the DB2 data source

When you have verified that the JDBC Provider is configured properly, the data source for Remote Control must be created using that JDBC Provider.

To create the data source complete the following steps:

1. Select **Resources > JDBC > Data Sources**.
2. Select the scope from the drop down menu that includes the node and the server.
   For example, Node=TEST-2008Node02, Server=server1.
3. Click **New**.
4. Specify the data source information.

    a. Enter basic data source information

    Data source name

    Specify a name for the data source. This can be any required name.

    JNDI Name

    This should be set to `jdbc/trcdb`

    Note: If this name is changed, you need to change the **common.properties** file also.

    b. Select JDBC Provider

    The data source will use the Universal JDBC Provider for DB2 that is predefined in WebSphere.

    i. If **DB2 Universal JDBC Driver Provider** is available, select **Select an existing JDBC provider** from the list. If it is not available, click **Create new JDBC provider**.
    ii. In the Database type list, select **DB2**.
    iii. Select **DB2 universal JDBC Driver provider**.
    iv. From the **Implementation type** list, select **Connection pool data source**.
    v. Click **Next**.
    vi. Accept the default values and click **Next**.

    c. Enter database specific properties for the data source

    Driver Type

    Select 4 from the list.

    Database name

    This is the name used when the **db2 create db** command was issued.

    Server name

    This is set to the IP or host name of the server where DB2® is installed. If DB2 is installed locally you can use localhost.

Port number

This is set to the port that was configured in DB2® for remote connections.

Click **Next**.

d. Setup security aliases
   i. From the **Component-managed authentication alias** list, select *your node*/DB2 where *your node* is the node you previously created for DB2.
   ii. Accept the default of **none** in the remaining lists.
   iii. Click **Next**.

e. Review the summary and click **Finish**.

5. To save the configuration changes, click **Save**.

When the data source has been created and the changes to the profile are saved, test that the data source is correctly configured. Select the data source from the list of data sources and click Test connection. If the connection is successful, a conformation message is displayed. A failure in the test should be corrected before continuing with the installation, as Remote Control will not work without a valid data source.

Oracle configuration

Creating Oracle database authentication data

Credentials to use for the database connection need to be established and added as a new entry to the JAAS-J2C authentication data.

To create an entry complete the following steps:

1. Click **Security > Global Security**.
2. On the right of the screen, expand **Java™ Authentication and Authorization Services** .
3. Click **J2C authentication data**.
4. To add a new entry, click **New** .
5. Supply the following information:

Alias

Specify a name for the authentication alias.

Userid

Type the ID that was defined when the Oracle database was created.This is the user that you created permissions for.

Password

Type the password that was defined when Oracle was installed.

6. Click **OK**.
7. Click **Save**.

Creating the Oracle JDBC provider

To establish access to your Oracle database you must create a JDBC provider for Oracle access.

To create the JDBC provider complete the following steps:

1. Select **Resources > JDBC > JDBC Provider**.
2. Select Scope and choose the one which has Node and Server.
3. Click **New**.
4. Specify the JDBC provider information

   Database type

   Set to `Oracle`.

   Provider Type

   Set to `Oracle JDBC Driver`.

   Implementation type

   Set to Connection Pool datasource.
5. Click **Next**.
6. The Class path is already pre-populated as `${ORACLE_JDBC_DRIVER_PATH}/ojdbc6.jar`. The directory location for `${ORACLE_JDBC_DRIVER_PATH}` to the jar files must be correct. This can be obtained from the Oracle server installation or downloaded from the Oracle website. For example, `C:\app\Administrator\product\11.2.0\dbhome_1\jdbc\lib`. Click **Next**.
7. Click **Finish**.
8. Click **Save**.

Verifying the Websphere variables

The JDBC Provider uses WebSphere® environment variables to define the paths to the JDBC driver JAR files. Verify that the correct values are defined by completing the following steps:

1. Select **Environment / WebSphere® Variables**.
2. Click **ORACLE_JDBC_DRIVER_PATH**
   and verify that this points to the directory location chosen in step 6 *(on page 49)* in the Creating the Oracle JDBC Provider section.
3. Click **OK**.
4. Click **Save**.

Creating the Oracle data source

When you have verified that the JDBC Provider is configured properly, the data source for Remote Control must be created using that JDBC Provider.

To create the data source complete the following steps:

1. Select **Resources > JDBC > Data Sources**.
2. Select the scope with Node and Server.
3. Click **New**.
4. Specify the data source information

    a. Specify the data source information.

    Data source name

    Specify a name for the data source. This can be any required name.

    JNDI Name

    This should be set to `jdbc/trcdb`

    Note: If this name is changed, further changes to the **common.properties** file are also required.

    Click **Next**.

    b. Select JDBC provider

    Click **Select Existing JDBC provider** and select **Oracle JDBC Driver**. Click Next.

    c. Enter database specific properties for the data source.

    URL

    url=jdbc:oracle:thin@*dbserver*:1521:*SID*

    where *dbserver* is the IP address of the server.

    SID is the Oracle database SID.

    Data store helper class name

    Accept the default Data store helper class name, **Oracle 11g.data store helper**.

    Accept remaining default selected values and click **Next**.

    d. Set up security aliases

i. Select **Component-managed authentication alias** and select the alias you previously created for Oracle.
ii. Accept the default of **none** in the remaining lists.
iii. Click **Next**.

e. On the summary screen, click **Finish** to create the data source.

5. Click **Save**.

You can select the newly created datasource and click **Test**, to test connectivity.

MS SQL configuration

Creating authentication data

Credentials to use for the database connection need to be established and added as a new entry to the JAAS-J2C authentication data.

To create an entry complete the following steps:

1. Click **Security > Global Security**.
2. On the right, expand **Java™ Authentication and Authorization Services** .
3. Click **J2C authentication data**.
4. To add a new entry, click **New**.
5. Supply the following information:

Alias

Specify a name for the authentication alias.

Userid

Type the ID that was defined when MS SQL was installed. This is the user that you created permissions for. Default is **sa**.

Password

Type the password that was defined when MS SQL was installed.

6. Click **OK**.
7. Click **Save**.

Creating the JDBC provider

To establish access to your MS SQL database you must create a JDBC provider for MS SQL access.

To create the JDBC provider complete the following steps:

1. Select **Resources > JDBC > JDBC Provider**.
2. Select **Scope** and choose the one which has Node and Server.

3. Click **New**.
4. Specify the JDBC provider information.

   Database type

   Set to `SQL Server`.

   Provider Type

   Set to `Microsoft JDBC Driver .`
5. Select Connection pool data source.
6. Click **Next**.
7. To accept the path to the jar files, click **Next**.
8. Click **Finish**.
9. Click **Save**.

Verifying the Websphere variables

The JDBC Provider uses WebSphere® environment variables to define the paths to the JDBC driver JAR files. The correct jdbc driver software must be downloaded from Microsoft. The following version is recommended:

Microsoft JDBC Driver 4.0 for SQL Server - sqljdbc_4.0.2206.100_enu.exe

Download the SQL Server jdbc driver and copy it to the root drive of the server. Run the file to extract the driver. The `sqljdbc4.jar` file is extracted to the following directory structure:

C:*extract_path*\sqljdbc_4.0\enu\

where *extract_path* is the directory chosen when you unzipped the file.

Note: The path cannot contain any spaces.

Verify that the correct values are defined by completing the following steps:

1. Select **Environment / WebSphere® Variables**.
2. Click **MICROSOFT_JDBC_DRIVER_PATH** and verify that this points to the Microsoft SQL Server JDBC driver, sqljdcb4.jar file that you extracted.
3. Click **OK**.
4. Click **Save**.

Creating the MS SQL data source

When you have verified that the JDBC Provider is configured properly, the data source for Remote Control should be created using that JDBC Provider.

To create the data source complete the following steps:

1. Select **Resources > JDBC > Data Sources**.
2. Select the scope with Node and Server.
3. Click **New**.
4. Specify the data source information

    a. Enter basic data source information

    Data source name

    Specify a name for the data source. This can be any required name.

    JNDI Name

    This should be set to **jdbc/trcdb**

    Note: If this name is changed, the **datasource.context** property in the `common.properties` must be changed after the WAR file is deployed. After the correct value is set, save the file and restart the application from the Websphere admin console.

    b. Select JDBC provider

    Select **Microsoft SQL Server JDBC Driver** or the required JDBC provider. Click **Next**.

    c. Enter database specific properties for the data source

    Database name

    This is the name used when you created the MS SQL database.

    Port number

    Port used when installing MS SQL. Default is 1433.

    Server name

    This is set to the IP or hostname of the server containing the MS SQL installation. If MS SQL is installed locally you can use localhost.

    d. Set up security Alias

    i. Select **Component-managed authentication alias** and select the alias you previously created for MS SQL.

    ii. Accept the default of **none** in the remaining lists.

    iii. Click **Next**.

    e. On the summary screen, click **Finish** to create the data source.

5. Click **Save**.

Deploying the Remote Control application

After you install and set up the application server, deploy the application code for Remote Control on the WebSphere® server. You require the `trc.war` file that can be obtained by using the additional setup utility to extract the server installation media.

Note:

1. The heap size must be set to at least 512 MB for this type of installation.

To deploy the server application, complete the following steps:

1. Extract the `trc.war` file by using the additional setup utility. For details about the files that are required and for running this utility, see Utility for extracting the component installation files *(on page 97)*.
2. In the WebSphere administrative console complete the following steps:
    a. Select **Applications > New Applications**.
    b. Click **New Enterprise Application**.
    c. Click browse and type the path to the **trc.war** file in a local or remote file system. Click **Next**.
    d. On the **Preparing for the application installation** screen, select **Fast path**. Click **Next**
    e. **Step 1: Installation options**
    The default options can be left. The application name can be changed to something more descriptive but it must not contain any spaces. Click **Next**.
    f. **Step 2: Map modules to servers**
    Leave the default association to the server. Click **Next**.
    g. **Step 3: Map virtual hosts for Web modules**
    The default association to the default_host, virtual host can be changed. Click **Next**.
    h. Step 4
    Use `/trc` as the context root, otherwise further changes must be made in the `trc.properties` file. Click **Next**.
    i. Step 5
    A summary of the chosen deployment settings is displayed before the installation of the Remote Control application proceeds.
    Click **Finish**

A status page for the installation in progress and the outcome when the installation is finished is displayed.

j. Click **Save** to save to the master configuration.

The Remote Control application is displayed in the list of Enterprise Applications with the descriptive name that you entered in the Installation options step of the deployment process. Before you start the application, you can customize the `trc properties` file and change the default values. The properties files are deployed with the application and are in the `installedApps` directory within WebSphere. For more information about the properties in the files, see the *BigFix® Remote Control Administrator's Guide*.

Note: Ensure that the correct server IP address or server name is set in the **URL** field in the **trc.properties** file, so that the targets connect to the correct server. If you are using HTTPS, the host name or IP address that is set in the URL property must exactly match the value of the **CN** field of the SSL certificate that is installed on the server.

Installing from the BigFix console

You can create and run a server installation task to install the server by using the BigFix® console. For more information, see the *BigFix® Remote Control Console User's Guide* and the chapter about Managing target and server configuration.

Install the target

The Remote Control target can be installed on every computer that you want to control remotely. You can also use it to start a remote control session over the internet, by using a broker to make the connection.

Remote Control provides two ways to install the target component. If you have access to the BigFix® console, use the deployment fixlets to deploy the target. For more information, see the *BigFix® Remote Control Console User's Guide*. Alternatively use the Remote Control target installation files.

Installing the Windows™ target

The `trc_target_setup.exe` file is required to install the Remote Control target component on a Windows™ system.

For details of how to obtain the Windows™ component installation files see, Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

1. Run the `trc_target_setup.exe` file.
2. Click **Next** at the welcome screen.
3. Accept the license agreement. Click **Next**.
4. Accept the default location for the installation files, or click **Change** to select a different location.

5. Specify the host name of the Remote Control server that the target connects to.
   For example, `trcserver.example.com`.

   Note: Select **Use secure connections (https)** if you selected to use HTTPS during the server installation.

6. On the **Server Address** window, for secure target registration, enter or paste the **Registration** token. Ensure that **Use secure connections (https)** is also selected. For more information about secure target registration, see Add a token for secure target registration *(on page 100)*
7. For advanced settings, click **Advanced settings**

   Server port

   The port must match the value that is entered for the **Server port on Webserver** parameter during the server installation.

   Server Context

   The server context is used as part of the URL for contacting the server. It must match the value that is entered after the '/' in the **Path to URL** field, on the **Web server parameters** screen during the server installation.

   Use a FIPS certified cryptographic provider

   Select this option to enable FIPS compliance on the target. For more information about enabling FIPS compliance, see Enable FIPS compliance on the target *(on page 145)*.

   Enable NIST SP800-131A compliance (Enables FIPS)

   Select this option to enable NIST SP800-131A compliance on the target. For more information about enabling NIST SP800-131A compliance, see NIST SP800-131A compliance in Remote Control *(on page 148)*.

8. Click **Next**.
9. On the **Proxy settings** screen if you are not using a proxy server, click **Next**.
   - To use a Proxy, select **Use a proxy server or a Remote Control Gateway**.
     a. Type in the IP address or host name for the Proxy server.
     b. Type in the port that proxy server is listening on.
     c. Select whether you are using an HTTP proxy or a Remote Control Gateway.
     d. Select **Proxy requires authentication** if you must authenticate with the proxy server. Enter the ID and password for authenticating to the proxy server. The user ID and password are automatically encrypted when the target starts. For more information about the automatic passphrase encryption, see the *BigFix® Remote Control Administrator's Guide*.

Note: When you rerun the target installer and select **Modify** after the user ID and password are encrypted, the encrypted user ID and password combination is displayed in the user ID field. The password field remains empty.

e. Click **Next**.

10. Accept or change the port value to be used to listen for incoming remote control sessions. Click **Next**.

Note: Your operating system might have a firewall, an antivirus or an intrusion detection system that is installed by default. For more details, see Target requirements *(on page 24)*.

11. To enable failover to peer-to-peer mode, select one of the following options:

Regardless of server status

A peer to peer session can be established between a controller and this target directly if the server is available or not. Click **Peer to Peer** policies to set the local policies for the target to use during a peer to peer session. Click **Next** to move through the peer to peer policies screens.

Only when server is down or unreachable

A peer to peer session can be established only if the server is down or the target cannot connect to the server. Click **Peer to Peer** policies to set the local policies for the target to use during a peer to peer session. Click **Next** to move through the peer to peer policies screens.

Never

A peer to peer session is not allowed directly between a controller and this target. If you select this option, continue from step 12 *(on page 75)*.

Peer to Peer policies

Session policies options

Table 8. Session policies options.

Installation option.	Target Property.	Default Value.	Description
Active	AllowActive	Selected.	Determines whether the target can take part in active peer to peer sessions. For more information about the different types of remote control session that can be started, see the *BigFix® Remote Control Controller User's Guide*. **Selected.** The target can take part in active peer to peer sessions and the Active option is available in the session type list in the controller window. The

Installation option.	Target Property.	Default Value.	Description
			Open connection window also displays an Active option. **Not selected.** The target cannot take part in active peer to peer sessions and the Active option is not available in the session type list in the controller window.
Guidance	AllowGuidance	Selected.	Determines whether the target can take part in guidance peer to peer sessions. For more information about the different types of remote control session that can be started, see the *BigFix® Remote Control Controller User's Guide*. **Selected.** The target can take part in guidance peer to peer sessions and the Guidance option is available in the session type list in the controller window. The **Open connection** window also displays a Guidance option. **Not selected.** The target cannot take part in guidance peer to peer sessions and the Guidance option is not available n in the session type list in the controller window.
Monitor	AllowMonitor	Selected.	Determines whether the target can take part in monitor peer to peer sessions. For more information about the different types of remote control session that can be started, see the *BigFix® Remote Control Controller User's Guide*. **Selected.** The target can take part in monitor peer to peer sessions and the **Monitor** option is available in the session type list in the controller window. The **Open connection** window also displays a **Monitor** option. **Not selected.** The target cannot take part in monitor peer to peer sessions and the Monitor option is not available in the session type list in the controller window.

Installation option.	Target Property.	Default Value.	Description
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 quality	LockColorDepth	Not selected.	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**. **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 background	RemoveBackground	Not selected.	If the target has a desktop background image set, this property can be used to remove the background 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.**

Installation option.	Target Property.	Default Value.	Description
			The desktop background image on the target is visible during a remote control session.
Stop screen saver updates when screen saver is active	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. The controller displays a simulated screen saver, so that the controller user is aware that a screen saver is active on the remote display. The controller user can remove the screen saver by pressing a key or moving the mouse. **Not selected.** A simulated screen saver is not displayed in the session window. The target screen is displayed as normal and the target continues to transmit screen updates.

Policies options

Table 9. Peer to peer policy descriptions -

Installer screen names.	Target property.	Default value.	Description
Disable chat	DisableChat	Not selected.	Determines whether you can start a chat session with the target and also chat to the controller user during a peer to peer session. **Selected.** If **ChatOnly** 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 started from the open connection window. During the session, the chat icon is available in the controller window.

Installer screen names.	Target property.	Default value.	Description
Save chat messagess	AutoSaveChat	Not selected.	Determines whether the chat messages that are entered during a chat session are saved. **Selected.** The chat messages are saved in an html file, in the working directory of the target. The location is defined by the target property **WorkingDir**. The file name is prefixed with *chat-*. For example, on a Windows™ system, a file that is named `chat-m15.html` is saved to the following location. `c:\Documents and Settings\All Users \Application Data\BigFix\Remote Control` **Not selected.** The chat messages are not saved to a file.
Disable file transfer from target to controller	DisableFilePull	Not selected.	Determine whether files can be transferred 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 from controller to target	DisableFilePush	Not selected.	Determines whether files can be transferred 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	DisableClipboard	Not selected.	Determines the availability of the clipboard transfer menu. Use this menu option to transfer the clipboard content between the controller and target during a remote control session. **Selected.**

Installer screen names.	Target property.	Default value.	Description
			The clipboard transfer menu is available during the session and you can transfer the clipboard content to and from the target. **Not selected.** The clipboard transfer menu is not available during the session.
Allow local recording	AllowRecording	Selected.	Determines whether the controller user can make and save a local recording of the session in the controlling system. Determines the availability of the record option on the controller window. For more information about recording sessions, see the *BigFix® Remote Control Controller User's Guide*. **Selected.** The record option is available in the controller window. **Not selected.** The record option is not available in the controller window.
Allow collaboration	AllowCollaboration	Selected.	Determines whether more than one controller can join a session. Determines the availability of the collaboration icon on the controller window. For details of collaboration sessions, see the *BigFix® Remote Control Controller User's Guide*. **Selected.** The collaboration icon is available in the controller window. **Not selected.** The collaboration icon is not available in the controller window.
Allow session handover	AllowHandover	Selected.	Determines whether 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. For more information about collaboration sessions, see the *BigFix® Remote Control Controller User's Guide*. **Selected.**

Installer screen names.	Target property.	Default value.	Description
			The handover option is available in the collaboration control window. **Not selected.** The handover option is not available in the collaboration control window.
Allow requests to disconnect existing session	AllowForceDisconnect	Not selected.	Determines whether a controller user is given the option to disconnect a session with a target so that they can connect to the target instead. Used with the **Managed** and **CheckUserLogin** properties. For more information about disconnecting sessions, see the *BigFix® Remote Control Controller User's Guide*. **Selected.** A **Disconnect session** option is available in the message window that is displayed when you attempt to connect to the target. **Not selected.** A **Disconnect session** option is not available when you attempt to connect to the target. The **CheckUserLogin** property must be set to Yes and **Managed** set to No for **AllowForceDisconnect** to take effect.
Disconnect grace time	ForceDisconnectTimeout	45	Number of seconds in which the current controller user must respond to the prompt to disconnect the current session. If they do not respond on time, 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.
Audit to Application Event 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 log can be used for audit purposes. **Selected.** Entries are displayed in the application event log of the target corresponding to each action carried out during the session. **Not selected.** No entries are logged to the application event log.

Security policies

Table 10. Peer to peer policy descriptions - Security policies.

Installer screen names.	Target property.	Default Value.	Description.
Authenticate by using Windows logon	CheckUserLogin	Selected.	Determines whether a logon window is displayed when the controller user clicks a session type button on the **Open Connection** window. **Yes** The logon window is displayed and the controller user must log on with a valid Windows™ ID and password. If the credentials are invalid, the target refuses the session. **No** The user acceptance window does not appear and the peer to peer session is established.

Must be a member of these Windows groups	CheckUserGroup	See description.	Default value.
			Windows™ systems.
			`BUILTIN\Administrators`
			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 listed groups. Otherwise, the session is refused. Multiple groups must be separated with a semicolon. For example, `wheel;trcusers`.
			Note: By default, on a Windows™ system, only the administrator user is granted access. On a Linux™ system, by default no users are granted access. To resolve this issue, complete one of the following steps.
			a. If the users must also be granted administrator rights, add them as members of the Administrators group on a Windows™ system or the wheel group on a Linux™ system.

Installer screen names.	Target property.	Default Value.	Description.

			b. If the users must not have administrator rights, complete the following steps.
			i. Create a group or use an existing group. For example, the following command might be run as root:
			`groupadd trcusers`
			.
			ii. Add the users to this group. For example, the following command might 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.

Allow privacy	AllowPrivacy	Selected.	Determines whether a controller user can lock the local input and display 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.
Allow input lock	AllowInputLock	Selected.	This property works with **Allow privacy** and on its own. Select **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**

Installer screen names.	Target property.	Default Value.	Description.
			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 **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 when session starts	EnablePrivacy	Not selected.	Determines whether the local input and display are locked for all sessions. Therefore, the target user cannot interact with the target screen during a remote control session. **Selected.** The target screen is blanked out by the privacy bitmap when the session starts. The target user cannot interact with the screen during 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 starts and the target user can interact with the screen.
Enable input lock when session starts	EnableInputLock	Not selected.	This property works with **Enable privacy**. Use **Enable input lock** to determine whether the target user can view their screen or not during a remote control session when privacy mode is enabled. **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.**

Installer screen names.	Target property.	Default Value.	Description.
			The target screen is not visible to the target user and the privacy bitmap is displayed on the target during the session. The target users mouse and keyboard are also disabled. **Note: Enable privacy** must be selected to allow **Enable input lock** to take effect.
Enable on-screen session notification	EnableOSSN	Not selected.	Determines whether a semi-transparent layer is placed onto the target screen. The layer displays text that indicates that a remote control session is in progress. Can be used when privacy is a concern so that the user is clearly notified when somebody remotely views or controls their PC. **Selected.** The semi-transparent layer is displayed on the target screen. The text indicates which type of remote control session is in progress. `For example : Remote Control - Active Mode.` The layer does not intercept keyboard or mouse actions. Therefore, the user is still able to interact with their screen. **Not selected.** A semi-transparent layer is not displayed on the target screen. **Note:** This policy is only supported on targets where a Windows™ operating system is installed.
Disable Panic Key	DisablePanicKey	Not selected.	Determines whether the target user can use the Pause Break key 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.**

Installer screen names.	Target property.	Default Value.	Description.
			The target user can use the Pause Break key to automatically end the remote control session.
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.

User acceptance policies

Table 11. Peer to peer policy descriptions - User acceptance policies.

Installer screen names.	Target property.	Default Value.	Description.
Take over session	ConfirmTakeOver	Selected.	Determines whether the user acceptance window is displayed when a remote control session is requested. **Selected.** The user acceptance window is displayed to the target user who can accept or refuse the session. **Not selected.** The user acceptance window is not displayed and the session is established.
Change session mode	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. The target user must accept or refuse the request.

Installer screen names.	Target property.	Default Value.	Description.
			Not selected. The user acceptance window is not displayed and the session mode is changed automatically.
File transfers	ConfirmFileTransfer	Selected.	Determines whether the user acceptance window is displayed when the controller user transfers files between the target and the controller. **Selected.** The acceptance window is displayed when the following options are selected. 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. **Note:** After they accept the request, the target user must select the filethat is to be transferred. ◦ 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.
System information	ConfirmSysInfo	Selected.	Determines whether the user acceptance window is displayed when the controller user requests to view the target system information. **Selected.** The user acceptance window is displayed when the controller user clicks the system information icon in the controller window. The target user must accept or refuse the request to view the target system information.

Installer screen names.	Target property.	Default Value.	Description.
			Not selected. The target system information is displayed automatically when the controller user clicks the system information icon.
Local recording	ConfirmRecording	Selected.	Determines whether the user acceptance window is displayed when the controller user clicks the record icon on the controller window. **Selected.** A user acceptance window is displayed when the controller user clicks the record icon on the controller window. If the target user clicks **Accept**, the controller user can select where to save the recording to. If the target user clicks **Refuse**, a refusal message is displayed to the controller. **Note:** After the target user accepts the request for recording, the acceptance window is not displayed again if the controller user stops and then restarts local recording in the same session. Also, the refusal message is displayed in English and is not translated. **Not selected.** When the controller user clicks the record icon on the controller window, the user acceptance window is not displayed. The controller user can then select where to save the recording to.
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.** The user acceptance window is displayed when the controller user tries to join the col-

Installer screen names.	Target property.	Default Value.	Description.
			laboration session. The target user must accept or refuse the request. If the target user clicks **Accept**, the additional controller joins the collaboration session. If they click **Refuse**, a message is displayed on the controller and the additional controller cannot join the collaboration session. **Not selected.** The additional controller automatically joins the collaboration session.
User acceptance grace time	AcceptanceGrace-Time	45	Sets the number of seconds to wait for the target user to respond before a session starts or times out. Used with **Take over session**. ◦ Acceptable values 0 - 60 - If set to 0 the activity starts without displaying the message box for user acceptance on the target. **Note:** If **Take over session** is selected, **User acceptance grace time** must be set to a value >0 to allow the target user time to respond.
Proceed on acceptance timeout	AcceptanceProceed	Not selected.	Continue with the session if the user acceptance timeout lapses. The target user does not click accept or refuse within the number of seconds defined for **Acceptance grace time**. **Selected.** The session starts. **Not selected.** The session does not start.
Do not prompt for user acceptance when user is not logged on.	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. **Not selected.** Session is not started and the following message is displayed. `Session rejected because`

Installer screen names.	Target property.	Default Value.	Description.
			there is no user logged to confirm the session
Enable 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 10. 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 displayed on the user acceptance window.

Session scripts

Table 12. Peer to peer policy descriptions - Session scripts policies.

Installer screen names.	Target property.	Default Value.	Description.
Run pre-session script	RunPreScript	Not selected.	Determines whether a user-defined script must be run before the remote control session starts. It is run just after the session is authorized 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 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 details of setting up pre-session scripts and post session scripts, see the Session policies chapter in the *BigFix® Remote Control Administrator's Guide*.

Installer screen names.	Target property.	Default Value.	Description.
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 details of setting up pre and post session scripts, see the Session policies chapter in the *BigFix® Remote Control Administrator's Guide*.
Proceed with session when script fails	ProceedOnScriptFail	Not selected.	Continue with the session 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 not found error, or a script that does not finish 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 ends immediately.

For the definition and more information about the properties, see Properties that can be set in the target configuration *(on page 178)*.

Session policies options

Table 13. Session policies options.

Installation option.	Target Property.	Default Value.
Active	AllowActive	Selected.
Guidance	AllowGuidance	Selected.
Monitor	AllowMonitor	Selected.
Enable high quality colors	EnableTrueColor	Not selected.
Lock color quality	LockColorDepth	Not selected.

Installation option.	Target Property.	Default Value.
Remove desktop background	RemoveBackground	Not selected.
Stop screen saver updates when screen saver is active	NoScreenSaver	Not selected.

Policies options

Table 14. Policy descriptions -

Installer screen names.	Target property.	Default value.
Disable chat	DisableChat	Not selected.
Save chat messages	AutoSaveChat	Not selected.
Disable file transfer from target to controller	DisableFilePull	Not selected.
Disable file transfer from controller to target	DisableFilePush	Not selected.
Disable clipboard transfer	DisableClipboard	Not selected.
Allow local recording	AllowRecording	Selected.
Allow collaboration	AllowCollaboration	Selected.
Allow session handover	AllowHandover	Selected.
Allow requests to disconnect existing session	AllowForceDisconnect	Not selected.
Disconnect grace time	ForceDisconnectTimeout	45
Audit to Application Event Log	AuditToSystem	Selected.

Security policies

Table 15. Security policies.

Installer screen names.	Target property.	Default Value.
Authenticate by using Windows logon	CheckUserLogin	Selected.
Must be a member of these Windows groups	CheckUserGroup	See description.
Allow privacy	AllowPrivacy	Selected.
Allow input lock	AllowInputLock	Selected.
Enable privacy when session starts	EnablePrivacy	Not selected.
Enable input lock when session starts	EnableInputLock	Not selected.

Installer screen names.	Target property.	Default Value.
Enable on-screen session notification	EnableOSSN	Not selected.
Disable Panic Key	DisablePanicKey	Not selected.
Inactivity timeout	IdleTimeout	360

User acceptance policies

Table 16. User acceptance policies.

Installer screen names.	Target property.	Default Value.
Take over session	ConfirmTakeOver	Selected.
Change session mode	ConfirmModeChange	Selected.
File transfers	ConfirmFileTransfer	Selected.
System information	ConfirmSysInfo	Selected.
Local recording	ConfirmRecording	Selected.
Collaboration	ConfirmCollaboration	Selected.
User acceptance grace time	AcceptanceGraceTime	45
Proceed on acceptance timeout	AcceptanceProceed	Not selected.
Do not prompt for user acceptance when user is not logged on.	AutoWinLogon	Selected.
Enable Hide windows	HideWindows	Not selected.

Session scripts

Table 17. Session scripts policies.

Installer screen names.	Target property.	Default Value.
Run pre-session script	RunPreScript	Not selected.
Run post-session script	RunPostScript	Not selected.
Proceed with session when script fails	ProceedOnScriptFail	Not selected.

Additional Features

Select **Install device driver for Virtual Smart Card Reader** to install the virtual smart card reader driver. For more information about the smart card reader driver, see Install a driver to support smart card authentication in the target *(on page 104)*.

12. Click **Install** to begin the installation.
13. When the installation is complete, click **Finish**.

Installing the Linux™ target

You can install the target component on a Linux™ computer by using the RPM file that is provided in the Remote Control installation files.

Note: The target component installation package depends on the following libraries: **glibc**, **libgcc**, **libblkid**, **libstdc++** etc.

Use the `trc-target-10.x.x.<arch>.rpm` file to install the target component in Linux™, where 10.x.x is the version that you want to install. For more information about how to obtain the Linux™ component installation files, see Obtain the installation files *(on page 29)*. Choose the appropriate method for obtaining the file.

Install a default target RPM file and then configure the target after the installation.

To install the `trc-<component>-10.x.x.<arch>.rpm` package of the component, run the dnf, yum, or zypper command by providing the install -y option and the RPM package file path. Otherwise if you want to manually resolve the dependencies, run the rpm -ivh trc-target-10.x.x.<arch>.rpm command. You can also get the complete dependency list by running the rpm -qpR trc-target-10.x.x.<arch>.rpm command.

When the target is installed, configure the target properties by editing the `/etc/trc_target.properties` file. For more information about target properties and their definitions, see Properties that can be set in the target configuration *(on page 178)*.

Install the BigFix® Remote Control Target for macOS

You can install the BigFix® Remote Control Target for macOS in numerous ways. Use the `trc_target.pkg` file to install the application in attended or unattended mode. You can also install the target by using a Fixlet® in the BigFix® console.

For information about how to obtain the BigFix® Remote Control Target for macOS component installation files, see Install the BigFix® Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

Installing the BigFix® Remote Control Target for macOS from the BigFix® console

You can use a Fixlet® in the BigFix® console to install the BigFix® Remote Control Target for macOS component. The deployment Fixlet® is available in the Remote Control site in the Systems Lifecycle domain.

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

To install the BigFix® Remote Control Target for macOS target component, 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 Target for macOS**.
5. In the **Task** pane, review the description and follow the instructions in the **Actions** box to start the task.
6. In the **Take Action** pane on the **Target** tab, select the relevant option for determining the computers on which to deploy the BigFix® Remote Control Target for macOS component.
7. Click **OK**.
   The summary screen shows the progress of the task and the status is set to **Complete** when it is finished.

Installing the BigFix® Remote Control Target for macOS by using the .pkg file

You can use the `trc_target.pkg` file to install the BigFix® Remote Control Target for macOS.

You can obtain the `pkg` file from Passport Advantage or from the Remote Control server UI. For more information, see Obtain the installation files *(on page 29)*. Two installation methods can be used when you have the `pkg` file: attended and unattended.

You can also apply custom configuration settings when you install the target. The configuration values are set in the `trc_target.cfg` file. Create the file and add your custom values. Copy the file to the computers on which you want to install the BigFix® Remote Control Target for macOS. Copy the `trc_target.cfg` file to the same directory as the `trc_target.pkg` file.

Your configuration settings are installed together with the target. The target configuration is installed to `/Library/Preferences/com.bigfix.remotecontrol.target.plist`.

To configure the target to support broker sessions, you must configure the **BrokerList** property and provide trusted certificates. Place a `broker.certs` file, that contains the trusted certificates in the same directory as the `trc_target.pkg` file. The package installs the `broker.certs` file to

`/Library/Application Support/com.bigfix.remotecontrol.target/TrustStore`.

For more information about the target properties that can be set in the `.cfg` file, see Properties that can be set in the target configuration *(on page 178)*.

If you do not apply any custom configuration, the target uses built in configuration settings when it installs.

Choose an installation method for installing the BigFix® Remote Control Target for macOS.

Attended Mode:

1. Double-click the `trc_target.pkg` file.
2. Click **Continue**.
3. Click **Install** to install to the startup disk. If your system has multiple disks, you can select the disk on which to install the target. Click **Change Install Location** to select an installation disk.
4. If you are a user with admin authority, type in your password when prompted. Otherwise, type a valid admin ID and password. Click **Install Software**.
5. When the installation completes, click **Close**.

Unattended mode:

1. Open a **Terminal** window and type the following command.

   sudo installer -pkg "/[path]/trc_target.pkg" -target /

   Where *[path]* is the path to the `.pkg` file.

After you install the .pkg file, open the `Remote Control Target.app` to start the target.

Run a target custom installation

Run an Remote Control target custom installation to install the target software by using parameters. You can run the installation in multiple ways.

Unattended and silent

No interaction is required by the user and no UI dialogs or progress bars are displayed to the user.

Unattended

No interaction is required by the user and an installation progress bar is displayed to the user.

Attended

The full installation UI is displayed and requires user interaction.

You can customize installation settings and also assign the target to a specific group during the installation.

Running a target custom installation on a Windows® system

To install the target software on a Windows® operating system, use the `trc_target_setup.exe` file.

For more information about obtaining this file, see Obtain the installation files *(on page 29)*.

To install the target, complete the following steps:

1. Create a folder in your root drive called `TRC`.
2. Copy `trc_target_setup.exe` to TRC.
3. Open a command prompt window and go to TRC.
4. Type `DIR` to verify that the exe file is in this folder.
5. To install the target, type the following command in one line.

   ```
   trc_target_setup.exe /s /v"/qn [INSTALLPARAMETER1][INSTALLPARAMETER2]...[INSTALLPARAMETERX]"
   ```

   Use the following installation parameters customize your installation.

   Note: Ensure that the correct values are assigned to the parameters as no validation of the values is carried out.

   /s

   Denotes a silent installation.

/v"

The string that is attached to **/v** contains the parameters for `msiexec.exe`, which is a piece of software that runs the installation.

/qn

Run a silent and unattended installation with no progress window and no UI.

You can also replace */qn* with the following parameters.

/qb

For an unattended installation with a basic UI and a small progress bar.

/qr

For an unattended installation with a reduced UI progress bar in a large window.

/qf

For an attended installation with full UI.

TRC_SERVER_HOSTNAME

The host name or IP address of the server. This property is required. Default value is *<blank>*.

For example, `TRC_SERVER_HOSTNAME=trc.myserver.com`.

TRC_SERVER_CONTEXT

This parameter value must match the last part of the path in the server URL. Default value is *trc*.

For example, `TRC_SERVER_CONTEXT=trc`.

TRC_SERVER_PORT

If the server runs on a non-standard port, specify the port number. Default value is 80.

For example, `TRC_SERVER_PORT=8080`.

TRC_SERVER_PROTOCOL

Choose between plain HTTP and secure HTTPS protocols. Valid values are http and https. Default value is http.

For example, `TRC_SERVER_PROTOCOL=http`.

TRC_PROXY_HOSTNAME

Host name or IP address for the proxy server, if you are using one. Default value is *<blank>*.

For example, `TRC_PROXY_HOSTNAME=proxy.company.com`.

TRC_PROXY_PORT

Port number for the proxy server. Default value is *<blank>*.

For example, `TRC_PROXY_PORT=8080`.

TRC_PROXY_USER_ID

The user ID, if the proxy requires authentication. Default value is *<blank>*. The user ID and password are automatically encrypted when the target starts, unless **DISABLEAUTOMATICPASSPHRASEENCRYPTION** is set to *Yes*. For more information about automatic passphrase encryption, see the *BigFix® Remote Control Administrator's Guide*.

For example, `TRC_PROXY_USER_ID=proxyuser`.

TRC_PROXY_PASSWORD

The password, if the proxy requires authentication. Default value is *<blank>*. The user ID and password are automatically encrypted when the target starts, unless **DISABLEAUTOMATICPASSPHRASEENCRYPTION** is set to *Yes*. For more information about automatic passphrase encryption, see the *BigFix® Remote Control Administrator's Guide*.

`TRC_PROXY_PASSWORD=v264xmpt`.

TRC_PROXY_AUTH_B64

The user ID and password, format `user: password`, encoded in base64. Overrides the user ID and password properties. If you do not want the password to be easily visible, use this parameter. Base64 is not encryption. Default value is *<blank>*.

For example, `TRC_PROXY_AUTH_B64=cHJveHl1c2VyOnYyNjR4bXB0`

The user ID and password are automatically encrypted when the target starts, unless **DISABLEAUTOMATICPASSPHRASEENCRYPTION** is set to *Yes*. For more information about automatic passphrase encryption, see the *BigFix® Remote Control Administrator's Guide*.

TRC_TARGET_PORT

To run the target on a non-standard port, specify the port number to use. Default value is 888.

For example, `TRC_TARGET_PORT=888`.

TRC_SERVER_HEARTBEAT_RETRY

The amount of time, in minutes, that the target waits before it resends a heartbeat to the server, when the server is not responding. Default value is 10.

For example, `TRC_SERVER_HEARTBEAT_RETRY=1`.

TRC_ACCESSIBILITY

Enables the accessible UI. Default value is *No*. Available on Windows® operating system.

GROUP_LABEL

The name of the group that the target is to be assigned to. To enable this feature, edit the `trc.properties` file and set *allow.target.group.override = true*. For more information about editing the properties files, see the *BigFix® Remote Control Administrator's Guide*. Default value is *DefaultTargetGroup*.

Note:

a. The GROUP_LABEL parameter is discarded if the target is already registered in the Remote Control server.
b. The target group that is specified must already be defined on the server.

For example, `GROUP_LABEL=NewTargetGroup`.

INSTALLDIR

Use this parameter to specify the directory for installing the target software to.

For example, `INSTALLDIR= c:\trc\target`.

ALLOWP2P

Use this parameter to enable peer to peer connections regardless of the server status. Default value is *No*.

ALLOWP2PFAILOVER

Use this parameter to enable failover to peer-to-peer mode when the server is down or unreachable. Default value is *No*.

AUDITTOSYSTEM

Use this parameter to log peer to peer session events in the targets application event log for auditing purposes. Default value is *No*.

AUTOSAVECHAT

Use this parameter to save the contents of the chat window to a file on the target. Default value is *No*.

AUTOWINLOGON

Determines whether a session can be started when no users are logged on at the target. Default value is *Yes*.

CHECKUSERGROUP

The controller user must be a member of the listed groups. Default value is `BUILTIN\Administrators` on Windows® systems and `wheel` on Linux® systems.

CHECKUSERLOGIN

Determines whether the login window is displayed when the controller user selects a session type in the **Open Connection** window. Default value is *Yes*.

CONFIRMFILETRANSFER

Determines whether the user acceptance window is displayed before the controller user transfer files from the target to the controller in a peer to peer session. Default value is *Yes*.

CONFIRMMODECHANGE

Determines whether the user acceptance window is displayed when the controller user selects a different session mode during the remote control session. Default value is *Yes*.

CONFIRMSYSINFO

Determines whether the user acceptance window is displayed when the controller user requests to view the target system information. Default value is *Yes*.

CONFIRMTAKEOVER

Determines whether the user acceptance window is displayed when a peer to peer session is requested. Default value is *Yes*.

DISABLEAUTOMATICPASSPHRASEENCRYPTION

Determines whether the proxy authentication user ID and password are automatically encrypted when the target starts. Default value is *No*. For more information about automatic passphrase encryption, see the *BigFix® Remote Control Administrator's Guide*.

DISABLECHAT

Determines whether you can start a chat session with the target and also chat to the controller user during a peer to peer session. Default value is *No*.

DISABLECLIPBOARD

Determines the availability of the clipboard transfer menu during a peer to peer session. Default value is *No*.

DISABLEFILEPULL

Determines whether you can transfer files from the target to the controller during a peer to peer session.

DISABLEFILEPUSH

Determines whether you can transfer files from the controller to the target during a peer to peer session. Default value is *No*.

FIPSCOMPLIANCE

Enable the use of a FIPS certified cryptographic provider for all cryptographic functions. Default value is *No*.

SP800131ACOMPLIANCE

Enable the use of NIST SP800-131A compliant algorithms and key strengths for all cryptographic functions. Default value is *No*.

HTTPSSTRICTVALIDATION

Determines whether the target uses the system truststore to verify HTTPS connections to the server. Default value is *No*.

LOGLEVEL

Set the logging level. The logging level determines the types of entries and how much information is added to the target log file. Possible values 0, 1, 2, or 4. However, use **LOGLEVEL=4** only by request from IBM software support. Default value is 2.

For example, `LOGLEVEL=2`.

LOGROTATION

Controls the period after which an older log file is overwritten. Set to **Daily**, **Weekly**, or **Monthly**. Default value is Weekly.

For example, `LOGROTATION=Monthly`.

You can also disable log rotation by using the value **Disabled**.

LOGROLLOVER

Controls the period after which a new log file is started. Therefore, this period must be shorter than the LOGROTATION period, not all combinations are valid. LOGROLLOVER cannot be disabled. Set to **Daily** or **Hourly**. Default value is Daily.

For example, `LOGROLLOVER=Daily`.

VSC

Use the parameter to install the device driver for the virtual smart card reader. Add **VSC=1** to the parameter list to install the driver.

Note: The appearance of **VSC** in the parameter list determines whether the driver is installed, not the value of the parameter. If **VSC**= n is in the parameter list, the driver is installed. If **VSC** is not in the parameter list, the driver is not installed. **VSC** can have any value. However, **VSC=1** is the suggested value.

For more information about installing the device driver for the virtual smart card reader during a silent installation, see Installing the virtual smart card reader driver by running a silent installation *(on page 105)*.

REGISTRATIONTOKEN

Use this parameter to provide the registration token to the target. The token is used to authenticate the target to the server when it first contacts the server. The value of the property is set to the registration token. For more information about installing the target with a secure registration token by running a silent installation, see Running a target silent installation with a secure registration token *(on page 101)*.

Note: To reconfigure the parameters on an existing target installation, use the parameter, **REINSTALL=ALL**. However, the parameter is ignored if it is used when you upgrade the target.

For example, on the command line you can type the following command:

trc_target_setup.exe /s /v"/qn REINSTALL=ALL"

To modify the target configuration and apply an upgrade, complete the following steps.

1. Perform a silent installation with the new version of target software. Do not use any parameters. If you do use parameters, the target is upgraded but the parameters are ignored and are not updated.
2. Perform a silent re installation with `REINSTALL=ALL` and any new parameters.

You can also specify the parameters that you want to override.

For example, to change the target port to 2222, type the following command.

trc_target_setup.exe /s /v"/qn TRC_TARGET_PORT=2222 REINSTALL=ALL"

Note: To view Help options during the installation, type the following command on the command line.
trc_target_setup.exe --help

Install the controller

The Remote Control controller can be installed locally on your system, to be used for connecting to a target directly if peer to peer mode is enabled.

Remote Control provides two ways to install the controller component. If you have access to the BigFix® console, use the deployment Fixlet® to deploy the controller. For more information, see the *BigFix® Remote Control Console User's Guide*. Alternatively use the Remote Control controller installation files.

Installing the controller on a Windows™ system

The `trc_controller_setup.exe` file is required to install the controller component on a Windows™ system.

For more information about how to obtain the component installation files for a Windows™ system, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

1. Run the `trc_controller_setup.exe` file.
2. On the file download window, select **Run** or **Save**

   Run

   Select **Run** to start the installation wizard.
   a. Click **Next** at welcome screen.
   b. Accept the license agreement, click **Next**.
   c. Accept or change the location for the installation files, click **Next**.

d. Click **Install**.
e. Click **Finish**.

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

Save

Select **Save** to save the `trc_controller_setup.exe` file to a selected location. Run the file to install the controller.

The controller is installed to the default location `\Program Files\BigFix\Remote Control\Controller` or the location that is selected during the installation.

Installing the Linux™ controller

Use the `trc-controller-10.x.x.noarch.rpm` and `trc-controller-jre-10.x.x.<arch>.rpm` files to install the controller component in Linux™. Where *10.x.x* is relevant to the version that you want to install. For more information about how to obtain the Linux™ component installation files, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

You can install the controller in two modes in Linux™, a FIPS-compliant controller or a standard controller.

Type the relevant command for installing the controller. Where *10.x.x* is relevant to the version that you want to install. .

- For the standard controller type

  #<install_command> trc-controller-10.x.x.noarch.rpm

- For a FIPS-compliant controller, install the standard controller and the FIPS-compliant JRE by running both commands.

  #<install_command> trc-controller-10.x.x.noarch.rpm

  #<install_command> trc-controller-jre-10.x.x.<arch>.rpm

To install the `trc-<component>-10.x.x.<arch>.rpm` package of the component, run the dnf, yum, or zypper command by providing the install -y option and the RPM package file path. Otherwise. if you want to manually resolve the dependencies, use the `rpm -ivh <package>.rpm` command. You can also get the complete dependency list by running the `rpm -qpR <package>.rpm` command.

Note: Standard controller installations work with the `trc-controller-10.x.x.noarch.rpm` file, with an alternative JRE installed on the system. If the controller is to be FIPS-compliant or if you don't have a

compatible JRE installed on the system, the `trc-controller-jre-10.x.x.<arch>.rpm` file must also be installed.

You can start the controller from your applications list when it is installed.

Install the BigFix® Remote Control Controller for macOS

The BigFix® Remote Control Controller for macOS can be installed in multiple ways. You can use the `trc_controller.pkg` file to install the application. You can also install the controller by using a Fixlet® in the BigFix® console.

For information about how to obtain the BigFix® Remote Control Controller for macOS component installation files see, Obtain the installation files *(on page 29)*. Choose the appropriate method for obtaining the file.

Installing the BigFix® Remote Control Controller for macOS from the BigFix® console

You can use a Fixlet® in the BigFix® console to install the BigFix® Remote Control Controller for macOS component. The deployment Fixlet® is available in the Remote Control site in the Systems Lifecycle domain.

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.
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.

Installing the BigFix® Remote Control Controller for macOS

You can use the `trc_controller.pkg` file to install the BigFix® Remote Control Controller for macOS.

You can obtain the `pkg` file from Passport Advantage or from the Remote Control server UI. For more information, see Obtain the installation files *(on page 29)*. To install the controller, complete the following steps.

1. Double-click the `trc_controller.pkg` file.
2. Click **Continue**.
3. Click **Install** to install to the startup disk. If your system has multiple disks, you can select which disk to install the controller on. Click **Change Install Location** to select an installation disk.
4. If you are a user with admin authority, type in your password when prompted. Otherwise, type a valid admin ID and password. Click **Install Software**.
5. When the installation completes, click **Close**.

After you install the .pkg file, open the `Remote Control Controller.app` to start the target.

Installing the controller in other supported operating systems

If you are using a supported operating system other than Windows™ operating system, like Linux™, extract the controller files by using the additional setup utility. Then, copy the required files to the system that you are running the controller on. You must run the additional setup utility on a Windows™ or Linux™ system. For more information about obtaining the additional setup utility files, see Install the Remote Control components *(on page 29)*.

Note: Ensure that you install a supported version of Java™ to run the controller on the other supported operating system. See Controller requirements *(on page 23)*.

To install the controller, complete the following steps:

1. After you extract the installation files, go to the `RCController` directory.
2. Copy the file `trc_console.zip` to the system that you are running the controller on.
3. Extract the files from the `trc_console.zip` file.
4. Type the following command to run the controller

   java -jar TRCConsole.jar

Installing a preconfigured controller component

You can apply custom configuration settings when you install the controller component.

Preconfiguring the controller is useful for unattended installations. You can set your configuration file values in the configuration file and copy the file to the computers that you want to install the controller on. Your configuration settings are installed together with the controller. The configuration values are set in the `trc_controller.cfg` file. You can create the file and add your custom values or you can edit a default configuration file. If you do not apply any preconfiguration, the default configuration file is installed when you install the controller component.

The property values in the `trc_controller.cfg` are global and are the same for all users who run the controller. However, a user can create a local configuration. The values in the users' local configuration are used when they run the controller and override the global values. To enforce the global property value, you can set a property to mandatory so that a user cannot edit the property in the **Configuration Window** in the controller UI. The mandatory global property overrides the local property.

To set a mandatory property, complete the following steps:

1. Open the `trc_controller.cfg` file.
2. Copy the property name and add *.mandatory = true* to the end.

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

enable.address.history=false
enable.address.history.mandatory=true

3. Save the file.

After you save the `trc_controller.cfg` file, install the controller.

Preconfigure the controller for a Windows™ operating system installation

1. Copy the `trc_controller.cfg` file to the same directory as the `trc_controller_setup.exe` or `trc_controller.msi file`.
2. Run the controller installation file.

The controller is installed with your configured settings.

Note: Preconfiguring the controller is not supported for installation on a Linux™ operating system. If necessary, you can modify and rebuild the controller `.rpm` file from the source `.rpm` file.

Use the content of the default configuration file to create your custom configuration file and set your own values.

fips.compliance=false

sp800131a.compliance=false

enable.address.history=true

enable.user.history=false

enable.domain.history=true

history.max.items=20

tool01.ToolName = Control Panel
tool01.ToolCommand = [SystemFolder]\\control.exe
tool01.ToolParameters =
tool01.ToolUser =

tool02.ToolName = Command Prompt
tool02.ToolCommand = [SystemFolder]\\cmd.exe
tool02.ToolParameters =
tool02.ToolUser =

```
tool03.ToolName = Administrator Command Prompt
tool03.ToolCommand = [SystemFolder]\\cmd.exe
tool03.ToolParameters =
tool03.ToolUser = admin

tool04.ToolName = Task Manager
tool04.ToolCommand = [SystemFolder]\\taskmgr.exe
tool04.ToolParameters =
tool04.ToolUser =

tool05.ToolName = Windows™ Explorer
tool05.ToolCommand = [WindowsFolder]\\explorer.exe
tool05.ToolParameters =
tool05.ToolUser =

tool06.ToolName=Terminal
tool06.ToolCommand=/usr/bin/gnome-terminal
tool06.ToolParameters =
tool06.ToolUser =

tool07.ToolName=Control Panel
tool07.ToolCommand=/usr/bin/gnome-control-center
tool07.ToolParameters =
tool07.ToolUser =

tool08.ToolName=
tool08.ToolCommand=
tool08.ToolParameters =
tool08.ToolUser =

tool09.ToolName=
tool09.ToolCommand=
tool09.ToolParameters =
tool09.ToolUser =

tool10.ToolName=
tool10.ToolCommand=
tool10.ToolParameters =
tool10.ToolUser =

# Custom keys
```

```
# example.KeySequenceName = Inject F1
# example.KeySequenceValue = [F1]
#
# For a list of supported key codes, please refer to the User's Guide

key01.KeySequenceName =
key01.KeySequenceValue =

key02.KeySequenceName =
key02.KeySequenceValue =

key03.KeySequenceName =
key03.KeySequenceValue =
```

Install the command-line tools

You can use the command-line tools to start a remote control session from the command-line, or run commands on a target system without target user interaction. The commands can be useful if you want to connect to a target without using the BigFix® Remote Control Server interface or for using as part of a script to run multiple commands in an automated fashion. The command-line tools are only available to run on Windows™ operating systems and Linux™ operating systems.

Remote Control provides two ways to install the command-line tools. If you have access to the BigFix® console, use the deployment fixlets to deploy the tools. For more information about deploying the components, see the *BigFix® Remote Control Controller User's Guide*. Alternatively use the Remote Control controller installation files.

Installing the cli tools on a Windows™ system

The `trc_cli_setup.exe` file is required to install the controller component on a Windows™ system.

For more information about how to obtain the Windows™ component installation files, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

1. Run the `trc_cli_setup.exe` file.
2. On the file download window, select **Run** or **Save**

   Run

   Select **Run** to start the installation.

   a. Click **Next** at the welcome screen.
   b. Accept the license agreement, click **Next**.
   c. Accept or change the location for the installation files, click **Next**.
   d. On the server address screen type in the information and click **Next**:

      Server host name

Enter the IP address or server name of the Remote Control server.

Use secure connections (https)

Select https to use secure connections to contact the server.

Advanced settings

Click **Advanced settings** for more configuration settings.

Server port

Enter the port number that the server is listening on.

Server context

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

Use a FIPS certified cryptographic provider

Select **Use a FIPS certified cryptographic provider** for installing FIPS-compliant tools.

Enable NIST SP800-131A compliance (Enables FIPS)

Select **Enable NIST SP800-131A compliance (Enables FIPS)** for installing NIST SP800-131A compliant tools.

e. On the **Proxy settings** panel, if you are not using a proxy server click **Next**.

- If you are using a Proxy, select **Use a proxy server or a Remote Control Gateway**. Type in the relevant information
  i. Type in the IP address or host name for the proxy server.
  ii. Type in the port that proxy server is listening on.
  iii. Select **Use an HTTP proxy** or **Use a Remote Control Gateway**.
  iv. Select **Proxy requires authentication** and enter the user ID and password for authenticating to the proxy server.The user ID and password are automatically encrypted when the target starts. For more information about the automatic passphrase encryption, see the *BigFix® Remote Control Administrator's Guide*.

Note: The CLI is unable to automatically encrypt the proxy credentials when the CLI is installed stand-alone, without the target and when the CLI is run by a standard user. If you use the CLI that is included in the target package, the proxy credentials are automatically encrypted by the target. You must restart the target after you edit the settings in the registry or configuration file. When you use the stand-alone CLI tools, you must run the

CLI once from an **Administrator Command Prompt** in a Windows operating system or when logged in as root in Linux.

v. Click **Next**.

f. Accept the default port or type in a value, click **Next**

g. Click **Install**.

h. Click **Finish**.

Save

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

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

The following executable files are in the selected directory.

`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 and see the output from the command on the computer that you issue the command from.

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

Installing the CLI tools in Linux™

You can install the CLI tools on a Linux™ computer by using the RPM file that is provided in the Remote Control installation files.

Note: The CLI component installation package depends on the following libraries: **glibc**, **libgcc**, **libblkid**, **libstdc++** etc.

Use the `trc-cli-10.x.x.<arch>.rpm` file to install the CLI tools in Linux™. Where *10.x.x* is relevant to the version that you want to install. For more information about obtaining the Linux™ component installation files, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

Note: If the `trc-target` RPM file is installed, you do not need to install the `trc-cli` RPM file because the CLI commands are already included in the target. For more information about using the commands, see the *BigFix® Remote Control Controller User's Guide*.

1. Type, the following command to install the command line software.
   Where *10.x.x* is relevant to the version that you want to install.

To install the `trc-<component>-10.x.x.<arch>.rpm` package of the component, run the dnf, yum, or zypper command by providing the install -y option and the RPM package file path. Otherwise, if you want to manually resolve the dependencies, then use the rpm -ivh trc-cli-10.x.x.<arch>.rpm command. You can also get the complete dependency list by running the rpm -qpR trc-cli-10.x.x.<arch>.rpm command.

2. When the installation is complete, edit the `/etc/trc_target.properties` file and set your configuration.
    - Set the value of **ServerURL** to the host name or IP address of your BigFix® Remote Control Server.
    - For FIPS-compliance set the value of **FIPSCompliance** to Yes.
    - For NIST SP800-131a compliance, set the value of *SP800131ACompliance* to yes.
3. Save the file.

For more information about using these commands, see the *BigFix® Remote Control Controller User's Guide*.

Install gateway support in Remote Control

For targets, controllers, and server on different networks that cannot directly contact each other you can install and configure gateway support.

Remote Control provides two ways to install the gateway support. If you have access to the BigFix® console, use the deployment fixlets to deploy gateway support. For more information, see the BigFix® Remote Control Console User's Guide. Alternatively you can use the Remote Control gateway support installation files.

Installing Windows gateway support

The `trc_gateway_setup.exe` file is required to install gateway support in a Windows operating system. For more information about how to obtain the Windows gateway support files, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

Note: You can also install gateway support with no user interaction by running a silent installation. For more information about a silent installation, see Installing the gateway support by running a silent installation *(on page 94)*.

To install gateway support, complete the following steps:

1. Run the `trc_gateway_setup.exe` file.
2. Click **Next** at the Welcome screen.
3. Accept or change the installation location and click **Next**.
4. Click **Install**.
5. Click **Finish** when the installation is complete.

When the gateway support is installed, you must configure it for your environment. For more information about configuring gateway support, see the *BigFix® Remote Control Administrator's Guide*.

Installing the gateway support by running a silent installation

To install the gateway support on a Windows® system by running a silent installation, complete the following steps:

1. Create a folder in your root drive called `TRC`.
2. Copy `trc_gateway_setup.exe` file to `TRC`.
3. Open a command prompt window and go to `TRC`.
4. Type in the following command all in one line:

   ```
   trc_gateway_setup.exe /s /v"/qn"
   ```

   /s

   Denotes a silent installation.

   /v"

   The string that is attached to /v contains the parameters for `msiexec.exe`, which is a piece of software that runs the actual installation.

   /qn

   Perform a silent installation with no progress window.

For more information about configuring gateway support, see the *BigFix® Remote Control Administrator's Guide*.

Installing Linux™ gateway support

You can install gateway support on a Linux™ computer by using the RPM file that is provided in the Remote Control installation files.

Note: The gateway component installation package depends on the following libraries: **glibc**, **libgcc**, **libblkid**, **libstdc++**.

Use the `trc-gateway-10.x.x.<arch>.rpm` file to install gateway support in Linux™. Where *10.x.x* is the version that you want to install. For more information about obtaining the Linux™ gateway support files, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

Type the following command at a command prompt to install the gateway support, where *10.x.x* is the version that you want to install.

To install the `trc-<component>-10.x.x.<arch>.rpm` package of the component, run the dnf, yum, or zypper command by providing the install -y option and the RPM package file path. Otherwise, if you want to manually resolve the dependencies then run the `rpm -ivh trc-gateway-10.x.x.<arch>.rpm` command. You can also get the complete dependency list by running the `rpm -qpR trc-gateway-10.x.x.<arch>.rpm` command.

When the gateway support installed, configure it for your environment. For more information about configuring gateway support, see the *BigFix® Remote Control Administrator's Guide*.

Install broker support

Broker support must be installed on the computers that connect the controller to the target computer when the target computer is not directly accessible by the controller and the connection is made across the internet.

Remote Control provides two ways to install the broker support. If you have access to the BigFix® console, use the deployment fixlets to deploy the broker support. For more information, see the *BigFix® Remote Control Console User's Guide*. Alternatively use the Remote Control broker installation files.

Installing Windows™ broker support

The Remote Control broker installation files are executable files that can be used to install broker support on a Windows™ computer.

The `trc_broker_setup.exe` file is required to install broker support on a Windows™ system. For more information about how to obtain the Windows™ broker support files, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

To install broker support on a Windows™ computer, complete the following steps.

1. Run the `trc_broker_setup.exe` file.
2. Click **Next** at the welcome screen.
3. Accept license terms and click **Next**.
4. Accept the default location or change the installation destination folder. Click **Next**.

   Default location is `\Program Files\BigFix\Remote Control\Broker`
5. Click **Install**.
6. Click **Finish**.

The following files are installed in the *[working dir]*`\Broker` directory, where *[working dir]* is determined by the version of Windows™ operating system that you are installing the broker support on.

For example, `\Documents and Settings\All Users\Application Data\BigFix\Remote Control`.

- `trc_broker.properties`
- `TRCICB-`*`computername-day`*`.log` where *computername* is the computer name of the system that the broker is installed on and *day* is the day of the week that the broker is installed on.

You must check that the **Remote Control- Internet Connection Broker** service is registered and is started.

Installing Linux™ broker support

You can install broker support on a Linux™ computer by using the RPM file that is provided in the Remote Control installation files.

Note: The broker component installation package depends on the following libraries: **glibc**, **libgcc**, **libblkid**, **libstdc++**.

Use the `trc-broker-10.x.x.<arch>.rpm` file to install the broker support in Linux™. Where *10.x.x* is the version that you want to install. For more information about obtaining the Linux™ component installation files, see Install the Remote Control components *(on page 29)*. Choose the appropriate method for obtaining the file.

At a command prompt, type the following command to install the broker software, where *10.x.x* is the version that you want to install.

To install the `trc-<component>-10.x.x.<arch>.rpm` package of the component, run the dnf, yum, or zypper command by providing the install -y option and the RPM package file path. Otherwise, if you want to manually resolve the dependencies, use the `rpm -ivh trc-broker-10.x.x.<arch>.rpm` command. You can also get the complete dependency list by running the `rpm -qpR trc-broker-10.x.x.<arch>.rpm` command.

The following files are installed in the `/opt/bigfix/trc/broker` directory.

- libcrypto.so
- libssl.so
- trc_icb
- A license directory

The `trc_broker.properties` file is installed in the `/etc` directory.

When the broker support is installed, configure the broker properties by editing the `trc_broker.properties` file.

Install Web Session Manager support

The Web Session Manager is automatically included with the broker support installation; no standalone package is needed and is compatible with both Windows and Linux environments.

The Remote Control Web Session Manager is installed automatically when broker support is installed. No separate installation package is required.

For information about installing broker support, see:

- **Windows systems**

  For installing Windows broker support, refer to Installing Windows broker support *(on page 95)*.

- **Linux systems**

  For installing Linux broker support, refer to Installing Linux broker support *(on page 95)*.

After broker support is installed, the Web Session Manager service is available and can be configured for browser-based remote control sessions.

Chapter 5. Utility for extracting the component installation files

Remote Control provides a utility that you can use to extract the installation files that are required for each component.

Extract the data from the `BigFix_Rem_Cntrl_V914_Image_3.tar` file. Go to the `\Disk1\InstData\platform\VM` directory where *platform* is relevant to your operating system. The utility can be run only by using the `trc_additional_setup.exe` or `trc_additional_setup.bin` file. To extract the installation files for other supported operating systems, for example, macOS, run one of the `trc_additional_setup` files to extract the installation files, then copy the `.pkg` files to the macOS system.

Use the following files to run the additional setup utility:

Windows® systems

`trc_additional_setup.exe`

Linux® systems

`trc_additional_setup.bin`

For more information about how to obtain the `BigFix_Rem_Cntrl_V914_Image_3.tar` file, see Obtain the installation files *(on page 29)*.

You can extract the following component installation files.

- Server Installation media: Use the files to run a manual server installation. The `trc.war` file and instructions are extracted.
- Target Installation media:
  - Windows Packages (`.exe` and `.msi`)
  - Linux Package (`.rpm`)
  - macOS Package (.pkg)
- Controller installation media:.
  - Windows Packages (`.exe` and `.msi`)
  - Linux Package (`.rpm`)
  - macOS Package (.pkg)
- Command Line Interface installation media:
  - Windows Packages (`.exe` and `.msi`)
  - Linux Package (`.rpm`)
- Gateway installation media:
  - Windows Packages (`.exe` and `.msi`)
  - Linux Package (`.rpm`)
- Internet Connection Broker installation media:
  - Windows Packages (`.exe` and `.msi`)
  - Linux Package (`.rpm`)

Extract the installation files by using the additional setup utility

To run the additional setup utility, complete the following steps:

1. Run the `trc_additional_setup` file relevant to your operating system.
   The file must be run from within the file structure that is extracted from the `BigFix_Rem_Cntrl_V914_Image_3.tar` file. For more information about which file to use, see Utility for extracting the component installation files *(on page 97)*.
2. Select the language and click **OK**.
3. Accept the license agreement and click **Next**.
4. Clear the options that you do not want to extract the files for. Only the options you require must remain selected.
   a. Server Installation media: to extract the files for installing the server.
   b. Target Installation media: to extract the files for installing the target.
   c. Controller Installation media: to extract the files for installing the controller.
   d. Command Line Interface Installation media: to extract the files for running the command line interface.
   e. Gateway Installation media: to extract the files for installing gateway support.
   f. Internet Connection Broker Installation media: to extract the files for installing broker support.
5. Click **Next**.
6. Accept or change the installation folder. Click **Next**.
7. On the summary screen, click **Install**.
8. When complete, click **Done**.
9. Go to the chosen installation folder.

The installation files are in the following directories:

- `RCServer` - server installation file, `trc.war`.
- `RCTarget` - target installation files.
- `RCController` - controller installation files.
- `RCCLI` - command line tools installation files.
- `RCGateway` - gateway installation files.
- `RCBroker` - broker installation files.

Chapter 6. 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.

The secure registration feature is enabled by default on a new Remote Control server installation when you use the installer program. After you install the server, create a registration token on the server and use it when you install the target. For more information about the secure registration feature and how to create a token, see the **Secure target registration** chapter in the *BigFix® Remote Control Administrator's Guide*

Enable secure target authentication in the server

The BigFix® Remote Control Server provides an installation option to enable secure registration of targets.

When the feature is enabled, the server verifies that a secure registration token that is sent by the target matches an existing token on the server. If the token is valid, the target is registered in the server and receives an endpoint token from the server. The target sends the endpoint token to the server each time it contacts the server.

Note: If you have existing targets in the database and you enable the secure registration feature, the existing targets cannot successfully contact the server because they do not have an endpoint token. Therefore, you must create or use a valid a secure registration token and reinstall the existing targets with the token so that they can continue to contact the server.

Enabling secure registration when you run the server installer program

You can enable the secure target registration feature when you install the server by using the installer program. The feature is enabled by default on a new server installation.

To enable the secure registration feature, complete the following steps:

1. Follow the installation steps in Installing by using the server installer *(on page 36)*.
2. On the **Web server parameters** window, ensure that **Force targets to use https** is selected.
3. Select **Use secure registration tokens to register targets**.
4. Complete the installation.

After you install the server and enable the secure target registration feature, create registration tokens. For more information about creating registration tokens, see the *BigFix® Remote Control Administrator's Guide*.

Enabling secure target registration after you install the server

You can enable the secure target registration feature after you install the server by editing properties in the `trc.properties` file.

To enable the secure registration feature after you install the server, complete the following steps.

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**.

You can also manually edit the properties files and set the property to true. Restart the server after you edit the file. The properties files are in the following directories:

Windows® systems

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

Where *installdir* is the directory that the BigFix® Remote Control Server is installed. For example,

```
C:\Program Files\BigFix\TRC\server\wlp\usr\servers\trcserver
\apps\TRCAPP.ear\trc.war\WEB-INF\classes
```

Linux® systems

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

Where *installdir* is the directory that the BigFix® Remote Control Server is installed. For example,

```
/opt/BigFix/TRC/server/wlp/usr/servers/trcserver/apps/TRCAPP.ear
/trc.war/WEB-INF/classes
```

Add a token for secure target registration

The BigFix® Remote Control Target provides an installation option to add a secure registration token. You can also add the token by running a Fixlet in the BigFix® console.

The token is used to prevent unauthorized targets from registering with the Remote Control server. Create a token on the server and use it when you install the target. The secure registration feature on the server must also be enabled.

The target sends the secure registration token to the server the first time it contacts the server. The server verifies that the token matches an existing token on the server. If the token is valid, the target is registered in the server and receives an endpoint token from the server.

Note:

The target includes the token in its callhome to the server only when it uses a secure connection to the server. The server URL that it uses to connect to the server must start with HTTPS.

Add the secure registration token when you install the target on a Windows™ system

On a Windows™ system, you can add a secure registration token in multiple ways:

- Add the token by using the target installer program.
- Add the token by running the target installation from the command line.
- Modify the target after installation.

Running the target installer with a secure registration token

When you install the target component, use the BigFix® Remote Control Target installer to provide the target with a secure registration token. The target uses the token to authenticate to the server when it contacts the server for the first time.

To run the target installer with a token, complete the following steps:

1. Follow the installation steps in Installing the Windows target *(on page 55)*.
2. On the **Server Address** window, for secure target registration, enter or paste the token in the **Secure registration token** field.
   Ensure that **Use secure connections (https)** is also selected. For more information about secure target registration, see Add a token for secure target registration *(on page 100)*.
3. Complete the installation.

Running a target silent installation with a secure registration token

Install the target along with a secure registration token when you run a new Remote Control target silent installation.

For more information about running a target custom installation, see the *BigFix® Remote Control Installation Guide*.

To install the target component and the token, run the following command on one line.
trc_target_setup.exe /s /v"/qn REGISTRATIONTOKEN=*xxxxxxxxxxx* TRC_SERVER_HOSTNAME=*yyyyyyyyyyyyyy*"

Replace *xxxxxxxxxxx* with the token and *yyyyyyyyyyyyyy* with the host name of your Remote Control server.

For more information about running a silent installation when you upgrade the target, see Upgrading the target with a secure registration token *(on page 102)*.

Adding the secure registration token after you install the target

If you install the target component and do not install the secure registration token, you can modify the target and add the token.

Select the method for adding the token.

To add the token by running the installer program, complete the following steps:

1. Go to the **Control Panel**. For example, **Start > Control Panel > Programs > Programs and Features**.
2. Right-click **Remote Control-Target**.
3. Select **Change**.
4. On the **Program Maintenance** window, select **Modify**.
5. Click **Next** until the **Server Address** window is displayed.
6. Enter or paste the token in the **Secure registration token** field. Ensure that **Use secure connections (https)** is also selected.
7. Click **Install**.
8. Click **Finish**.

To add the token by editing the target registry, complete the following steps:

1. Edit the target registry and go to `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`

   Note: On a 64-bit system, all the 32-bit registry keys are under the **Wow6432Node** key. For example, `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`

2. Right-click **RegistrationToken**.
3. Click **Modify**.
4. Enter or paste the token.
5. Restart the target.

Upgrading the target with a secure registration token

Upgrade the Remote Control target with a secure registration token.

The upgrade process requires two steps. You must upgrade the target first, then run an installation with the token.

- To use the installer to upgrade the target with a token, complete the following steps:

  1. Run the `trc_target_setup.exe` file.
  2. Select **Yes** for an automatic upgrade.
  3. Click **Next**.
     If a **Files in Use** window is displayed, click **OK**.

4. Click **Finish**.
5. To add the token, complete the steps in, Adding the secure registration token after you install the target *(on page 102)*.

- To run a silent installation to upgrade the target with a token, complete the following steps.

  1. At a command prompt type trc_target_setup.exe /s /v"/qn" to upgrade the target.
  2. To add the token run trc_target_setup.exe /s /v"/qn REGISTRATIONTOKEN=xxxxxx REINSTALL=ALL"

     Where *xxxxxx* is replaced by the token that you saved when you created a token.

Add the registration token when you install a target on a Linux™ system

On a Linux™ system, you can add a registration token for secure target authentication by editing the `/etc/trc_target.properties` file after you install the target.

To add a secure registration token to a Linux target, complete the following steps after you install the target. For more information about installing the target on a Linux system, see Installing the Linux target *(on page 76)*.

1. Edit the `/etc/trc_target.properties` file.
2. Add the registration token property and set it to the value of your registration token. Set **RegistrationToken** = *xxxxxxxxxxxxxx*, where *xxxxxxxxxxxxxx* is replaced with your token data. For example, 6386e21f-4316-460b-b339-deb3d132f3c7
3. Save the file.
4. Restart the target service. For more information, see Starting, stopping, or restarting the Linux components *(on page 109)*.

Chapter 7. Install a driver to support smart card authentication in the target

The BigFix® Remote Control Target provides an installation option to install a virtual smart card reader driver. You can also install the driver by running a fixlet in the BigFix® console.

The device driver for the 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*.

The device driver for the virtual smart card reader is supported only in Windows 10 or later and Windows Server 2016 or later.

Installing the virtual smart card reader driver by using the installer

Use the BigFix® Remote Control Target installer to install the device driver for the virtual smart card reader when you install the target component. You can also use the installer to install the driver on a system that has the target component already installed.

For more information about adding the driver after you install the target, see Adding or removing the virtual smart card reader driver by using the installer *(on page 104)*.

To install the target software and the device driver for the virtual smart card reader, complete the following steps:

1. Follow the installation steps in Installing the Windows target *(on page 55)*
2. On the **Additional features** window, select **Install device driver for Virtual Smart Card Reader**.

After you install the driver, you must install a certificate so that the target can automatically enable the driver when smart card authentication is requested. For more information about installing the certificate by running a Fixlet, see the *BigFix® Remote Control Console User's Guide*. You can also download the certificates and install them manually. For more information, see the *BigFix® Remote Control Console User's Guide*.

Adding or removing the virtual smart card reader driver by using the installer

After you install the target component, you can add or remove the device driver for the virtual smart card reader by using the installer.

If you install the target component and do not install the device driver, you can modify the target and add the driver. To add the driver, complete the following steps:

1. Go to the **Control Panel**. For example, **Start > Control Panel > Programs > Programs and Features**.
2. Right-click **Remote Control-Target**.
3. Select **Change**.
4. On the **Program Maintenance** window, select **Modify**.
5. Click **Next** until the **Additional features** window is displayed.
6. Select **Install device driver for Virtual Smart Card Reader**. Click **Next**.
7. Click **Install**.
8. Click **Finish**.

The target can automatically enable the driver when smart card authentication is requested during a remote control session. Use the same procedure to remove the driver. In step 6 *(on page 105)*, clear **Install device driver for Virtual Smart Card Reader**.

After you install the driver, you must install a certificate so that the target can automatically enable the driver when smart card authentication is requested. For more information about installing the certificate by running a Fixlet, see the *BigFix® Remote Control Console User's Guide*. You can also download the certificates and install them manually. For more information, see the *BigFix® Remote Control Console User's Guide*.

Installing the virtual smart card reader driver by running a silent installation

Install the device driver for the virtual smart card reader when you run an Remote Control target silent installation.

You can install the driver when you run a silent installation on a computer that does not have the target component. You can also add or remove the driver from an installed target. For more information about running a target custom installation, see Run a target custom installation *(on page 78)*.

- To install the target component and the device driver for the virtual smart card reader, run the following command.

  trc_target_setup.exe /s /v"/qn VSC=1"

- To add the driver to an installed target, run the following command.

  trc_target_setup.exe /s /v"/qn ADDLOCAL=vsc REINSTALL=service"

- To remove the driver from an installed target, run the following command.

  trc_target_setup.exe /s /v"/qn REMOVE=vsc REINSTALL=service"

After you install the driver, you must install a certificate so that the target can automatically enable the driver when smart card authentication is requested. For more information about installing the certificate by running a Fixlet, see

the *BigFix® Remote Control Console User's Guide*. You can also download the certificates and install them manually. For more information, see the *BigFix® Remote Control Console User's Guide*.

Installing the virtual smart card reader driver when you upgrade the target

Install the device driver for the virtual smart card reader when you upgrade the Remote Control target.

- To install the driver when you upgrade the target by using the installer, complete the following steps:
    1. Run the `trc_target_setup.exe` file.
    2. Select **Yes** for an automatic upgrade.
    3. Click **Next**.
       If a **Files in Use** window is displayed, click **OK**.
    4. Click **Finish**.
    5. To install the driver, complete the steps in, Adding or removing the virtual smart card reader driver by using the installer *(on page 104)*.
- To install the driver when you upgrade by running a silent installation, complete the following steps.
    1. At a command prompt type trc_target_setup.exe /s /v"/qn" to upgrade the target.
    2. To add the driver run trc_target_setup.exe /s /v"/qn ADDLOCAL=vsc REINSTALL=service".

After you install the driver, you must install a certificate so that the target can automatically enable the driver when smart card authentication is requested. For more information about installing the certificate by running a Fixlet, see the *BigFix® Remote Control Console User's Guide*. You can also download the certificates and install them manually. For more information, see the *BigFix® Remote Control Console User's Guide*.

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.

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.

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 *(on page 29)*.
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.

Chapter 8. Manage the component services

After you install the Remote Control components, if you change their configuration, you can stop, start, or restart the component services.

Follow the steps in the section that is relevant to your operating system.

Starting, stopping, or restarting the Windows™ components

You can start, stop, or restart the Remote Control Windows™ components from within the Control Panel.

To manage the Remote Control Windows™ components, complete the following steps.

1. In **Control Panel** select **Administrative tools > Services**.
2. Highlight the relevant service.

   Server service

   Remote Control- Server

   Target service

   Remote Control- Target

   Gateway service

   Remote Control- Gateway

   Broker service

   Remote Control- Internet Connection Broker
3. Choose the appropriate method for selecting an action for the service.
   You can right-click and select **start**, **stop**, or **restart** or select **Start**, **Stop**, or **Restart** from the list on the left.

Starting, stopping, or restarting the Linux™ components

You can start, stop, or restart the Remote Control Linux™ components from within the Control Panel.

Depending on the version of Linux™ you are using, use one of the following commands to manage the components.

- `/sbin/service component action`
- `/etc/init.d/component action`

Where *component* is the component service that you want to manage and *action* is start, stop, or restart.

Server

For example, to start the server service.

- `/sbin/service trcserver start`
- `/etc/init.d/trcserver start`

Target

For example, to stop the target service.

- `/sbin/service trctarget stop`
- `/etc/init.d/trctarget stop`

Gateway

For example, to restart the gateway service.

- `/sbin/service trcgateway restart`
- `/etc/init.d/trcgateway restart`

Broker

For example, to restart the broker service.

- `/sbin/service trcbroker restart`
- `/etc/init.d/trcbroker restart`

Chapter 9. Enabling email

To use the email function, you must install and set up an email server. For example, for a forgotten password, to export and email a report, or to request access to certain targets.

To enable the email function, complete the following steps:

1. Log on to Remote Control server with a valid admin ID and password.
2. Click **Admin > Edit properties files**.
3. Select **trc.properties**.
4. Edit the following variables

   email.enabled

   Set to true to enable email.

   SMTP.server

   Set to the address of your mail server.

   SMTP.authentication

   Set to true of false, Set to true to authenticate with the SMTP ID and password.

   SMTP.userid

   User ID for the SMTP server.

   SMTP.password

   Password for the SMTP server.

5. Click **Submit**.

The email function is enabled.

Chapter 10. Configure LDAP

Remote Control provides Lightweight Directory Access Protocol Version 3 support. You can use LDAP to enable authentication and integration of users and their associated group membership into the Remote Control database.

All configuration information that is required for LDAP authentication is in the `ldap.properties` file. Before you configure, some prerequisite information must be obtained. This information simplifies the configuration process.

- A user name and password to be used by Remote Control to establish a connection with the Active Directory server. This user name must have the authority necessary to read all the required information from the directory tree.
- The fully qualified server host name or IP address of the Active Directory server to be used with Remote Control.
- In an Enterprise scenario, a secondary backup LDAP server would also be configured in Remote Control.

Setting up LDAP synchronization

To enable LDAP authentication, synchronization with the LDAP server must also be enabled. Edit values in the `common.properties` file and the `ldap.properties` file to enable synchronization.

To perform the basic configuration for LDAP authentication, complete the following steps:

1. Click **Admin > Edit properties file**.
2. Ensuring that you are editing the `common.properties` file, edit the following properties

authentication.LDAP

To enable or disable LDAP authentication.

True

LDAP user authentication is enabled.

Note: Each time the synchronization with Active Directory takes place the users and user groups are deleted from the Remote Control database and then imported from Active Directory. Therefore, if LDAP is enabled, new users and new user groups must be created in Active Directory and not in Remote Control.

False

LDAP user authentication is not enabled. Users are authenticated against the Remote Control database.

```
authentication.LDAP=true
```

authentication.LDAP.config

Defines the file that contains the LDAP configuration properties.

```
authentication.LDAP.config=ldap.properties
```

sync.ldap

Synchronize the users and groups from Active Directory with the Remote Control database. Takes the values true, to synchronize or false, for no synchronization.

True

The LDAP server is synchronized with the Remote Control database to reflect any changes that are made in LDAP.

False

No synchronization takes place. If synchronization is disabled, you must manually import the users into the Remote Control database. Otherwise, they cannot log on to the Remote Control server. The users must exist in the Remote Control database so that they can be associated with the relevant permissions that are required to establish remote control sessions.

Note: The synchronization is performed by running a scheduled task. The task pulls the LDAP information from the LDAP server and updates the database with any changes that are made to the user or group information. Within the `trc.properties` file, two attributes define the time interval that the scheduler uses to check for scheduled tasks.

scheduled.interval

The frequency hat the server must check for scheduled tasks. The number of units of time between each checking period. Default is 60.

Note: If you change this value, restart the server service for the new value to take effect.

sync.LDAP.task_run_time

Use to indicate the time of the day the a fixed time synchronization has to occur. This is an alternate setting to scheduled.interval. Possible values: 24 hours notation of the time in HH:MM:SS. For Example 02:00:00 to perform the synchronization at 2 AM.

Note:

- When using usingsync.LDAP.task_run_time the actual task execution time is affected by the scheduled.interval setting, as the LDAP synchronization occurs within the context of the task scheduler. The actual execution time can span

from sync.LDAP.task_run_time to sync.LDAP.task_run_time + scheduled.interval.

- The server must be restarted to use fixed time synchronization.

scheduled.interval.period

The unit of time to be used along with the scheduled interval to specify how often the server must check for scheduled tasks. Default is minutes.

The **scheduled.interval** attribute is set to 60 as default and the **scheduled.interval.period** set to minutes, that is, the server checks for and runs any scheduled tasks every 60 minutes. To accurately reflect any changes to the users or groups, set the **scheduled.interval** attribute to a lower value so that the synchronization can occur more frequently.

3. Click **Submit**.

Verifying connection information

Use parameters to define how Remote Control connects to the LDAP server. The connection is used to query the LDAP server for the user and group information that is imported into Remote Control.

Any changes to the `ldap.properties` file do not take effect until you select **Admin**,**Reset Application**. To avoid multiple restarts or an extended outage use an LDAP browser and the **LDAP Configuration Utility** as an aid to the entire configuration process.

To verify the connection information by using an LDAP browser, define an LDAP server profile by entering the fully qualified host name and credential information. When you open an LDAP browser for the first time, provide details for a new profile.

The profile can include the following information.

Host

Host name or FQDN of the preferred LDAP Server.

Port

Port that is used to communicate with the directory. Typically, port 389 but if your environment contains child domains, port 3268 must be used instead. Port 3268 points to the Global catalog that includes the child domains.

Base DN

The root point to bind to the server. For example, `DC=mydomain,DC=mycompany,DC=com`.

After the information is entered, the LDAP Browser displays attribute names and values available at the root of the Active Directory tree.

When a connection is established, use the same information that is used in the LDAP browser to set the parameters in the `ldap.properties` file.

- Click **Admin > Edit properties files**
- Select **ldap.properties** from the list
- When modifications are complete, click **Submit**

The application must be reset for the changes to take effect. Click **Admin > Reset Application** or restart the server service.

The properties file can also be edited manually by locating it on the BigFix® Remote Control Server. The file is in the `[installdir]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes` directory, where *installdir* is the directory that the BigFix® Remote Control Server is installed in. For example, `C:\Program Files\BigFix\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes`

Note: Remote Control is provided with a default `ldap.properties` file and many of the extended configuration options are commented out. To enable the options, the file must be edited manually.

Note: The BigFix® Remote Control Server is capable of managing one Global catalog only. This means that domain controllers of different domains cannot be managed by the same BigFix® Remote Control Server.

Users belonging to a domain which is not included in the forest specified in the server configuration cannot be added to the users of the same BigFix® Remote Control Server.

Configuring connection credentials

Use the following properties to set valid credentials for connecting to the LDAP server.

Note: Check that a successful connection to the LDAP browser can be established by using these credentials to verify that they are valid.

1. Edit the `ldap.properties` file.
2. Configure the following properties.

ldap.connectionName

The user name that is used to authenticate to a read-only LDAP connection.
If left not set, an anonymous connection is attempted. For example, `administrator@mydomain.mycompany.com`.

ldap.connectionPassword

The password that is used to establish a read-only LDAP connection. The password can be entered here in plain text or it can be encrypted. Use the LDAP wizard to encrypt your password. For more information, see Configure LDAP properties by using the LDAP wizard.

ldap.connectionPasswordEncrypted

True

The LDAP password is encrypted.

False

The LDAP password is not encrypted and entered as plain text.

ldap.connectionURL

The directory URL used to establish an LDAP connection. Type in the URL of your LDAP server.

```
ldap://myldapserver.mydomain.mycompany.com
```

Setting connection security

The following properties define the level of security to be used on the connection to the LDAP server. Set the following parameter to `simple` so that the Remote Control server can communicate with most Active Directory servers.

ldap.security_authentication

Specifies the security level to use. Value can be set to one of the following strings: none, simple, strong. If this property is unspecified, the behavior is determined by the service provider.

```
ldap.security_athentication=simple
```

While most LDAP servers support simple plain text login, some Active Directory administrators require a secure connection. Remote Control supports two types of secure connections to an Active Directory server, **SASL** (Digest-MD5) or **SSL**. If you cannot connect to the Active Directory server and see the following error in the `trc.log`:

```
LDAP Authentication.exception[LDAP: error code 8 - 00002028: LdapErr: DSID-0C09018A,
comment: The server requires binds to turn on integrity checking if SSL\TLS are not
already active on the connection, data 0, vece ]
```

Remote Control needs to be configured for either SASL or SSL connections.

SASL (Simple Authentication and Security Layer)

The following parameters relate to using SASL to secure the connection to the LDAP server. If you are not using SASL, the parameters must not be edited. Comment out the parameters. The following values are used to configure Remote Control to connect to Active Directory that uses SASL in a test environment. Consult your organizations active directory support team to acquire the correct values for your company.

ldap.security_authentication

Specifies the security level to use. If this property is unspecified, the behavior is determined by the service provider. If you are using SSL, the value is set to simple. If you are using SASL, the value is set to the SASL mechanism DIGEST-MD5.

```
ldap.security_authentication= DIGEST-MD5
```

Note: `DIGEST-MD5` is not supported when FIPS is enabled due to security compliance restrictions (MD5 is not FIPS-compliant).

ldap.connectionRealm

The Realm name where the user ID and password resides.

```
ldap.connectionRealm= mydomain.mycompany.com
```

ldap.connectionQop

This value can be one of:

- auth = Authentication only
- auth-int = Authentication and integrity checking by using signatures
- auth-conf = (SASL only) Authentication, integrity and confidentiality checking by using signatures and encryption.

```
ldap.connectionQop= auth-conf
```

ldap.connectionMaxbuf

Number that indicates the size of the largest buffer the server is able to receive when you use *auth-int* or *auth-conf*. The default is 65536.

```
ldap.connectionMaxbuf= 16384
```

ldap.connectionStrength

Connection strength can be one of: low, medium, high.

```
ldap.connectionStrength= high
```

SSL (Secure Socket Layer)

The following parameters define the use of SSL to connect to the Active Directory server. To use SSL, you must install a Root CA public key certificate keystore on the Remote Control Server. If SSL is not used, the parameters can be commented out in the `ldap.properties` file.

ldap.security_protocol

Specifies the security protocol to use. The value is a string that is determined by the service provider. For example, ssl. If this property is unspecified, the behavior is determined by the service provider.

```
ldap.security_protocol =ssl
```

ldap.ssl_keyStore

Enter the location of the keystore file.

```
ldap.ssl_keyStore=PathOfKeyStoreFile
```

ldap.ssl_keyStorePassword

Enter the location of the keystore password.

```
ldap.ssl_keyStorePassword=KeystorePassword
```

Setting user authentication properties

Authenticating the user

Use the following properties to define how the user is authenticated when they attempt to log on to the Remote Control server. To configure the following sections use the LDAP browser as described for each parameter, to derive the correct settings.

ldap.digest

Digest algorithm that is used by LDAP. Values are SHA, MD2, or MD5 only. The default is cleartext. If the LDAP servers returns a password, Remote Control uses the Digest algorithm to encrypt the user input password and compare it with the password it receives from the LDAP server. If no password is returned from the LDAP server, Remote Control uses the user name and password that is provided by the end user to authenticate with LDAP.

```
ldap.digest=SHA
```

ldap.userid

ldap.userid is the LDAP attribute that contains the user ID that is mapped to the **userid** field in the Remote Control database. The **userPrincipalPattern** property then needs to know whether the *@domainname*, UPN suffix, is added for Active Directory authentication.

sAMAccountName

sAMAaccount must be used so that the user ID only portion of the logon, without the UPN Suffix, is used.

userPrincipalName

userPrincipalName must be used to force all logons to use the full User Principal Name.

Note: It is recommended to set **ldap.userid** to this value to ensures that it does not contain any invalid characters. For example, an apostrophe.

The **ldap.userid** relates to other configuration values in the `ldap.properties` file.

For example, if the ldap.userid is set to userPrincipalName, the user must log on to Remote Control with their full ID. For example, `awilson@example.com`.

- The **ldap.userSearch** variable would be (userPrincipalName={0}).
- The **ldap.principalPattern** would be {0}.

If the ldap.userid is set to use sAMAccountName, the user must log on to Remote Control with just the user ID part of their ID. For example, awilson. The following parameters must be set so that the fully qualified name is appended.

For example

- The **ldap.userSearch** variable would be (userPrincipalName={0}@mydomain.mycompany.com)

  For a user awilson@example.com, the **ldap.userSearch** variable would be (userPrincipalName={0})
- The **ldap.principalPattern** would be {0}@mydomain.mycompany.com.

  For a user awilson@example.com, the **ldap.principalPattern** would be `{0}@example.com`.

ldap.userPassword

The name of the LDAP attribute in the user's directory entry that contains the user's password. In Active Directory, password is the default name of the attribute.

```
ldap.userPassword=password
```

ldap.userEmail

The name of the LDAP attribute in the user's directory entry that contains the user's email address.

Note: The **ldap.userEmail** property cannot have a null value. If your Active Directory Tree does not contain email information, a different attribute must be used. For example, **ldap.userEmail** might be set to **userPrincipalName**.

ldap.userRealm

Realm name that is used for user authentication. This setting is optional and can be commented out, in the `ldap.properties` file, for most configurations.

```
ldap.userRealm=users.company.domain.com
```

ldap.principalPattern

Pattern for construction of user principal for using LDAP authentication. Some LDAP servers require email address, for example, `userid@domain.com` and others require the user ID only. The string “{0} is substituted by the users user ID entered at the login screen.

Searching for the users directory entry

The method available for finding the end-users information involves defining a starting point in the Active Directory tree and allowing Remote Control to recursively search through the tree for the userid. For most Active Directory implementations this is the preferred method as users are usually spread out in several locations in an Active Directory tree. This method is especially helpful if user information is contained under a single branch of the tree but broken up by department or underneath the branch

Note: It should be noted that when LDAP has been enabled, new users and new user groups should be created in Active Directory and **not** in Remote Control. This is because each time the synchronization with Active Directory takes place the users and user groups are deleted from the Remote Control database and then imported again from Active Directory.

To use the recursive search configure the following parameters:

ldap.userBase

The base LDAP directory entry for looking up users that match the search criteria. If not specified, the search base is the top-level element in the directory context.

```
for example OU=mylocation,DC=mycompany,DC=com
```

You can refine your search by going deeper into the OU structure and selecting to search only within a specific organizational unit for example an OU called Users and therefore you would set the property value as

```
ldap.userBase=OU=Users,ou=mylocation,dc=mydomain,dc=mycompany,dc=com
```

This would instruct Remote Control to look for users matching the criteria, only within the Users OU (and any OUs that belong to the Users OU if ldap.groupSubtree is set to true)

ldap.userSearch

Defines the LDAP query that is used to import Active Directory users to Remote Control. The defined query needs to filter the results such that only those users which match the search criteria are imported to Remote Control. The default value is

(objectClass=user)

which means, look for users in any object that is a user object within the userbase. That is import all Active Directory users to Remote Control.

Note: When using the above it should be noted that some environments can have thousands of users therefore it is important to create a filter which will only import the required users. To limit the users that are imported to only those users who match the search criteria and are members of the groups that were imported into Remote Control through the **ldap.groupSearch** filter, you should set the property **ldap.userInGroup** to true. It should also be noted that as well as being imported into the relevant groups that are returned in the group search, users are also imported

into the **DefaultGroup**. Setting **ldap.userInGroup** to false will import all users who match the search criteria, regardless of their group membership.

The search can therefore be further refined by using more complex queries. For example if you have the following values set

```
ldap.groupBase=(OU=mylocation.DC=mycompany.DC=com)
Ldap.userSearch: (&(objectClass=user)(|(memberOf=CN=Department1,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com) (memberOf=CN=Department3,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com))(name={0}))
```

If there were three groups defined, Department1, Department2 and Department3 the above query would authenticate and import any users that are defined as objectclass user and are members of the Department1 OR Department3 groups. Users from Department2 would not be able to logon to Remote Control.

The (&(name={0}) is added to the end to specify that the name attribute is used for logging in. This value has to match whatever attribute was specified as ldap.userid.

ldap.userSubtree

Set this value to true if you want to recursively search the sub tree of the element specified by the userBase attribute for the user's directory entry. The default value of false causes only the top level to be searched (a nonrecursive search). This is ignored if you are using the userPattern expression.

```
ldap.userSubtree=true
```

Importing Active Directory Groups

One of the greatest benefits of integrating with Active Directory is being able to use existing Active Directory groups. After Active Directory groups are imported, an administrator must define the permissions for each group and group membership is handled inherently by Active Directory. To import Active Directory groups, configure the following properties in the `ldap.properties` file.

Note: If the Active Directory server is a global catalog you can successfully import all groups in the domain forest however only the members of the Universal Groups will be automatically assigned to them. This occurs because Universal Groups are the only group type whose full membership list replicates to every Global Catalog server in the forest. So other groups type don't report membership information on the global catalog.

ldap.groupName

The LDAP attribute name that is used for the group search.

```
ldap.groupName=cn    OR   ldap.groupName=name
```

ldap.groupDescription

The LDAP attribute name to be used to get the description for the group. It is set to description by default.

```
ldap.groupDescription=description
```

ldap.groupNameTrim

Set to true or false. Limits the group name that is imported to the Remote Control database to 64 characters. The recommended value is false.

ldap.groupMembers

LDAP attribute name to be used to find the members of the groups that are returned as a result of the specified search. The default value is member.

```
ldapgroupMembers=member
```

ldap.groupSubtree

If set to true, Remote Control searches recursively through the subtree of the element that is specified in the **ldap.groupBase** parameter for groups that are associated with a user. If left unspecified, the default value of false causes only the top level to be searched, and no recursive search is run. True or False (default).

ldap.groupBase

The base LDAP directory entry for starting the search for groups to synchronize. If left unspecified, the default is to use the top-level element in the directory context.

```
for example OU=mylocation,DC=mycompany,DC=com
```

To refine your search and go deeper into the OU structure, select to start the search only within a specific organizational unit. For example, an OU called Test. Set the property to the following value.

```
OU=Test,OU=mylocation,DC=mycompany,DC=com
```

Therefore, Remote Control looks for groups that match the criteria, only within the Test OU (and any OUs that belong to the Test OU if **ldap.groupSubtree** is set to true).

ldap.groupSearch

Defines the LDAP query that is used to import AD groups to Remote Control. The defined query needs to filter the results such that only those groups that are needed are imported to Remote Control.

`ldap.groupSearch=(objectClass=group)`

Imports all AD groups found in the OU specified in the **ldap.groupBase** property to Remote Control. Some environment can have thousands of groups.

`ldap.groupSearch=(&(objectClass=group)(cn=*SMS*))`

Imports all groups that contain SMS in the **cn** attribute. For example, *visio-sms-users*.

`ldap.groupSearch=(&(objectClass=group)(cn=admins))`

Imports all groups that are named admins.

`ldap.groupSearch=(&(objectClass=group)(cn=admins*))`

Imports all groups that have the text admins in the name. For example, administrators, server-administrators.

ldap.groupMembers

LDAP attribute name to be used to find the members of the groups that are returned as a result of the specified search. The default value is member.

These queries can be tested by using the LDAP browsers directory search option or the LDAP configuration utility in the Remote Control server UI.

Testing the Connection

When the `common.properties` & `ldap.properties` files are updated, reset the Remote Control application by selecting **Admin > Reset Application**.

When the service restarts, log on to the Remote Control server by using an Active Directory user ID and password. If the entries in the LDAP properties file are correct, you are authenticated and logged on successfully.

BigFix® Remote Control Server connects directly to LDAP. Therefore, any password changes within LDAP are immediately effective only if the LDAP password change synchronizes to the LDAP server that is set within the `ldap.properties` file.

Note: The default ADMIN user ID within the BigFix® Remote Control Server application always authenticates against the BigFix® Remote Control Server regardless of whether LDAP authentication is enabled. If there is a connectivity problem between BigFix® Remote Control Server and LDAP, the ADMIN user can always log on.

If there are any errors in the `ldap.properties` file, you see a failed logon message. The **Logon** screen is displayed with an Invalid user name or wrong password message.

To determine the cause of the failure look in the `trc.log` file. View the application log by using the server UI.

- In the BigFix® Remote Control Server UI, click **Admin > View application log**
- Click **CTRL+END** to reach the end of the file.

The following common errors can be displayed. The errors indicate a problem with creating the initial connection between BigFix® Remote Control Server and Active Directory.

AcceptSecurityContext error, data 525

Returns when user name is invalid.

AcceptSecurityContext error, data 52e

Returns when user name is valid but password or credentials are invalid. Prevents most other errors from being displayed as noted.

AcceptSecurityContext error, data 530

Logon failure: account logon time restriction violation. Displays only when presented with valid user name and password credentials.

AcceptSecurityContext error, data 531

Log on failure: user is not allowed to log on to this computer. Displays only when presented with valid user name and password credentials.

AcceptSecurityContext error, data 532

Logon failure: the specified account password is expired. Displays only when presented with valid user name and password credentials.

AcceptSecurityContext error, data 533

Logon failure: account currently disabled. Displays only when presented with valid user name and password credential.

AcceptSecurityContext error, data 701

The user's account is expired. Displays only when presented with valid user name and password credential.

AcceptSecurityContext error, data 773

The user's password must be changed before they log on for the first time. Displays only when presented with valid user name and password credential.

AcceptSecurityContext error, data 775

The referenced account is locked out and cannot be logged on to. Displays even if invalid password is presented.

LDAP Authentication.exceptionmyserver.mydomain.com:389

Displays when the server name specified by **ldap.connectionURL** is unreachable.

Verifying that the groups are imported

When authentication is successful and you are logged on to the Remote Control server, click **User groups > All User Groups** to verify that the correct groups were imported from Active Directory.

After the groups are imported into Remote Control, define permissions for the newly imported groups.

Sample LDAP Configuration File

The file is a sample configuration file. It uses a simple connection to Active Directory with importing of Active Directory groups

LDAP Properties

Server Authentication definition

The directory URL used to establish an LDAP connection

ldap.connectionURL=ldap://myldapserver

define the secondary LDAP server name, if the primary is down we can use an alternative LDAP server

#–**ldap.alternateURL=**

The username used to authenticate a read-only LDAP connection. If left not set, an anonymous connection is made.

ldap.connectionName=administrator@mydomain.MyCompany.com

The password used to establish a read-only LDAP connection.

ldap.connectionPassword=myPassword

Instructs Remote Control to read the value of the password parameter as encrypted (true) or plain text (false). See Admin guide for instructions on generating encrypted password

ldap.connectionPasswordEncrypted=false

The fully qualified Java™ class name of the JNDI context factory to be used for

this connection. If left unset, the default JNDI LDAP provider class is used.

--- -**ldap.contextFactory=com.sun.jndi.ldap.LdapCtxFactory**

SASL Definition

specifying the security level to use. Its value is one of the following strings: "simple" or "DIGEST-MD5".

. If using SSL, you have to use simple.

ldap.security_authentication=simple

#Identifies the realm or domain from which the connection name should be chosen

---- **ldap.connectionRealm=**

#Quality of protection

QOP can be one of: auth, auth-int, auth-conf

auth -- Authentication only

auth-int --Authentication and integrity checking by using signatures

auth-conf -- (SASL only) Authentication, integrity and confidentiality checking

by using signatures and encryption.

----**ldap.connectionQop=auth**

Number indicating the size of the largest buffer the server is able to receive when

using "auth-int" or "auth-conf". The default is 65536.

ldap.connectionMaxbuf=16384

Strength can be one of: low,medium,high

----**ldap.connectionStrength=high**

SSL Definition

specifying the security protocol to use. Its value is a string determined by

the service provider (for example: "ssl"). If this property is unspecified, the behaviour

is determined by the service provider.

----**ldap.security_protocol=ssl**

Access the keystore, this is where the Root CA public key cert was installed

No need to specify the keystore password for read operations

----**ldap.ssl_keyStore=PathOfKeyStoreFile**

----**ldap.ssl_keyStorePassword=KeystorePassword**

specifying how referrals encountered by the service provider are to be processed.

The value of the property is one of the following strings:

"follow" -- follow referrals automatically

"ignore" -- ignore referrals

"throw" -- throw ReferralException when a referral is encountered.

If this property is not specified, the default is determined by the provider.

----**ldap.referrals=follow**

define Group search for LDAP

The base LDAP directory entry for looking up group information. If left unspecified,

the default is to use the top-level element in the directory context.

ldap.groupBase=OU=Groups,OU=mylocation,DC=mydomain,DC=mycompany,

DC=com

#The LDAP filter expression used for performing group searches.

ldap.groupSearch=(&(objectClass=group) (name=TRC*))

Set to true if you want to recursively search the subtree of the element specified in

the groupBase attribute for groups associated with a user. If left unspecified, the default

value of false causes only the top level to be searched (a nonrecursive search).

ldap.groupSubtree=true

#The LDAP attribute that we should use for group names.

ldap.groupName=name

#The LDAP attribute that we should use for group descriptions

ldap.groupDescription=description

This is the attribute specifying user members within a group

ldap.groupMembers=member

User search definition

#The base of the subtree containing users

#If not specified, the search base is the top-level context.

ldap.userBase=OU=Users,OU=mylocation,DC=mydomain,DC=mycompany, DC=com

The LDAP filter expression to use when searching for a user's directory entry, with {0} marking

where the actual username is inserted.

ldap.userSearch=(&(objectClass=User)(sAMAccountName={0}))

Set this value to true if you want to recursively search the subtree of the element specified by

the userBase attribute for the user's directory entry. The default value of false causes only the

top level to be searched (a nonrecursive search).

ldap.userSubtree=true

#Set this value to true if a user has to be a member of the groups found in the group search

ldap.userInGroup=true

Digest algorithm (SHA, MD2, or MD5 only)

Remote control will use it to encrypt the user input password and

compare it with password it receives from the LDAP server. If left unspecified, the default value is "cleartext".

---- **ldap.digest=SHA**

#LDAP attribute used for userids

ldap.userid=sAMAccountname

LDAP User password attribute

ldap.userPassword=password

LDAP Attribute containing the Users Email address

ldap.userEmail=userPrincipalName

If the following parameters are defined they are mapped into the local remote control database

ldap.forename=givenName

ldap.surname=sn

ldap.title=title

ldap.initials=initialsg

ldap.company=company

ldap.department=department

ldap.telephone=telephoneNumber

ldap.mobile=mobile

ldap.state=st

ldap.country=Co

Other property definitions

#Set this value to the page size of LDAP search retrievals (default=500).

Do not set this to anything greater than the max page size for the LDAP server (for example, AD has a limit of 1000)

ldap.page.size=500

Chapter 11. Configure Microsoft Entra ID

Remote Control provides Microsoft® Entra ID support. You can use Microsoft® Entra ID to enable authentication and integration of users and their associated group membership into the Remote Control database.

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

- Client ID
- Tenant ID
- Secret

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

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

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

Setting up Microsoft Entra ID synchronization

To enable Microsoft Entra ID authentication with SAML 2.0 Single sign-on (SSO), synchronization must be enabled. Edit values in the `common.properties` file and the `identity_providers.properties` file to enable synchronization.

To perform the basic configuration for Microsoft Entra ID authentication, complete the following steps:

1. Click **Admin > Edit properties** file.
2. Ensuring that you are editing the `common.properties` file, edit the following properties

   sync.entraID

   Synchronizes the users and groups from Microsoft Entra ID with the Remote Control database. Takes the values true, to synchronize or false, for no synchronization.

   True

   Microsoft Entra ID is synchronized with the Remote Control database to reflect any changes that are made.

   False

   No synchronization takes place. If synchronization is disabled, you must manually import the users into the Remote Control database. Otherwise, they cannot log on to the Remote Control server. The users must exist in the Remote Control database

so that they can be associated with the relevant permissions that are required to establish remote control sessions.

Note:

Only one synchronization task can be enabled at the same time; if this property is enabled together with the LDAP synchronization (**sync.LDAP**), then only the LDAP synchronization task will be executed. The synchronization is performed by running a scheduled task. The task automatically deletes all users and groups data while starting so before running it is recommended to perform a backup. The task also pulls the Microsoft Entra ID information and updates the database with any changes that are made to the user or group information. Within the `trc.properties` file, two attributes define the time interval that the scheduler uses to check for scheduled tasks.

scheduled.interval

The frequency that the server must check for scheduled tasks. The number of units of time between each checking period. Default is 60.

Note: If you change this value, restart the server service for the new value to take effect.

sync.entraID.task_run_time

Use to indicate the time of the day the a fixed time synchronization has to occur. This is an alternate setting to scheduled.interval. Possible values: 24 hours notation of the time in HH:MM:SS. For Example 02:00:00 to perform the synchronization at 2 AM.

Note:

- When using using **sync.entraID.task_run_time** the actual task execution time is affected by the **scheduled.interval** setting, as the Microsoft Entra ID synchronization occurs within the context of the task scheduler. The actual execution time can span from **sync.entraID.task_run_time** to **sync.entraID.task_run_time** + **scheduled.interval**.
- The server must be restarted to use fixed time synchronization.

scheduled.interval.period

The unit of time to be used along with the scheduled interval to specify how often the server must check for scheduled tasks. Default is minutes. The **scheduled.interval** attribute is set to 60 as default and the **scheduled.interval.period** set to minutes, that is, the server checks for and runs

any scheduled tasks every 60 minutes. To accurately reflect any changes to the users or groups, set the **scheduled.interval** attribute to a lower value so that the synchronization can occur more frequently.

3. Click **Submit**.

Verifying connection information

Use parameters to define how Remote Control connects to Microsoft Entra ID. The connection is used to query Microsoft Entra ID for the user and group information that is imported into Remote Control.

Any changes to the `identity_providers.properties` file do not take effect until you select **Admin > Reset Application**. To avoid multiple restarts or an extended outage use the **Microsoft Entra ID Configuration Utility** as an aid to the entire configuration process.

In order to establish a connection to an existing Enterprise application, set the parameters in the `identity_providers.properties` file.

- Click **Admin > Edit properties files**
- Select **identity_providers.properties** from the list
- When modifications are complete, click **Submit**

The application must be reset for the changes to take effect. Click **Admin > Reset Application** or restart the server service.

The properties file can also be edited manually by locating it on the BigFix® Remote Control Server. The file is in the `[installdir]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes` directory, where *installdir* is the directory that the BigFix® Remote Control Server is installed in. For example, `C:\Program Files\BigFix\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes`

Note: Remote Control is provided with a default `identity_providers.properties` file and many of the extended configuration options are commented out. To enable the options, the file must be edited manually.

Note: In order to successfully connect to Microsoft Entra ID, the App Registration needs to have at least the following Microsoft Graph API permissions:

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

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

Configuring connection credentials

Use the following properties to set valid credentials for connecting to Microsoft Entra ID.

1. Edit the `identity_providers.properties` file.
2. Configure the following properties.

entraID.clientID

The Client ID used to establish a connection to Microsoft Entra ID.

entraID.tenantID

The Tenant ID used to establish a connection to Microsoft Entra ID.

entraID.secret

The secret that is used to establish a read-only connection to Microsoft Entra ID. This secret can be entered here in plain text or it can be encrypted. Use the **Microsoft Entra ID Configuration Utility** to encrypt your secret. For more information, see Configure Microsoft Entra ID properties by using the configuration utility.

entraID.secretEncrypted

True

The Microsoft Entra ID secret is encrypted.

False

The Microsoft Entra ID secret is not encrypted and is entered as plain text.

entraID.authorityHost

Specifies the Azure Authority Host to use. Its value is one of the following strings:

- https://login.microsoftonline.com for Public Cloud
- https://login.microsoftonline.us for US Government

Setting user authentication properties

Authenticating the user

Use the following properties to define how the user is authenticated when they attempt to log on to the Remote Control server. To configure the following sections use Microsoft Entra ID Configuration Utility as described for each parameter, to derive the correct settings.

entraID.userID

entraID.userID is the Microsoft Entra ID attribute that contains the user ID that is mapped to the userid field in the Remote Control database.

Note: It is recommended to set **entraID.userid** to **userPrincipalName** to ensure that, after enabling the SAML 2.0 Single sign-on (SSO), the Microsoft Entra User will be able to login to the Remote Control Server.

Searching for the users

Remote Control allows searching through all the available users that matches the chosen user filter.

Note: It should be noted that when Microsoft Entra ID has been enabled, new users and new user groups should be created in Microsoft Entra ID and **not** in Remote Control. This is because each time the synchronization with Microsoft Entra ID takes place the users and user groups are deleted from the Remote Control database and then imported again from Microsoft Entra ID.

To filter users, configure the following parameter:

entraID.userFilter

Defines the Microsoft Entra ID filter that is used to import users to Remote Control. The defined query needs to filter the results such that only those users which match the search criteria are imported to Remote Control. The default value is empty.

Note: When using the above parameter, note that some environments can have thousands of users therefore it is important to create a filter which will only import the required users. To limit the users that are imported to only those users who match the search criteria and are members of the groups that were imported into Remote Control through the **entraID.groupFilter** filter, you should set the property **entraID.userInGroup** to true. It should also be noted that as well as being imported into the relevant groups that are returned in the group search, users are also imported into the **DefaultGroup**. Setting **entraID.userInGroup** to false will import all users who match the search criteria, regardless of their group membership. The search can therefore be further refined by using more complex queries. For more information, refer to https://learn.microsoft.com/en-us/graph/filter-query-parameter.

Importing Groups

One of the greatest benefits of integrating with Microsoft Entra is being able to use existing groups. After Microsoft Entra groups are imported, an administrator must define the permissions for each group and group membership is handled inherently by Microsoft Entra. To import Microsoft Entra groups, configure the following properties in the `identity_providers.properties` file.

entraID.groupFilter

The Microsoft Entra filter that is used for the group search. It is set to **startswith(displayName,'TRC')** by default. For more information, please refer to https://learn.microsoft.com/en-us/graph/filter-query-parameter.

Testing the Connection

The connection to Microsoft Entra ID can be tested with **Admin > Microsoft Entra ID Configuration Utility**.

When the `common.properties` & `identity_providers.properties` files are updated, reset the Remote Control application by selecting **Admin > Reset Application**.

When the service restarts, log on to the Remote Control server by using the SAML 2.0 Single Sign-on (SSO) with Microsoft Entra ID as the identity provider. If the entries in the `identity_providers.properties` file are correct, you are authenticated and logged on successfully.

Verifying that the groups are imported

When authentication is successful and you are logged on to the Remote Control server, click **User groups > All User Groups** to verify that the correct groups were imported from Microsoft Entra ID. After the groups are imported into Remote Control, define permissions for the newly imported groups.

Migrating from LDAP to Microsoft Entra ID

In order to migrate to Microsoft Entra ID all the existing LDAP users and groups that are used with the Remote Control Server please consider the following steps:

1. Create the same group hierarchy and users on Microsoft Entra ID.

   Note: In order to retain the existing permissions, it is recommended to create the new groups on Microsoft Entra ID with the same names of the ones that were available with LDAP.

2. Use the **Admin > Microsoft Entra ID Configuration Utility** in order to test the connection and to apply the required configuration for groups and users.
3. Disable the LDAP authentication and synchronization and enable the Microsoft Entra ID synchronization by setting the following properties in the common.properties file:
   - **authentication.LDAP=false**
   - **sync.LDAP=false**
   - **sync.entraID=true**

   Note: It is recommended to perform a database backup.

4. Enable the SAML 2.0 Single sign-on (SSO) on the Remote Control Server with Microsoft Entra ID as the Identity Provider (IdP). For more information please see Chapter 4. Configure SAML 2.0 authentication on the server.
5. Restart the Remote Control Server service.
6. Microsoft Entra ID users can login to the Remote Control Server by using SAML 2.0 Single sign-on (SSO).

Note: After enabling SAML 2.0 Single sign-on (SSO), the Microsoft Entra ID users can login with their **userPrincipalName** (for instance, *user@contoso.onmicrosoft.com*). For more information, visit https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-userprincipalname#upn-in-microsoft-entra-id

For this reason it is recommended to check the value of the following parameter into the `identity_providers.properties` file:

- **entraID.userID**=userPrincipalName

7. Check that the old group hierarchy has been successfully restored after the first Microsoft Entra ID synchronization. To check, go to **User groups > All User Groups**.

Sample Microsoft Entra ID Configuration File

The file is a sample configuration file that can be used in order to configure Microsoft Entra ID in the Remote Control Server.

Identity Providers Properties

Connection Definition for Microsoft Entra ID

Client ID used to establish a connection to Microsoft Entra ID

entraID.clientID=

Tenant ID used to establish a connection to Microsoft Entra ID

entraID.tenantID=

Secret used to establish a connection to Microsoft Entra ID

entraID.secret=

Instructs Remote Control to read the value of the secret parameter as encrypted (true) or plain text (false)

entraID.secretEncrypted=false

Specifies the Azure Authority Host to use. Its value is one of the following strings:

"https://login.microsoftonline.com/" -- Public Cloud

"https://login.microsoftonline.us/" -- US Government

entraID.authorityHost=https://login.microsoftonline.com/

Base URL for Microsoft Entra ID

entraID.baseUrl=https://graph.microsoft.com/v1.0

Default scope for Microsoft Entra ID

entraID.defaultScope=https://graph.microsoft.com/.default

Groups Definition for Microsoft Entra ID

Microsoft Entra ID filter expression used for groups searches

 e.g. startswith(displayName,'TRC')

entraID.groupFilter=startswith(displayName,'TRC')

Users Definition for Microsoft Entra ID

Microsoft Entra ID filter expression used for users searches

 e.g. startswith(displayName,'Bob')

entraID.userFilter=startswith(displayName,'Bob')

Set this value to true if a user has to be a member of the groups found in the group search

entraID.userInGroup=false

Microsoft Entra ID attribute used for User ID

entraID.userID=userPrincipalName

Microsoft Entra ID attribute containing the Users Email address

entraID.userEmail=userPrincipalName

entraID.forename=givenName

entraID.surname=surname

entraID.employeeID=employeeId

entraID.title=jobTitle

entraID.location=officeLocation

entraID.company=companyName

entraID.department=department

entraID.address=streetAddress

entraID.mobile=mobilePhone

entraID.state=state

entraID.country=country

Other Settings for Microsoft Entra ID

Set this value to the page size of Microsoft Entra ID search retrievals (default=500). It must be between 1 and 999 (both inclusive)

entraID.pageSize=500

Chapter 12. Federal information processing standard (FIPS) compliance in Remote Control

The US Federal information processing standard 140-2 (FIPS 140-2) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software.

When configured in FIPS 140-2 mode, Remote Control uses the following FIPS 140-2 approved cryptographic modules:

The IBM Java JCE FIPS 140-2 Cryptographic Module (IBMJCEFIPS) is a scalable, multipurpose cryptographic module that supports many FIPS approved cryptographic operations. This module is used in the Remote Control Server ((until versions 10.0.0.0736 included) and in the Remote Control Controller up to version 10.0.0.0518 included (Windows and Linux Only). The certificate number for this cryptographic module is #2715 is held on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2715.

The IBM Java JCE FIPS 140-2 Cryptographic Module (IBMJCEPlusFIPS) supersedes the IBMJCEFIPS. The new provider has similar functionality to the older equivalent but offers support for newer algorithms, additional hardware-accelerated cryptographic capabilities (where supported) and performance enhancements. This module is used in the Remote Control Server starting from version 10.0.0.0818 until version 10.1.0.0128 included. The certificate number for this cryptographic module is #3064 is held on the NIST website at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3064. Starting from version 10.1.0 Fix Pack 2 the Remote Control Server is using the IBM Java JCE FIPS 140-3 Cryptographic Module (IBMJCEPlusFIPS). Starting from version 10.1.0 Fix Pack 5 the Remote Control Server is using the OpenJCEPlusFIPS provider. The certificate number for this cryptographic module is #4755 is held on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4755.

The BC-FJA (Bouncy Castle FIPS Java API) (BCFIPS) is a comprehensive suite of FIPS Approved algorithms implemented in pure Java. This module is used in the Remote Control Controller starting from Version 10.0.0.0600 (Windows, Linux and MacOS) until 10.1 Fix Pack 4. The certificate number for this cryptographic module is #3514 is held on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3514.

Starting from version 10.1.0 Fix Pack 5 the Remote Control Controller is using the IBM Java JCE FIPS 140-3 Cryptographic Module. The certificate number for this cryptographic module is #4755 is held on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4755.

The OpenSSL FIPS Object Module is a general purpose cryptographic module. This module is used in the Remote Control Target, Broker, and other native components. The certificate number for the cryptographic module used in Remote Control version up to 10.0.0.0818 included is #1747 is held on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1747. The certificate number for the cryptographic module used in Remote Control starting from version 10.1.0 is #4282 is held on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4282.

Enable FIPS compliance on the server

Enabling FIPS compliance on a server installation with a stand-alone Open Liberty Application Server

The BigFix® Remote Control Server uses the middleware infrastructure that is provided by Open Liberty® secure HTTP communications. Therefore, to enable FIPS for a manual BigFix® Remote Control Server installation requires that you configure Open Liberty® for FIPS-compliant mode. You must also configure the BigFix® Remote Control Server through a setting in the `common.properties` configuration file.

To enable FIPS compliance for a manual installation, complete the following steps:

1. Configure Open Liberty

   Note: Running in FIPS mode in IBM® Open Liberty ® with the IBM® JRE and the IBM® JSSE provider currently does not work when you use an MS SQL database. These options work with MS SQL when FIPS is not enabled in IBM® WebSphere.

2. Log on to the BigFix® Remote Control Server with a valid admin ID and password.
3. Click **Admin > Edit properties files**
4. In the `common.properties` file set **FIPS.compliance** to true.
5. Click **Submit**.
6. Click **Admin > Reset Application**.

Note: The FIPS enablement changes in WebSphere affect all other applications that are running on the server. Therefore, browser settings for the users who access the other applications must be changed to support Transport Layer Security (TLS), if required by their browser version.

Enabling FIPS compliance on an automated server installation

Enable During Server Installation

To enable FIPS compliance on the BigFix® Remote Control Server, run the Remote Control Server Installer and select **Enable FIPS** and **Enable NIST SP800-131A** in the **Web server parameters** panel.

Enable Manually

To enable FIPS compliance can be configured manually on the BigFix® Remote Control Server instead of running the Remote Control Server Installer by following this procedure:

1. Edit the `java.security` file that is found at the following directory.

   Windows® systems

   %TRC_SERVER_PATH%`\java\jre\lib\security\java.security`

   Where *%TRC_SERVER_PATH%* is the path for the installation directory for the BigFix® Remote Control Server.

Linux® / UNIX® systems

$TRC_SERVER_PATH/java/jre/lib/security/java.security

Where *$TRC_SERVER_PATH* is the path for the installation directory for the BigFix® Remote Control Server.

2. Modify the *security.provider.x*= list so the following entry is the first one in the list:

   security.provider.1=com.ibm.crypto.plus.provider.OpenJCEPlusFIPS

   Fix the number sequence of the other items in this list so that all items are numbered in sequence.

   For example:

   - The full list after the changes when performed on a Remote Control server build 10.0.0.0808 until 10.1 Fix Pack 4 is as follows:

     ```
     security.provider.1=com.ibm.crypto.plus.provider.IBMJCEPlusFIPS
     security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
     security.provider.3=com.ibm.crypto.plus.provider.IBMJCEPlus
     security.provider.4=com.ibm.crypto.provider.IBMJCE
     security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
     security.provider.6=com.ibm.security.cert.IBMCertPath
     security.provider.7=com.ibm.security.sasl.IBMSASL
     security.provider.8=com.ibm.xml.crypto.IBMXMLCryptoProvider
     security.provider.9=com.ibm.xml.enc.IBMXMLEncProvider
     security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
     security.provider.11=sun.security.provider.Sun
     ```

   - The full list after the changes when performed on a Remote Control server build 10.0.0.0807 or earlier is as follows:

     ```
     security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPS
     security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
     security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
     security.provider.4=com.ibm.crypto.provider.IBMJCE
     security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
     security.provider.6=com.ibm.security.cert.IBMCertPath
     security.provider.7=com.ibm.security.sasl.IBMSASL
     security.provider.8=com.ibm.xml.crypto.IBMXMLCryptoProvider
     security.provider.9=com.ibm.xml.enc.IBMXMLEncProvider
     security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
     security.provider.11=sun.security.provider.Sun
     ```

3. Add the following lines:

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

4. Save the file.
5. Edit the `jvm.options` that are found in the following directory.

   Windows® systems

   %TRC_SERVER_PATH% `\wlp\usr\servers\trcserver\jvm.options`

   Where *%TRC_SERVER_PATH%* is the path for the installation directory for the BigFix® Remote Control Server.

   Linux® / UNIX® systems

   $TRC_SERVER_PATH`/wlp/usr/servers/trcserver/jvm.options`

   Where *$TRC_SERVER_PATH* is the path for the installation directory for the BigFix® Remote Control Server.

6. Add the following lines:
   - Remote Control server build 10.1 FP 5 or later

     ```
     -Dsemeru.fips=true
     -Dsemeru.customprofile=OpenJCEPlusFIPS.FIPS140-3-Strongly-Enforced
     ```

   - Remote Control server build 10.1 FP 2 until 10.1 FP 4

     ```
     -Dcom.ibm.jsse2.usefipsprovider=true
     -Dcom.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS -Xenablefips140-3
     ```

   - Remote Control server build 10.1 FP 2 or later

     ```
     -Dcom.ibm.jsse2.usefipsprovider=true
     -Dcom.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS
     -Xenablefips140-3
     ```

   - Remote Control server build 10.0.0.0808 until version 10.1.0.0128 included

     ```
     -Dcom.ibm.jsse2.usefipsprovider=true
     -Dcom.ibm.jsse2.sp800-131=strict
     -Dcom.ibm.jsse2.overrideDefaultTLS=true
     -Dcom.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS
     ```

   - Remote Control server build 10.0.0.0807 or earlier

     ```
     -Dcom.ibm.jsse2.usefipsprovider=true
     -Dcom.ibm.jsse2.sp800-131=strict
     -Dcom.ibm.jsse2.overrideDefaultTLS=true
     ```

7. Save the file.

8. Log on to the BigFix® Remote Control Server with a valid admin ID and password.
9. Click **Admin > Edit properties files**
10. In the `common.properties` file set **FIPS.compliance** to true.
11. Click **Submit**.
12. Click **Admin > Reset Application**. Restart the server service.
13. Restart the server service.

Check to see whether the BigFix® Remote Control Server is configured for FIPS by completing the following step.

- Click **Admin > View Current Server Status**.

The following fields show that FIPS compliance is enabled.

- Enabled FIPS mode: The value of this field is determined by the **FIPS.compliance** property in the `common.properties` file.
- JVM configured for FIPS: The value of this field is determined by the configuration of the JVM and the security providers that are listed in the `java.security` file.

Troubleshooting:

- **Browser or Controller connection with the Remote Control server may fail**

  If the server is configured to operate in FIPS mode with the following exception in the `messages.log` file `java.lang.NullPointerException com.ibm.ws.channel.ssl.internal.SSLConnectionLink 238`, Browser or Controller connection with the Remote Control server might fail.

  This is a side effect of the adoption of IBM Java 8.0.6.26. If the issue persists, do the following:

  1. Stop the Remote Control Server.
  2. Open the `..\TRC\java\jre\lib\security\java.security` file and add the `RSAPSS` value as the last entry of the `jdk.tls.disabledAlgorithms`.

     The updated property list must look as follows:

     ```
     jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, DESede,
      \ EC keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC, RSAPSS
     ```

  3. Start the Remote Control Server.

- **The Join Broker Session operation may fail**

  When the secondary controller connects to the primary controller and the environment is configured to operate in FIPS mode, the Join Broker Session operation may fail. The primary controller may show an exception like the foll following exception in the `messages.log` file:

  ```
  SEVERE - The connection was refused with pkt type [260]
  ```

This is a side effect of the adoption of IBM Java 8.0.6.26. If the issue persists, do the following:

Open the `..\Controller\jre\lib\security\java.security` file and add the `RSAPSS` value as the last entry of the `jdk.tls.disabledAlgorithms`. The updated property list should look as follows:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, DESede, \ EC
 keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC, RSAPSS
```

- **The playback of a session recording via the Server Web Interface may fail to start with no error message shown if the Server is Configured to operate in FIPS mode**

  This is a side effect of the adoption of IBM Java 8.0.6.26. If the issue persists, do the following:

  1. Save the `TRCPlayer.trcjws` file as provided by the server.
  2. Edit the File and remove the line `<argument>--forcefips</argument>`
  3. Save the file and execute the `TRCPlayer.trcjws` file by clicking on it.

Enabling FIPS compliance on the controller

The Controller installation package includes a FIPS certified JRE which is used to run the application. When the Controller start is triggered from the Remote Control server, the FIPS settings which are set on the server are automatically applied to the application. So in this case once FIPS compliance is enabled no other actions are needed.

However, if the Controller is started manually to establish a peer-to-peer session with a Target, you need to edit the local Controller configuration.

The local Controller configuration must be changed to enable the FIPS compliance for peer-to-peer sessions.

Note: Only required if you are running the controller locally for establishing peer-to-peer sessions (a Remote Control server is not being used).

To set FIPS compliance on the Controller when operating in peer to peer mode update the local configuration as follows:

Edit the `trc_controller.cfg` file on the system that the controller is installed on.

Windows® systems

`[controller install dir]\trc_controller.cfg`

Where *[controller install dir]* is the installation directory that is chosen when you install the controller.

Linux® / UNIX® systems

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

Set the **fips.compliance** property to True and save the file.

Check to see whether the controller is configured for FIPS by completing the following step during a remote control session.

- Click **Controller tools > Show session information** in the controller window.

Enable FIPS compliance on the target

The Remote Control target includes FIPS-capable OpenSSL libraries. You can enable FIPS compliance at installation time or by editing the target registry on a Windows® system or by changing the configuration file on a Linux® system.

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

Using the target user interface, choose the appropriate option to verify that the target is in FIPS mode.

- On the Remote Control- Target user interface, click **Actions Menu > Connection info**
- Hover the mouse over the **Remote Control** icon in the system notification area.

Enabling FIPS compliance on a Windows™ target

On a Windows™ system, you can enable FIPS compliance on the target in two ways; during installation or by editing the target registry after installation.

Enabling FIPS compliance by using the target installer

Enable the FIPS compliance target property during installation by completing the following steps:

1. On the **Server Address** panel of the target installer, click **Advanced settings**.
2. Select **Use a FIPS certified cryptographic provider** and **Use secure connections (https)**. Continue with the rest of the target installation.

Performing a silent installation

When performing a silent target installation, run the installation command and use the **FIPSCOMPLIANCE** property to enable FIPS on the target . For more details of performing a silent installation, see Running a target custom installation on a Windows system *(on page 78)*.

Use the following properties when enabling FIPS mode

- TRC_SERVER_PROTOCOL=https
- TRC_SERVER_PORT=443
- FIPSCOMPLIANCE=yes

For example : trc_target_setup.exe /s /v"/qn TRC_SERVER_HOSTNAME=yourserver TRC_SERVER_PROTOCOL=https TRC_SERVER_PORT=443 FIPSCOMPLIANCE=yes"

where ***yourserver*** is the hostname or IP address of your BigFix® Remote Control Server.

Enabling FIPS compliance after target installation

After you install the Remote Control target, you can enable FIPS compliance by editing the target registry. To enable FIPS compliance, complete the following steps.

1. Run the regedit command at a command prompt window.
2. In the Windows™ registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`
3. Right-click **FIPSCompliance** and select **Modify**.
4. Type `yes` in the **Value data** field and click **OK**.
5. Restart the target service.
   For more information about restarting the target service, see Manage the component services *(on page 109)*.
   Follow the steps in the section that is relevant to your operating system.

Enabling FIPS compliance in Linux® or UNIX® based operating systems

After you install the Remote Control target, you can enable FIPS compliance by editing the `trc_target.properties` file. To enable FIPS compliance, complete the following steps:

1. Edit the `/etc/trc_target.properties` file.
2. Set the value of *FIPSCompliance* to yes and save the file.
3. Restart the target service.
   For more information about restarting the target service, see Manage the component services *(on page 109)*.
   Follow the steps in the section that is relevant to your operating system.

Enabling FIPS compliance on the gateway

You can enable FIPS compliance on the gateway component by editing the gateway configuration file that is created when you install gateway support.

The `trc_gateway.properties` file is in the following directory.

Windows™ systems

`\Documents and Settings\All Users\Application Data\BigFix\Remote Control\Gateway`

or `\ProgramData\BigFix\Remote Control\Gateway`.

Linux™ systems

`/etc`

To enable FIPS compliance, complete the following steps.

1. Edit the `trc_gateway.properties` file.
2. Set **FIPSCompliance = Yes**.
3. Save the file.

4. Restart the gateway service.
   For more information about restarting the gateway service, see Manage the component services *(on page 109)*. Follow the steps in the section that is relevant to your operating system.

Enabling FIPS compliance on the broker

You can enable FIPS compliance on the broker component by editing the broker configuration file that is created when you install broker support.

The `trc_broker.properties` file is in the following directory.

Windows® systems

`\Documents and Settings\All Users\Application Data\BigFix\Remote Control \broker`.

or `\ProgramData\BigFix\Remote Control\broker`.

Linux® systems

`/etc`

To enable FIPS compliance, complete the following steps.

1. Edit the `trc_broker.properties` file.
2. Set **FIPSCompliance = Yes**.
3. Save the file.
4. Restart the broker service.
   For more information about restarting the broker service, see Manage the component services *(on page 109)*.
   Follow the steps in the section that is relevant to your operating system.

Chapter 13. NIST SP800-131A compliance in Remote Control

Remote Control version 10.0.0 components can be configured for NIST SP800-131A compliance.

The National Institute of Standards and Technology (NIST) Special Publications (SP) 800-131A standard strengthens algorithms and increases the cryptographic key lengths to improve security.

The following prerequisites are required:

- Ensure that all keys have at least a key security strength greater than or equal to 112 bits. RSA keys must be at least 2048 bits.
- Ensure that all certificates are created with the new key strengths. Any RSA certificates that use keys shorter than 2048 bits must be replaced with a certificate that uses 2048-bit keys or higher.
- Ensure that all certificates are signed by an allowed signature algorithm of minimum SHA-2.

When you enable NIST SP800-131A compliance, the TLSv1.2 protocol is used for providing secure connections. Therefore, you must ensure that your browser is compatible.

Compliance with NIST SP800-131A also requires that the cryptographic provider is FIPS 140-2 certified. When SP800-131A compliance is enabled, FIPS 140-2 compliance is enabled automatically, even when it is disabled in the settings.

For NIST SP800-131A compliance, you must configure all your components. There is no compatibility with earlier versions of the components.

Note:

- There is no support for NIST SP800-131A with Oracle JVMs. Therefore, to take advantage of the NIST support, you must install the stand-alone controller component.
- The NIST SP800-131A support has been deprecated due to the availability of the new FIPS 140-3 module. For more information about the FIPS 140-3 module, see Federal information processing standard (FIPS) compliance in Remote Control *(on page 139)*.

Enable NIST SP800-131A compliance on the server

You can enable NIST SP800-131A compliance on the Remote Control server during installation, when you are using the server installer program. You can also enable NIST compliance after installation. To enable NIST SP800-131A compliance for a manual BigFix® Remote Control Server installation, you must configure theBigFix® Remote Control Server and WebSphere®.

Enabling NIST SP800-131A compliance during the server installation

To enable NIST SP800-131A compliance during installation, follow the instructions in Installing by using the server installer *(on page 36)*. Select **Enable NIST SP800-131A compliance (Enables FIPS)** on the **Web server parameters** pane during the installation.

Enabling NIST SP800-131A compliance on a server with a stand-alone WebSphere Application Server

The BigFix® Remote Control Server uses the middleware infrastructure that is provided by WebSphere® secure HTTP communications. Therefore, to enable NIST SP800-131A compliance for a manual BigFix® Remote Control Server installation you must configure BigFix® Remote Control Server and WebSphere®.

To enable NIST SP800-131A compliance for a manual server installation, complete the following steps after you install the server.

1. Configure WebSphere

   Refer to the IBM WebSphere® documentation on how to enable NIST SP800-131A in WebSphere®. Follow the instructions relevant to your version of WebSphere®.
2. Log on to the BigFix® Remote Control Server with a valid admin ID and password.
3. Click **Admin > Edit properties files**
4. In the `common.properties` file set **sp800131a.compliance** to true.
5. Click **Submit**.
6. Click **Admin > Reset Application**.
7. Restart the server service.
   For more information about restarting the server service, see Manage the component services *(on page 109)*. Follow the steps in the section that is relevant to your operating system.

Note: NIST SP800-131A enablement changes in WebSphere® affect all other applications that are running on that server. Therefore, browser settings for the users who access those other applications must be changed to support Transport Layer Security (TLS).

For example, to enable TLS in Firefox, complete the following steps.

- In the browser, go to the **about:config** page.
- Click **I'll be careful, I promise**.
- In the search field search for **security.tls.version.max**.
- Set the value to 3.

Enabling NIST SP800-131A compliance after you install the server

After you install the server by using the installer program, you can enable NIST SP800-131A compliance in a number of ways.

However, if you did not already enable FIPS you must enable if first. For more information about enabling FIPS after you install the server, see Enabling FIPS compliance on an automated server installation *(on page 140)*.

You must also make sure that the server certificate is compliant by ensuring that you follow the prerequisites for NIST support. For more information about certificate prerequisites, see NIST SP800-131A compliance in Remote Control *(on page 148)*.

To enable NIST SP800-131A compliance after an automated BigFix® Remote Control Server installation, complete the following steps.

1. Choose the appropriate method for enabling the NIST configuration.

   Option 1

   a. Go to the tools directory that is in the server installation directory.
   b. Edit the `trcsetup.cmd` or `trcsetup.sh` file, depending on your operating system.
   c. In the line that calls the `ssl.cmd` or `ssl.sh` file, change the 0 that is before **trc** to a 1. Change the 0 that is at the end of the command to a 1 also. For example,

      The command before the change is,

      ```
      ...\tools\ssl.cmd" "C:\Program Files (x86)\BigFix\TRC\server"
       1 0 "C:\" "%CERTSTOREPW%" "servername.localnet" 0 trc
        "%CERSTOREPWSELF%" "TrC" "0"
      ```

      The command after the change is,

      ```
      ...\tools\ssl.cmd" "C:\Program Files (x86)\BigFix\TRC\server"
       1 0 "C:\" "%CERTSTOREPW%" "servername.localnet" 1 trc
        "%CERSTOREPWSELF%" "TrC" "1"
      ```

   d. Save the file.
   e. In the same directory, edit `tmem.sh` or `tmem.cmd`, depending on your operating system.
   f. Set the value of **NIST800=1**. Set the value of **FIPSON=1** if it is not already set.
   g. Run the following command.

      ```
      trcsetup userid password certpassword
      ```

      Where *userid* and *password* are the database connection credentials and *certpassword* is your certificate file password.

Note: Derby does not have database credentials, therefore use `userid` and `password` for the credentials. Type the following command when you are using Derby.

```
trcsetup userid password certpassword
```

Option 2 - Temporary NIST configuration

Note: The configuration changes set in this option are overwritten if you run the `trcsetup` or `tmem` files again.

a. Edit the `ssl.xml` file that is in the `[installdir]\wlp\usr\servers\trcserver` directory.

   Where

   [installdir]

   Is the server installation directory.

b. Add **sslProtocol="TLSv1.2"** to the line **ssl id="defaultSSLConfig"**. For example,

```
<server>
<ssl id="defaultSSLConfig" sslProtocol="TLSv1.2"
/>
<keystore id="defaultKeyStore" password="TrCWebAS"
/>
</server>
```

c. Save the `ssl.xml` file.
d. In the same directory, edit the `jvm.options` file.
e. Add the lines, **-Dcom.ibm.jsse2.sp800-131=strict** and **-Dcom.ibm.jsse2.overrideDefaultTLS=true**.
f. Save the file.

2. Log on to the BigFix® Remote Control Server with a valid admin ID and password.
3. Click **Admin > Edit properties files**
4. In the `common.properties` file, set **sp800131a.compliance** to true.
5. Click **Submit**.
6. Click **Admin > Reset Application**. Restart the server service.
   For more information about restarting the server service, see Manage the component services *(on page 109)*.
   Follow the steps in the section that is relevant to your operating system.

Check to see whether the BigFix® Remote Control Server is configured for NIST SP800-131A by completing the following step.

- Click **Admin > View Current Server Status**.

The following fields show that NIST SP800-131A compliance is enabled.

- Enabled NIST SP800-131A mode
- JVM configured for NIST SP800-131A mode

Creating a certificate for an MS SQL database when NIST SP800-131A is enabled

When you enable NIST SP800-131A compliance and you are using an MS SQL database, you must create a certificate.

To generate the certificate, you can use the IBM® Key Management tool. You can access the IBM® Key Management tool if the Remote Control server is installed with embedded components and also if the controller component is installed. It is also provided by IBM® WebSphere® Application Server.

Note: To create a certificate with 4096 key size or greater, you must overwrite the restriction policy files `local_policy.jar` and `US_export_policy.jar`.

Go to the following directory and copy the `local_policy.jar` and `US_export_policy.jar` files.

Windows™ systems

```
TRC\server\java\demo\jce\policy-files\unrestricted
```

Linux™ systems

```
TRC/server/java/demo/jce/policy-files/unrestricted
```

Replace the following files with the JAR files that you copied.

Windows™ systems

```
TRC\server\java\jre\lib\security\local_policy.jar
```

```
TRC\server\java\jre\lib\security\US_export_policy.jar
```

Linux™ systems

```
TRC/server/java/jre/lib/security/local_policy.jar
```

```
TRC/server/java/jre/lib/security/US_export_policy.jar
```

To create and install the certificate, complete the following steps:

1. Install one of the supported versions of MS SQL server and the latest patches. Minimum requirement is MS SQL Server 2012 Service Pack 3.
2. Create a keystore with a self-signed certificate.

a. Open a command line window.

b. Go to one of the following directories to run the keytool.

Remote control server that is installed with embedded components

Go to the Remote Control server installation directory.

WebSphere® Application Server is installed

Go to the WebSphere® Application Server installation directory.

The controller component is installed

Go to the `...\Controller\jre` directory. For example,

Windows™ systems.

```
C:\Program Files\BigFix\Remote Control\Controller\jre
```

Linux™ systems.

```
/opt/bigfix/trc/controller/jre
```

c. Change to the `bin` directory.

d. Run the `ikeyman` file relevant to your operating system.

Windows™ systems

```
ikeyman.bat
```

Linux™ systems

```
ikeyman.sh
```

e. Select **Key Database File > New**

f. Select **PKCS12** for **Key database type**.

g. Click **Browse** and go to the location in which you want to store the keystore.

h. Type a file name for your file and click **Save**.

i. Click **OK**.

j. Enter and confirm a password to protect the keystore and click **OK**.

k. Select **Create > New Self-Signed Certificate**

l. Enter a name for the **Key Label**.
For example, the host name of the server.

m. Select **X509 V3** for the **Version**.

n. Select a **Key Size** value.

Recommended value for NIST SP800-131A compliance is 2048 or greater.

o. Select **SHA256WithRSA** for the **Signature Algorithm**

p. Type a **Common Name**.
Set to the DNS host name of your server.
For example, `trcserver.example.com`.

q. Enter any additional optional information as required.

r. Enter a **Validity Period**.
Set the number of days that the certificate is valid for. Default is 365 days.

s. Set the **Subject Alternative Names**, **DNS Name** option to the DNS host name of your server.

t. Click **OK**.

3. Add the certificate store to the database server.

a. At a command line, run `mmc.exe`.

b. Add a certificate snap-in.
   i. Select **File > Add/Remove Snap-in**.
   ii. Select the **Certificates** snap-in and click **Add**.
   iii. Select **Computer account** and click **Next**.
   iv. Ensure that the **Local computer** option is selected and click **Finish**.
   v. Click **OK**.

c. Import the certificate
   i. In the **Console1** window, go to **Console Root > Certificates**.
   ii. Right click **Certificates** and select **All Tasks > Import**.
   iii. Click **Next** on the **Welcome** window.
   iv. Click **Browse** and select the certificate store that you created.
   v. Click **Next**.
   vi. Enter the password for the certificate store and click **Next**.
   vii. Ensure that **Place all certificated in the fololwing store** is selected and that **Certificate Store** is set to **Personal**. Click **Next**.
   viii. Click **Finish**.

4. Manage private keys.
   a. Right-click the certificate file and select **All Tasks > Manage Private Keys**.
   b. Click **Add**.
   c. Click **Check Names**, select **MSSQLSERVER** and click **OK**.
   d. Click **OK** on the **Select Users and Groups** window.
   e. Set permissions for **MSSQLSERVER** on the **Permissions** window and click **OK**. For example, select **Allow** for **Read** for a Read-only option.

5. To complete the configuration, run the SQL Server Configuration Manager.
    a. Expand **SQL Server Network Configuration**.
    b. Right click **Protocols for MSSQLSERVER** and select **Properties**.
    c. On the **Certificates** tab, select your imported certificate.
    d. On the **Flags** tab set **Force Encryption** to *Yes* and click **OK**.
    e. Click **OK** on the Warning window.
    f. Select **SQL Server Services**.
    g. Right-click **SQL Server (MSSQLSERVER) > Restart** in the right pane.

Enabling NIST SP800-131A compliance on the controller

The IBM® JRE for Windows® operating system and Linux® (Intel®) operating systems is included with Remote Control and is installed when you install the controller software.

If you are using a Windows® system, the JRE is included in the controller package `trc_controller_setup.exe` and `trc_controller.msi`. For Linux® systems, the JRE is included in the package `trc-controller-jre-10.x.x.<arch>.rpm`. Where 10.x.x is the version that you want to install. The packages install the IBM® Java™ Run-time Environment preconfigured with the IBM® FIPS certified cryptographic provider and NIST SP800-131A enabled. The packages also register the MIME type `application/x-trc-jws` and a file association for `*.trcjws` files.

To check whether the controller is connected in FIPS or NIST SP800-131A mode during a remote control session, click **Controller tools > Show session information**. Encryption is set to AES FIPS when FIPS mode is enabled and is set to TLSv1.2 when NIST mode is enabled.

Enabling NIST SP800-131A compliance in the stand-alone controller

After you install the stand-alone controller, you can edit the properties file to enable NIST SP800-131A compliance.

If you install the controller component locally to start peer to peer remote control sessions, you must edit the `trc_controller.cfg` file to enable NIST SP800-131A compliance. To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `trc_controller.cfg` file on the system that the controller is installed on.

    Windows® systems

    [controller install dir]\trc_controller.cfg

    Where *[controller install dir]* is the installation directory you chose when you installed the controller.

    Linux® systems

    `opt/Bigfix/trc/controller/trc_controller.cfg`

2. Set **sp800131a.compliance** to true.
3. Save the file.

Enable NIST SP800-131A compliance on the target

You can enable NIST SP800-131A compliance on the Remote Control target in various ways. NIST SP800-131A compliance can be enabled during installation when you are using the target installation program. You can enable NIST SP800-131A compliance after the installation by editing the target registry on Windows® systems, or by editing the configuration file on Linux® systems.

Using the target user interface, choose the appropriate option to verify that NIST SP800-131A compliance is enabled on the target.

- On the Remote Control- Target user interface, click **Actions Menu > Connection info**.
- Hover the mouse over the **Remote Control** icon in the system notification area.

Enabling NIST SP800-131A compliance in a Windows® target

When you are using a Windows operating system, you can enable NIST SP800-131A compliance on the target in two ways. You can enable compliance during installation or by editing the target registry after installation.

Enabling NIST SP800-131A compliance during the target installation

To enable the NIST SP800-131A compliance target property during installation, follow the instructions in Install the target *(on page 55)*. On the **Server Address** screen of the target installer, click **Advanced settings**. Select **Enable NIST SP800-131A compliance (Enables FIPS)**.

Enabling NIST SP800-131A compliance during silent installation of the target

To enable NIST SP800-131A compliance during a silent installation of the target, you can use the **SP800131A** parameter in the installation command. For more information about a target silent installation, see Running a target custom installation on a Windows system *(on page 78)*.

Use the following parameters to enable NIST SP800-131A compliance.

- TRC_SERVER_PROTOCOL=https
- TRC_SERVER_PORT=443
- SP800131A=yes

For example, `trc_target_setup.exe /s /v"/qn TRC_SERVER_HOSTNAME=`*`yourserver`*` TRC_SERVER_PROTOCOL=https TRC_SERVER_PORT=443 SP800131A=yes"`

Where *yourserver* is the host name or IP address of your BigFix® Remote Control Server.

Enabling NIST SP800-131A compliance after target installation

After you install the Remote Control target, you can enable NIST SP800-131A compliance by editing the target registry. To enable NIST SP800-131A compliance, complete the following steps.

1. Run the regedit command at a command prompt window.
2. In the Windows™ registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`
   On a 64-bit system, the 32-bit registry keys are under the WOW6432Node key.
   For example, `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`.
3. Right-click **SP800131ACompliance** and select **Modify**.
4. Type `yes` in the **Value data** field and click **OK**.
5. Restart the target service.
   For more information about restarting the target service, see Manage the component services *(on page 109)*.
   Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on Linux® or UNIX® based targets

After you install the Remote Control target, you can enable NIST SP800-131A compliance by editing the `trc_target.properties` file. To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `/etc/trc_target.properties` file.
2. Set the value of *SP800131ACompliance* to yes and save the file.
3. Restart the target service.
   For more information about restarting the target service, see Manage the component services *(on page 109)*.
   Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on the gateway

You can enable NIST SP800-131A compliance on the gateway component by editing the gateway configuration file that is created when you install gateway support.

The `trc_gateway.properties` file is in the following directory.

Windows™ systems

`\Documents and Settings\All Users\Application Data\BigFix\Remote Control\Gateway`

or `\ProgramData\BigFix\Remote Control\Gateway`.

Linux™ systems

`/etc`

To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `trc_gateway.properties` file.
2. Set **SP800131ACompliance = Yes**.
3. Save the file.
4. Restart the gateway service.
   For more information about restarting the gateway service, see Manage the component services *(on page 109)*. Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on the broker

You can enable NIST SP800-131A compliance on the broker component by editing the broker configuration file that is created when you install broker support.

The `trc_broker.properties` file is in the following directory.

Windows® systems

`\Documents and Settings\All Users\Application Data\BigFix\Remote Control \broker`

or `\ProgramData\BigFix\Remote Control\broker`.

Linux® systems

`/etc`

To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `trc_broker.properties` file.
2. Set **SP800131ACompliance = Yes**.
3. Save the file.
4. Restart the broker service.
   For more information about restarting the broker service, see Manage the component services *(on page 109)*.
   Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on the CLI tools

NIST SP800-131A compliance can be enabled during installation when you are installing the CLI tools on a Windows operating system. You can enable NIST SP800-131A after you install the CLI tools in Linux by editing the configuration file.

Enabling NIST SP800-131A compliance when you install the Windows cli tools

To enable NIST SP800-131A compliance during the installation of the command line interface tools, follow the instruction in Installing the cli tools on a Windows system *(on page 90)*. Click **Advanced settings** on the **Server Address** screen, and select **Enable NIST SP800-131A compliance (Enables FIPS)** during the installation.

Enabling NIST SP800-131A compliance on the cli on Linux® or UNIX® based targets

After you install the cli tools, you can enable NIST SP800-131A compliance by editing the `trc_target.properties` file. To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `/etc/trc_target.properties` file.
2. Set the value of *SP800131ACompliance* to yes.
3. Save the file.

Chapter 14. Verifying the server installation

When you complete the server installation, you can verify it by completing the following steps:

1. In a browser window, type the address of the Remote Control server. For example,`http://yourservername/trc` where *yourservername* is the host name or IP address of your Remote Control server.
2. Verify that the Remote Control logon screen is displayed.
3. Log on with the following admin ID and password - *id=admin*, *password=password*.
4. At the change details screen, change the password by following the instructions that are given.

Chapter 15. Recover from installation errors

If you experience installation errors, use the following chapters to identify the problem and address it.

Recovery steps

Use the following information as a starting point to find log files and other information to help you recover from installation errors.

If you must contact HCL Software Support, gather the following information.

- If you are using a Windows™ operating system, any event log that is relevant to the installation error.
- The installation log files.
- Operating system version, including any service packs.
- The version of the WebSphere® Application Server, database server, and Java™.
- Hardware description.
- Installation media type.
- Windows™ services that were active during the unsuccessful installation. For example, antivirus software.

The following files can also be used to gather information about any errors that might occur.

`\tsetup.ini`

Contains some basic information, logged during an automated installation.

`[installdir]\install.log`

Contains internal debug messages.

`[installdir]\inst.ini`

Contains all parameters about the installation.

`[installdir]\wlp\usr\server\trcserver`

Contains configuration xml files.

`[installdir]\wlp\usr\server\trcserver\logs\messages.log`

`[installdir]\wlp\usr\server\trcserver\logs\messages_xxxxxxx.log`

`[installdir]\wlp\usr\server\trcserver\logs\ffdc directory`

Errors during installation

The following topics describe recovery actions for errors that might occur during the Remote Control server installation when you use the server installer program.

Not enough memory

Symptom

Memory error reported during the installation and the installation does not continue.

Cause

The memory check at the beginning of the installation determines that the computer that you are installing on does not have the required minimum memory for installation.

Solution

For more information about the requirements for memory, see Server requirements *(on page 16)* .

DB2® connection error when database options are verified

Symptom

DB2® database connection error reported during installation.

Causes

During the installation if you select DB2® as the database, the installer verifies the information that is given in the database options screen. The user ID, password, and port values are used to establish a connection to the database. If a connection is not successful, an error is reported. This error also contains the error reported by DB2®.

Solution

This error can be reported for any of the following reasons.

- Incorrect values are entered in the database options screen. Go back to the previous screen and verify the information.
- There is no database instance present. If you are planning to use DB2®, it must be installed before the Remote Control server. A database instance must also be created.
- Cannot connect to the remote database. If you are using a remote database, verify that you can ping the IP address of the remote system.

Oracle pre-checks

Symptom

Oracle database connection error reported during installation.

Cause

During the installation if you select Oracle as the database, the installer verifies the information that is given in the database options screen by connecting to the database. If the connection fails, an error is reported. The error message contains the error that is returned from Oracle.

Solution

Go back to the previous screen and use the information that is given to correct the problem.

For example: If the Oracle database is not created before the installation, the following error is reported.

```
Failed to verify userid, password, server, database and driver
file combination supplied.Please verify details and try again.
 ( Listener refused the connection with the following error:
ORA-12505. TNS:listener does not currently know of SID given in
connect descriptor
The Connection descriptor used by the client was:
127.0.0.1:1521:TRCDB
```

In this case, you must cancel the installation and create the Oracle database before you install Remote Control again.

libstdc++.so.5 error when installing the server using the installation program

Symptoms

The server installation aborts with the following exception error in Linux®.

```
This application has unexpectedly quit:Invocation of this Java application has caused an
InvocationTargetException. This application will now exit".
```

The installation log may show the following error

```
java.lang.unsatisfiedlinkerror :fontmanager (libstdc++.so.5: can not open shared object file:No
such file or directory)
```

Causes

Missing package required.

Solution

Install the **libstdc++.so.5** package. This can be installed by installing the **compat-libstdc++-33** package which includes libstdc++.so.5.

Errors after installation

When the installation of Remote Control is complete and the application service starts, you can log on. If you cannot log on successfully, use the following information to resolve the problem.

- Check that the server service is running.

  Windows™ systems

  In Windows™ services, check that the following service is started

  Remote Control-Server.

  Linux™ systems

The following service is created `/etc/init.d/trcserver` or `/etc/rc.d/init.d/trcserver` and started.

Note: To manually stop or start the server type the following command.

`/etc/init.d/trcserver [parameter]` Where *parameter* is *stop*, *start*, or *restart*.

- Check the log files in the `[installdir]\wlp\usr\server\trcserver\logs` directory for any reported errors. You can also check the `trc.log` file in the server installation directory.
- If you are using an Oracle database, check that the user ASSET exists.

Out of memory error

Symptom

Out of memory errors are reported in the log files when the BigFix® Remote Control Server is started. `Failed to instantiate heap` is reported in them.

Causes

There is not enough memory available to run the application. The reason for the error is that the maximum memory that is allocated to the heap is too high, and can be affected by other applications that are running or installed.

During installation, the installer attempts to set up the Remote Control application to use up to 70% of available RAM. The percentage is lowered if a Java virtual machine™ (JVM) cannot be started. However, if other software is installed, an out of memory error might also be reported in the Remote Control log files.

Solution

The solution to this problem is to use a supplied script to manually set the memory parameters to a lower value. This script, can be found in the Remote Control installation directory. Use the script to set the memory parameters and the number of threads and web connections.

- `tmem.cmd` - for Windows® systems.
- `tmem.sh` - for UNIX based systems.

Run the following command from the Remote Control installation directory:

```
tmem.cmd minmem maxmem
```

Note: Use tmem.sh for UNIX based systems.

minmem; maxmem

Sets the minimum and maximum memory to be allocated.

Note: The 32-bit Java that is supplied in 32-bit eWAS can use a maximum of 2.7 GB only, no matter how much RAM is available.

You can also use the tmem.cmd and tmem.sh command to adjust the following parameters.

maxwebconn

Sets the number of web connections allowed. The default is 85 and can increase to 175.

maxthreads; minthreads

Sets the minimum and maximum threads allowed. Maximum threads are 50, increasing to 150.

To edit these parameters in version 10.x.x, complete the following steps:

1. Edit `trcsetup.cmd` or `trcsetup.sh`.
2. Edit the line that contains the call to the `memory.cmd` file. For example, `C:\TRC\server\tools\memory.cmd 163 49 135 1`

   Where
   - **maxwebconn** = parameter 1 (163)
   - **minthreads** = parameter 2 (49)
   - **maxthreads** = parameter 3 (135)

   Do not edit parameter 4. Keep the value 1.
3. Change the required values.
4. Save the `trcsetup` file.
5. Type the following command.

   ```
   trcsetup userid password certpassword
   ```

   Where *userid* and *password* are the database connection credentials and *certpassword* is your certificate file password.

   Note: Derby does not have database credentials, therefore use user ID and password for the credentials. Type the following command when you are using Derby:

   trcsetup userid password *certpassword*

Database connection authorization failure

Symptom

A database connection authorization failure error is reported in the log files.

Causes

The database password might be invalid.

Solution

Change the password by running the following command from the Remote Control installation directory:

Windows® systems.

`[installdir]\tools\tdbpasswd.cmd userid password`. Where *installdir* is the Remote Control installation directory and *userid* and *password* are the database logon credentials.

UNIX based systems.

`[installdir]/tools/tdbpasswd.sh userid password.` Where *installdir* is the Remote Control installation directory and *userid* and *password* are the database logon credentials.

Run the command to change the database password for the application. Restart the Remote Control service after you run the command.

Application welcome page does not display

Symptom

The Remote Control server welcome page does not appear when you type in the Remote Control server URL in your browser.

Cause

The issue can occur for a number of reasons, which are reported in the log files.

Solution

Look through the `install.log` file in the server installation directory, for any reported errors.

DB2® connection error when database options are verified

Symptom

DB2® database connection error reported during installation.

Causes

During the installation if you select DB2® as the database, the installer verifies the information that is given in the database options screen. The user ID, password, and port values are used to establish a connection to the database. If a connection is not successful, an error is reported. This error also contains the error reported by DB2®.

Solution

This error can be reported for any of the following reasons.

- Incorrect values are entered in the database options screen. Go back to the previous screen and verify the information.
- There is no database instance present. If you are planning to use DB2®, it must be installed before the Remote Control server. A database instance must also be created.
- Cannot connect to the remote database. If you are using a remote database, verify that you can ping the IP address of the remote system.

Targets cannot contact the server

Symptom

Targets are not registering or updating their details on the BigFix® Remote Control Server.

Causes

- The target does not have the correct URL for the server.
- The host name part of the URL, that is used to contact the server, does not match the common name in the server's SSL certificate.

Solution

When you install the target software the target contacts the server by using http or https, and the server URL that is defined during the installation of the target. However, there are two important things to note to ensure that the connection between the server and target is successful.

- The target must have the correct URL for the server.
- The host name part of the URL must match the common name in the server's SSL certificate.

When the BigFix® Remote Control Server is installed with the installation program, you must ensure that you supply the correct values in the **Web server parameters** window. By default, the **upload data to server** field is populated with the computer name from the Windows® operating system settings. The server installer program uses the field value to generate the server URL. The URL is then saved in the `trc.properties` file, in the **url** property and is also saved in the SSL certificate. Therefore, make sure that you specify the correct computer name during the installation. If you specify an incorrect value, the following problem might occur.

When a target contacts the server for the first time, it uses the **ServerURL** property from the target registry or configuration file to contact the server. When the server responds to the target, it includes the server address that is assigned to the **url** property in the `trc.properties` file. The target uses this URL to contact the server. If the address that is sent to the target is incorrect, the target can register once and then is not able to contact the server again. After a while, the target is marked as being offline. You are also unable to start sessions with this target, because the target does not have a correct working URL with which to authenticate an incoming session.

The common name that is in the server's SSL certificate must be a host name that resolves to the IP address of the server. If the SSL certificate has, for example, *mytrcserver*, but on the target there

is no way to translate *mytrcserver* to the IP address of the server, your environment is not correctly configured. The only names that are correctly supported are fully qualified domain names that are registered in the DNS. For example, *mytrcserver.example.ibm.com*. To use only *mytrcserver*, the server and target must be on the same local network and have WINS configured.

You can check that the DNS server is properly configured by using the nslookup command to query the full computer name and IP address.

For example: At a command prompt type, the following commands.

```
C:\>nslookup

Default Server:  dns.example.ibm.com
Address:  192.0.2.0



Type in the hostname of your server

> mytrcserver.example.ibm.com
Server:  dns.example.ibm.com
Address:  192.0.2.0

Name:    mytrcserver.example.ibm.com
Address:  192.0.2.1



Type in the ip address of your server

> 192.0.2.1
Server:  dns.example.ibm.com
Address:  192.0.2.0

Name:    mytrcserver.example.ibm.com
Address:  192.0.2.1
```

you can see that the server host name resolves to the correct IP address.

Errors when you use Oracle as the database

Symptom

`java.lang.ArrayIndexOutOfBoundsException` error reported when you use an Oracle database.

Cause

There is a problem with the Oracle jdbc drivers.

Solution

Choose the appropriate option to resolve the problem.

- Use the Oracle 10.2g JDBC 4 drivers. The drivers work with oracle 9, 10 and 11.
- If you are using the Oracle 11g drivers, manually edit the `trc.properties` file and set the following property **oracle.increment.keys.off=1**.

Note: Restart the server service.

Errors when trying to connect to the Microsoft® SQL database in FIPS compliancy mode

Symptom

Errors when trying to connect to the Microsoft® SQL database in FIPS compliancy mode

Cause

Using the IBM® JRE and the IBM® JSSE provider and Websphere Application Server, which has been enabled for FIPS compliancy currently, does not work when using an MS SQL database.

Solution

These options only work with MS SQL when FIPS is **not** enabled in IBM® Websphere.

Chapter 16. Uninstall the components

After you install the various Remote Control components, you can uninstall them in various ways.

Uninstall the server

To remove the Remote Control server, the method you choose depends on the type of installation that was run. If you installed the server by using the Remote Control installation program, you can uninstall the software by using the installer or by using Add or Remove programs. If you ran a manual installation of BigFix® Remote Control Server, you must uninstall the software by using the IBM® WebSphere Application Server administration console.

Uninstalling the server by using the installer

Use the following procedure to uninstall the Remote Control server software if you are using a Windows® operating system or a Linux® operating system.

To uninstall the Remote Control server by using the installer, complete the following steps :

1. Navigate to the Remote Control server installation directory.
   The default directory or the specific directory that you chose when you installed the server. For example,

   Windows® systems

   ```
   \Program Files\BigFix\TRC\server
   ```

   Linux® systems

   ```
   /opt/BigFix/Tivoli/TRC/server
   ```

2. Double click **Uninstall Remote Control - Server.exe**
3. Click **Uninstall**.
4. Click **Done** when finished.

The Remote Control features, files, and folders that were created by the installer are removed.

Uninstalling the server application in IBM® Websphere Application Server

If you have performed a manual installation of the BigFix® Remote Control Server software, you can uninstall the software using the IBM® Websphere Application Server administration console by completing the following steps:

To access the Administrative Console complete the following steps:

1. In your browser type

   ```
   https://[server : port]/ibm/console
   ```

where *server* is the ipaddress or name for the application server machine for example localhost or 192.0.2.0 and *port* is the port that the server is listening on.

2. Logon with the ID and password that were defined when installing Websphere.
3. Expand Applications and click **Enterprise applications**.
4. Select the check box for the Remote Control server application.
5. Click **Uninstall**.
6. Select **Save** to save to the Master Configuration.

Uninstalling the server using Add or Remove programs

If you are using a Windows® operating system you can uninstall the server software, using Add or Remove Programs by completing the following steps :

1. Open the **Control Panel**.
2. Double click **Add or Remove Programs**.
3. Select **Remote Control - Server**.
4. Click **Change Remove**.
5. Click **Uninstall**.
6. Click **Done** when finished.

Uninstalling the target on Windows™ systems

Using **Add or Remove Programs** to remove the target software from a Windows™ system.

To remove the target software by using Add or Remove Programs complete the following steps:

1. Open the **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Select **IBM Remote Control - Target**.
4. Click **Remove**.
5. Click **Yes** at the prompt.

The Remote Control target software is removed from your system.

Uninstalling the target on Linux® systems

To remove the target software on Linux® systems, complete the following steps:

1. To find the Remote Control package name that is installed, run the following command.

```
rpm  -qa  |grep  trc
```

2. Run the following command:

```
rpm  -e <trcpackage>
```

where *trcpackage* is your package name.

```
For example: rpm -e trc-target
```

You can verify that the target is removed by completing the following steps:

1. Run the command in step 1 *(on page 170)* to make sure that there is no Remote Control package installed.
2. Run the following command to make sure that no Remote Control process is running.

```
ps  -ef  |grep  trc
```

Chapter 17. Upgrade from previous versions

When upgrading Remote Control from version 9.x to version 10 for the first time, there is no specific component upgrade order to follow.

When upgrading the Server, the installer will detect that an earlier version of the server is present, and that server instance is upgraded to version 10.

When upgrading the Target, Broker, Gateway and Controller the upgrade process consists of:

- Installing the version 10 component
- Migrating the component configuration
- Uninstalling the earlier version of the component

If you are upgrading from a version of Remote Control older than 9.0.0 may lead to compatibility issues if the different components are not upgraded in the correct order.

This limitation applies only to environments where the gateway and broker components are deployed. In these environments, the broker and gateway must be updated before the server or the target components. After they are upgraded, the targets and server can be upgraded in the order that best suits your environment, since there are no dependencies between them.

Upgrade to Version 10 from earlier versions

When upgrading the Server, the installer will detect that an earlier version of the server is present, and that server instance is upgraded to version 10. The existing database does not need to be migrated and the configuration settings can be preserved.

Upgrade process

When upgrading the Target, Broker, Gateway and Controller the upgrade process consist of:

- Install the version 10 component.
- Migrate the component configuration.
- Uninstall the earlier version of the component.

Note: During the upgrade process the broker certificate is not relocated. After the broker upgrade verify that the CertificateFile parameters in the broker configuration are accurate.

Upgrade the gateway component

You can upgrade the gateway component by using any of the following methods:

Using the installation files

For more information about obtaining the component installation files, see Obtain the installation files *(on page 29)*. For more information about installing the gateway support on a Windows system, by using the installation files, see Installing Windows gateway support *(on page 93)*. For more information about installing the gateway support in Linux, by using the installation files, see Installing Linux gateway support *(on page 94)*.

Using the BigFix® console

If you have the BigFix® console infrastructure installed, you can use the update fixlet to upgrade the gateway support. For more information about the upgrade fixlet, see the *BigFix® Remote Control Console User's Guide*.

Upgrade the broker component

You can upgrade the broker support by using any of the following methods:

Using the installation files

For more information about obtaining the component installation files, see Obtain the installation files *(on page 29)*. For more information about installing the broker support on a Windows™ system, by using the installation files, see Installing Windows broker support *(on page 95)*. For more information about installing the broker support in Linux™, by using the installation files, see Installing Linux broker support *(on page 95)*.

Using the BigFix® console

If you have the BigFix® console infrastructure installed, you can use the update fixlet to upgrade the broker support. For more information about the upgrade fixlet, see the *BigFix® Remote Control Console User's Guide*.

Note: The upgrade process from version 9.x, it's important to note that the broker certificate is not relocated. After the broker upgrade, it is crucial to verify the accuracy of the `CertificateFile parameters` in the broker configuration.

Note: The upgrade process to version 10.1.0 may overwrite the existing `trc_broker.properties` file. Make a backup copy of the *trc_broker.properties* file before proceeding with the upgrade. After the upgrade review your current broker configuration and remove any existing `DefaultTLSCipherList`, `DefaultHTTPSCipherList`, and `ServerTLS*` properties to ensure that the Broker operates with version 10.1.0 hardened configuration.

Upgrade the server component

If you already installed the BigFix® Remote Control Server software, you can upgrade the component by carrying out a similar installation type to your original installation.

Note about backup/restore database: Although SQL databases are robust products, database corruption can still occur, and so performing a backup is a fundamental task for any database administrator or developer, and it is a good practice to perform periodic database backups before any major change. For example, if we are talking about an MS SQL database, which is the most common, the backup/restore database can be done either through the graphical interface of SQL Server Management Studio / SSMS (easiest method) or using Transact-SQL (T-SQL) commands. However, database maintenance activities are usually out of scope of BigFix Remote Control administration, so please refer to the official and specific database documentation for details about the suggested procedures.

Before you start the upgrade, you must back up your property files and any recording files if applicable. Back up any certificates, if applicable. For more information about backing up and restoring certificates, see the *BigFix® Remote Control Administrator's Guide*

Property files

- `common.properties`
- `ldap.properties`
- `trc.properties`
- `log4j2.properties`
- `controller.properties`

The files are in the following directories.

Windows® systems

`[InstallDir]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes\` Where *InstallDir* is the Remote Control server installation directory. For example, `C:\Program Files ( x86)\BigFix\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes\`

Linux® systems

`[InstallDir]wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes/` Where *InstallDir* is the Remote Control server installation directory.

Recordings Files

The video recordings folder is defined by the **rc.recording.directory** property in the **trc.properties** file.

You can upgrade the server component by using any of the following methods:

Using the installation files

For more information about obtaining the component installation files, see Obtain the installation files *(on page 29)*. For information about installing the server, by using the installer, see Installing by using the server installer *(on page 36)*.

Note: During the installation, select to keep existing property files and do not select to drop the database.

For information about installing the server, on WebSphere 8.5, see Installing on WebSphere Application Server version 8.5.5: deploying the war file *(on page 44)*.

Using the BigFix® console

If you have the BigFix® console infrastructure installed, do not run this wizard for the upgrade activity.

Upgrade the target component

You can upgrade the target component by using any of the following methods:

Using the installation files

For more information about obtaining the component installation files, see Obtain the installation files *(on page 29)*. For more information about installing the target component on a Windows™ system, by using the installation files, see Installing the Windows target *(on page 55)*. For more information about installing the target component on a Linux™ system, by using the installation files, see Installing the Linux target *(on page 76)*.

Using the BigFix® console

If you have the BigFix® console infrastructure installed. you can use the update fixlet to upgrade the target component. For more information about the upgrade fixlet, see the *BigFix® Remote Control Console User's Guide*.

Upgrade the controller component

The controller component upgrade is a major upgrade. Any existing properties are backed up and added to the new properties file.

If you are using a Linux™ operating system and are upgrading from IBM® Endpoint Manager for Remote Control version 9.0.1 or earlier, edit the `trc_controller.cfg.rpmnew` file. Compare the property values in the file with the values in the `trc_controller.cfg` file. Merge the differences into the `trc_controller.cfg` file and save the file.

Any of the following methods can be used to upgrade the controller component:

Using the installation files

For more information about obtaining the component installation files, see Obtain the installation files *(on page 29)*. For more information about installing the controller component on a Windows™ system, by using the installation files, see Installing the controller on a Windows system *(on page 84)*. For more information about installing the controller component in a Linux™ system, by using the installation files, see Installing the Linux controller *(on page 85)*.

Using the BigFix® console

If you have the BigFix® console infrastructure installed, you can use the update fixlet to upgrade the controller component. For more information about using the update fixlet, see the *BigFix® Remote Control Console User's Guide*.

Chapter 18. Maintaining the target installation

The BigFix® Remote Control Target installation can be modified by using a maintenance program.

You can access the maintenance program on a system with Microsoft® Windows® by running the `trc_target_setup.exe` program. To access the maintenance program, complete the following steps:

1. Go to the target installation directory. For example, `\Program Files\BigFix\Remote Control\RCTarget`
2. Double-click `trc_target_setup.exe`.
3. At the welcome screen click **Next**.
4. Select an option and click **Next**

   Modify

   Select this option to go through the target installation screens to modify the previously installed values.

   To modify the installation properties, follow from step 5 *(on page 56)*.

   Repair

   Select this option to fix missing or corrupted files, shortcuts, and registry entries.

   a. Click **Repair**.
   b. Click **Finish**.

   Remove

   Select this option to remove the target software and all of its features.

   a. Click **Remove**.
   b. Click **Finish**.

Appendix A. Properties that can be set in the target configuration

You can configure target properties either during or after installation. The operating system on the target system determines which properties can be configured. The target properties determine the actions that can be carried out during a peer-to-peer session. If you set a server URL and set the **Managed** property to Yes, the actions are determined by the policies that are set on the Remote Control server.

For more information about which properties are configurable in each operating system, see Table 22: Operating systems that the property is configurable in *(on page 200)*.

Windows™ systems

The target properties are saved in the target registry. Edit the target registry to modify the properties:

1. On a 64-bit system, all the 32-bit registry keys are under the **Wow6432Node** key. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`

   Note: On a 32-bit system, go to `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`

2. Right-click the required property and select **Modify**
3. Set the required value and click **OK**.
4. Restart the target service.

Linux™ systems

The target properties are saved to the `/etc/trc_target.properties` file. Edit the file after installation to configure the target.

1. Edit the `trc_target.properties` file.
2. Modify the required properties.
3. Save the file.
4. Restart the target service.

macOS devices

You can configure the properties in the `trc_target.cfg` file when you install the target. For more information, see Installing the BigFix Remote Control Target for macOS by using the .pkg file *(on page 77)*. The target properties are saved to `/Library/Preferences/com.bigfix.remotecontrol.target.plist`. To modify a target property, complete the following steps:

1. Open the `Terminal.app`.
2. To modify a property, enter the following command.

sudo defaults write /Library/Preferences/com.bigfix.remotecontrol.target.plist **Keyword Value**

Where **Keyword** is the property name and **Value** is the value for the property. For example,

sudo defaults write /Library/Preferences/com.bigfix.remotecontrol.target.plist LogLevel 4

3. Restart the target.
   - For BigFix Remote Control version 10 update 6 or earlier
     a. Click **Remote Control Target > Quit Remote Control Target**
     b. Open the `Remote Control Target` app
   - For BigFix Remote Control version 10 update 7
     a. Enter `sudo launchctl unload /Library/LaunchDaemons/RCTargetDaemon.plist`
     b. Enter `sudo launchctl load /Library/LaunchDaemons/RCTargetDaemon.plist`

Target property definitions

Table 18. Installation option descriptions

Target property	Default Value	Description
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 yourRemote Control server. For example, `http://trcserver.example.com/trc` **Note:** If you provide a server URL and you want the target to take part only in remote control sessions that are started from the server, set **AllowP2P** to No.
ProxyURL	Blank	Host name or IP address for a proxy server, if you are using one.
BrokerList	Blank	The list of host names or IP addresses of the brokers and their ports, that you want the target to connect to. In the format, **hostname1:port,hostname2:port,hostname3:port.**
GroupLabel	Blank	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** property in the `trc.properties` file on

Table 18. Installation option descriptions (continued)

Target property	Default Value	Description
		the server must be set to Yes for the **GroupLabel** property value to be applied. **Note:** • The **allow.target.group.override** property in the `trc.properties` file on the server must be set to Yes for the **GroupLabel** property value to be applied when the target is not already registered with the server. • The **allow.override.at.triggered.callhomes** property in the `trc.properties` file on the server must be set to Yes for the **GroupLabel** property value to be applied when the target performs periodic callhomes after the target has registered with the server. • You can specify a single target group name or a list of target groups with a semicolon separator in the format **Group1;Group2**.
PortToListen	888	Specify the TCP port that the target listens on. The default value for the BigFix® Remote Control Target for macOS is 8787.
AllowP2P	Yes	Used to enable peer-to-peer mode. Use this parameter to enable peer to peer connections regardless of the server status. Default value is No **No** 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. **Yes** A peer-to-peer session can be established between a controller user and this target. **Note:** If this option is Yes and a server URL is provided, the target can take part in both peer-to-peer sessions and sessions that are initiated from the server.

Table 18. Installation option descriptions (continued)

Target property	Default Value	Description
AllowP2PFailover	No	Use this parameter to enable failover to peer-to-peer mode when the server is down or unreachable. **AllowP2P** must also be set to *Yes*. Default value is *No*. **No** The session does not failover to peer-to-peer mode when the server is down or unreachable. **Yes** The session does failover to peer-to-peer mode when the server is down or unreachable.
FIPSCompliance	No	Use this property to enable the use of a FIPS-certified cryptographic provider for all cryptographic functions. For more information about enabling FIPS compliance, seeFederal information processing standard (FIPS) compliance in Remote Control *(on page 139)*. **Note:** If you enable FIPS compliance on the target, you must 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. 1. 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**

Table 18. Installation option descriptions (continued)

Target property	Default Value	Description
		`opt/BigFix/trc/controller/trc_controller.cfg` 2. Set the **fips.compliance** property to Yes and save the file.
SP800131ACompliance	No	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 NIST SP800-131A compliance in Remote Control *(on page 148)*. **Note:** If you enable NIST SP800-131A compliance on the target, you must 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. 1. 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` 2. Set the **sp800131A.compliance** property to Yes and save the file.
Accessibility	No	Select this option to enable the accessibility UI. Available only on **Windows** operating system.

Table 18. Installation option descriptions (continued)

Target property	Default Value	Description
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.
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. **Daily** Start a new log file every day.
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**

Table 18. Installation option descriptions (continued)

Target property	Default Value	Description
		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 19. Session option properties.

Target property	Default Value	Description
AllowMonitor	Yes	Determines whether the target can take part in monitor peer-to-peer sessions. For information about the different types of remote control session that can be established, see the *BigFix® Remote Control Controller User's Guide*. **Yes** 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. **No** 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.
AllowGuidance	Yes	Determines whether the target can take part in guidance peer-to-peer sessions. **Yes** The target can take part in guidance peer-to-peer sessions. The **Guidance** option is available in the session

Table 19. Session option properties. (continued)

Target property	Default Value	Description
		type list in the controller window. The **Open connection** window also lists a **Guidance** option. **No** 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.
AllowActive	Yes	Determines whether the target can take part in active peer-to-peer sessions. **Yes** 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 contains an **Active** option. **No** 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.
DisableChat	No	Determines the ability to start a chat session with the target and also chat to the controller user during a peer-to-peer session. **Yes** 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. **No** A **Chat Only** session can be initiated from the open connection window. During the session, the chat icon is available in the controller window.
DisableFilePull	No	Determines the ability to transfer files from the target to the controller during the session. **Yes** Files cannot be transferred from the target to the controller. **No**

Table 19. Session option properties. (continued)

Target property	Default Value	Description
		Files can be transferred from the target to the controller.
DisableFilePush	No	Determines the ability to transfer files from the controller to the target during the session. **Yes** Files cannot be transferred from the controller to the target. **No** Files can be transferred from the controller to the target.
DisableClipboard	No	Determines the availability of the clipboard transfer menu in the controller UI in a peer-to-peer session. Use the menu to transfer the clipboard content between the controller and target during a remote control session. **Yes** The clipboard transfer menu is not available during the session to transfer the clipboard content to and from the target. **No** The clipboard transfer menu is available during the session.
AllowRecording	Yes	The controller user can make and save a local recording of the session in the controlling system. **Yes** The record option is available in the controller window. **No** The record option is not available in the controller window.
AllowCollaboration	Yes	Use this property to allow more than one controller to join a session. Determines the availability of the collaboration icon on the controller window. **Yes** The collaboration icon is available in the controller window. **No**

Table 19. Session option properties. (continued)

Target property	Default Value	Description
		The collaboration icon is not available in the controller window.
AllowHandover	Yes	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. **Yes** The **Handover** button is displayed in the collaboration control panel. **No** The **Handover** button is not displayed in the collaboration control panel.
AllowForceDisconnect	No	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. **Yes** The disconnect button is displayed in the message window. **No** The disconnect button is not displayed in the message window.
ForceDisconnectTimeout	45	Number of seconds you must wait for the controller user 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.
AutoWinLogon	Yes	Determines whether a session can be started when no users are logged on at the target. **Yes** Session is started with the target. **No** Session is not started and the following message is displayed. `Session rejected because there is no user logged to confirm the session`

Table 19. Session option properties. (continued)

Target property	Default Value	Description
RunPreScript	No	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**. **Yes** When a remote control session is requested, the defined script is run before the controller user has access to the target. **No** 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*.
RunPostScript	No	Determines whether a user-defined script is run after the remote control session finishes. **Yes** When a remote control session ends, the user-defined script is run. **No** 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*.
ProceedOnScriptFail	No	The cction 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. **Yes** If the pre-script or post-script run fails, the session continues. **No** If the pre-script or post-script run fails, the session does not continue and ends.
WorkaroundW2K3RDP	No	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 sys-

Table 19. Session option properties. (continued)

Target property	Default Value	Description
		tem 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 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 Yes. **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 a blank desktop is displayed on the controller 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.
EnableTrueColor	No	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**. **Yes.** The target desktop is displayed in true color 24-bit mode at the start of the session. Partial screen updates are also enabled. **No.** 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.

Table 19. Session option properties. (continued)

Target property	Default Value	Description
LockColorDepth	No	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**. **Yes.** 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. **No.** The color quality can be changed during the session. The **Performance settings** icon is enabled in the controller window.
RemoveBackground	No	If a desktop background image is set on the target, this property can be used to remove the background from view during a remote control session. **Yes.** The desktop background image on the target is not visible during a remote control session. **No.** The desktop background image on the target is visible during a remote control session.
NoScreenSaver	No	Stops the target from sending screen updates when it detects that the screen saver is active. **Yes.** While the screen saver is active on the target system, the target stops transmitting screen updates. The controller displays a simulated screen saver so that the controller user is aware that a screen saver is active on the remote display. The controller user can remove the screen saver by pressing a key or moving the mouse. **No.** A simulated screen saver is not displayed in the session window. The target screen is displayed as normal and the target continues to transmit screen updates.

Table 19. Session option properties. (continued)

Target property	Default Value	Description
Managed	Yes	Determines whether the target registers with the Remote Control server. **Yes.** The target registers with the Remote Control server and periodically contacts the server. **No.** The target does not register with the Remote Control server. The target can take part only in peer-to-peer sessions.

Table 20. User acceptance property descriptions

Target property	Default Value	Description
ConfirmTakeOver	Yes	Determines whether the acceptance window is displayed on the target, when a remote control session is requested. **Yes** The user acceptance window is displayed and the target user can accept or refuse the session. **No** The user acceptance window is not displayed and the session is established.
ConfirmModeChange	Yes	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. **Yes** The user acceptance window is displayed each time a session mode change is requested and the target user must accept or refuse the request. **No** The user acceptance window is not displayed and the session mode is changed automatically.
ConfirmFileTransfer	Yes	Determines whether the user acceptance window is displayed when the controller user selects to transfer files between the target and the controller. **Yes** The acceptance window is displayed in the following two cases. The target user must accept or refuse the file transfer.

Table 20. User acceptance property descriptions (continued)

Target property	Default Value	Description
		• 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. **No** The acceptance window is not displayed and files are transferred automatically from the target to the controller system when requested.
ConfirmSysInfo	Yes	Determines whether the user acceptance window is displayed when the controller user requests to view the target system information. **Yes** 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. **No** The target system information is displayed automatically when the controller user clicks the system information icon.
ConfirmRecording	Yes	Determines whether the user acceptance window is displayed when the controller user clicks the record icon on the controller window. **Yes** 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. **No**

Table 20. User acceptance property descriptions (continued)

Target property	Default Value	Description
		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.
ConfirmCollaboration	Yes	Determines whether the user acceptance window is displayed when another controller user requests to join a collaboration session with a target. **Yes** 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. **No** The additional controller automatically joins the collaboration session when they try to connect to the master controller of the session.
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 Yes, **Acceptance grace time** must be set to a value >0 to provide the target user with enough time to respond.
AcceptanceProceed	No	The 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**. **Yes** Session is established. **No** Session is not established.

Table 20. User acceptance property descriptions (continued)

Target property	Default Value	Description
HideWindows (Deprecated)	No	**Note:** The "Allow to show/hide selected windows during the session" feature has been deprecated for all versions above Windows 10. Determines whether the **Hide windows** check box is displayed on the user acceptance window when **Confirm incoming connections** is also set to Yes. **Yes** The **Hide windows** check box is displayed on the user acceptance window. **No** The **Hide windows** check box is not visible on the user acceptance window.
DisableGUI_CLI	No	Lets the user to send actions to the target through command line. **Yes** The GUI command line interface is disabled. **No** The GUIcommand line interface is enabled. **Note:** The command line interface is only available in managed mode and when the BrokerList property is not empty.

Table 21. Security property descriptions

Target property	Default Value	Description
CheckUserLogin	Yes	Determines whether a logon window is displayed when the controller user clicks a session type button 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 session is established.
CheckUserGroup	see description	Default value.

Table 21. Security property descriptions (continued)

Target property	Default Value	Description

		Windows™ systems
		`BUILTIN\Administrators`
		Linux™ systems
		`wheel`
		When **CheckUserGroup** 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.
		1. To also grant administrator rights to the users, make them members of the Administrators group on Windows™ systems or the wheel group on Linux™ systems.
		2. For users with no administrator rights, complete the following steps.
		a. Create a group or use an existing group. For example, the following command can be run as root:
		`groupadd trcusers`
		.
		b. 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>`
		c. Add the group to the list in the **Authorized user group** field.

AuditToSystem	Yes	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.

Table 21. Security property descriptions (continued)

Target property	Default Value	Description
		Yes Entries that correspond to each action that is carried out during the session, are logged in the application event log of the target. **No** No entries are logged to the application event log.
AutoSaveChat	No	Determines whether the chat text, entered during a chat session, can be saved. **Yes** 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 machine 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/`. On Mac systems, the file is saved to `/Users/<user>/Library/Application Support/com.bigfix.remotecontrol-.target`. **No** The chat text is not saved to a file.
EnableFileTransferSystemAccess	No	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. **Yes** The file transfer session uses System privileges (Windows) or root privileges (Linux) on the target file system. **No**

Table 21. Security property descriptions (continued)

Target property	Default Value	Description
		The file transfer session uses the privileges of the logged on user on the target file system. **Note:** If the option is set to No, and there is no logged on user on the target during the file transfer session, an error message is displayed.
SessionDisconnect	No	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.
AllowPrivacy	Yes	Determines whether a controller user can lock the local input and screen of the target in a remote control session. Determines the visibility of the **Enable Privacy** option on the controller window. **Yes** The **Enable Privacy** option is available in the **Perform Action in target** menu in the controller window. **No** The **Enable Privacy** option is not available in the **Perform Action in target** menu in the controller window.
AllowInputLock	Yes	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. **Yes** 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. **No** The lock target input menu item is not enabled in the **Perform action in target** menu in the controller window.

Table 21. Security property descriptions (continued)

Target property	Default Value	Description
		Note: If the option to **Enable Privacy** is Yes during a session, the remote user input is automatically locked. It is not possible to enable privacy without also locking the input.
EnablePrivacy	No	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. **Yes** 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. **No** The target screen is not blanked out when the session is started and the target user can interact with the screen.
EnableInputLock	No	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, during a remote control session. **Yes** The target screen is visible to the target user during the session, while in privacy mode but the mouse and keyboard control is locked. **No** 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. **Note: Enable privacy** must be Yes for **Enable input lock** to take effect.
DisablePanicKey	No	Determines whether the Pause Break key can be used by the target user to automatically end the remote control session. **Yes**

Table 21. Security property descriptions (continued)

Target property	Default Value	Description
		The target user cannot use the Pause Break key to automatically end the remote control session. **No** The target user can use the Pause Break key to automatically end the remote control session.
EnableOSSN	No	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. **Yes** 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. The user is still able to interact with their screen. **No** No overlay is displayed on the target computer. **Note:** This policy is only supported on targets where a Windows™ operating system installed.
DisableGUI	No	Determines whether the target UI is visible 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. **Yes** The target UI 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. **No**

Table 21. Security property descriptions (continued)

Target property	Default Value	Description
		The target UI is displayed on the target as the session is starting and is available to the target user during the remote control session.

Operating systems that the property is configurable in

Table 22. Operating systems that the property is configurable in

Property name	Windows™	Linux™	macOS
ServerURL	*	*	**
ProxyURL	*	*	**
BrokerList	*	*	*
GroupLabel	*	*	**
PortToListen	*	*	*
AllowP2P	*	*	*
AllowP2PFailover	*	*	**
FIPSCompliance	*	*	
SP800131ACompliance	*	*	
Accessibility	*		
LogLevel	*	*	*
LogRollover	*	*	*
LogRotation	*	*	*
AllowMonitor	*	*	*
AllowGuidance	*	*	*
AllowActive	*	*	*
DisableChat	*	*	*
DisableFilePull	*	*	*
DisableFilePush	*	*	*
DisableClipboard	*	*	
AllowRecording	*	*	*
AllowCollaboration	*	*	*

Table 22. Operating systems that the property is configurable in (continued)

Property name	Windows™	Linux™	macOS
AllowHandover	*	*	*
AllowForceDisconnect	*	*	
ForceDisconnectTimeout	*	*	
AutoWinLogon	*	*	**
RunPreScript	*	*	
RunPostScript	*	*	
ProceedOnScriptFail	*	*	
WorkaroundW2K3RDP	*		
EnableTrueColor	*	*	*
LockColorDepth	*	*	*
RemoveBackground	*		
NoScreenSaver	*		
Managed	*	*	**
ConfirmTakeOver	*	*	*
ConfirmModeChange	*	*	*
ConfirmFileTransfer	*	*	*
ConfirmSysInfo	*	*	*
ConfirmRecording	*	*	*
ConfirmCollaboration	*	*	*
AcceptanceGraceTime	*	*	*
AcceptanceProceed	*	*	*
HideWindows	*	*	
CheckUserLogin	*	*	
CheckUserGroup	*	*	
AuditToSystem	*	*	*
AutoSaveChat	*	*	*
EnableFileTransferSystemAccess	*	*	**
SessionDisconnect	*	*	

Table 22. Operating systems that the property is configurable in (continued)

Property name	Windows™	Linux™	macOS
AllowPrivacy	*		
AllowInputLock	*		
EnablePrivacy	*		
EnableInputLock	*		
DisablePanicKey	*		
EnableOSSN	*		
DisableGUI	*		**
DisableGUI_CLI	*	*	**

Note: ** Property supported starting from macOS Remote Control target V10 Update 7.

Appendix B. AV Exclusions on Windows, Linux and MAC

This topic provides guidance on configuring anti-virus (AV) and intrusion detection system (IDS) exclusions for BigFix Remote Control on Windows, Linux, and Mac platforms. It details the specific directories and processes that should be excluded to prevent interruptions or failures during remote control sessions. Proper configuration helps ensure reliable operation and avoids common errors related to AV or IDS interference.

Remote Control AV Exclusions

BigFix Remote Control Target activity may be interrupted or “shimmed” by anti-viruses or Intrusion Detection Systems (IDS). Sometimes, it may result in failures when establishing the remote control session. To address this issue, you need configure the Anti-viruses and IDS's to exclude the following directories and processes.

Note: The specifications mentioned in this topic are related to the exclusion of folders paths and processes for real-time scans and heuristics.

Remember: Ensure that the scheduled scans are configured and enabled from a security perspective.

The following folders and sub-folder paths should be excluded:

Note: The `<user>` folder may contain the audit logs. Specify each sub folder to be scanned (for example: Documents), except for the `.trc` folder.

Windows™

- `%DRIVE%:\ProgramData\BigFix\Remote Control\*`
- `%DRIVE%:\Program Files (x86)\BigFix\*`
- `%DRIVE%:\Program Files\BigFix\*`
- `%DRIVE%:\Users\<user>\`
- `%DRIVE%:\Users\<user>\.trc\*`

Linux™

- `%DRIVE%:/var/opt/bigfix/trc/*`
- `%DRIVE%:/var/opt/bigfix/trc/target/*`
- `%DRIVE%:/opt/bigfix/trc/target/*`
- `%DRIVE%:/opt/BigFix/*`
- `%DRIVE%:/home/<user>/`

MAC™

- `%DRIVE%: /Library/Application Support/com.bigfix.remotecontrol.target/*`
- `%DRIVE%:/Library/LaunchDaemons/`

- `%DRIVE%:/Applications/Remote Control Target.app/*`
- `%DRIVE%:/Applications/Remote Control Target.app/*`
- `%DRIVE%:/Users/<user>/Library/Application Support/com.bigfix.remotecontrol.target/*`
- `%DRIVE%:/Users/<user>/File Transfer/*`
- `%DRIVE%:/Users/<user>/*`

Additionally, the following processes should be excluded:

Note: The Remote Control processes use some ports to communicate among each other (locally). The port is chosen dynamically from the OS in the following ranges:

- On Windows Vista and later: a value between `49152` and `65535`
- On Windows Server 2003 and earlier: a value between `1025` and `5000`

For more information, refer to bind function (winsock.h).

Windows™

- `%DRIVE%:\Program Files (x86)\BigFix\Remote Control\Target\trc_base.exe`
- `%DRIVE%:\Program Files (x86)\BigFix\Remote Control\Target\trc_gui.exe`
- `%DRIVE%:\Program Files (x86)\BigFix\Remote Control\Target\trc_dsp.exe`
- `%DRIVE%:\Program Files\BigFix\Remote Control\Target\trc_base.exe`
- `%DRIVE%:\Program Files\BigFix\Remote Control\Target\trc_gui.exe`
- `%DRIVE%:\Program Files\BigFix\Remote Control\Target\trc_dsp.exe`

Linux™

- `/opt/bigfix/trc/target/trc_base`
- `/opt/bigfix/trc/target/trc_dsp`
- `/opt/bigfix/trc/target/trc_ft`
- `/opt/bigfix/trc/target/trc_gui`

MAC™

- `/Applications/Remote Control Target.app/Contents/MacOS/trc_base`
- `/Applications/Remote Control Target.app/Contents/MacOS/trc_ft`
- `/Applications/Remote Control Target.app/Contents/MacOS/trc_gui.app/Contents/MacOS/trc_gui`
- `/Applications/Remote Control Target.app/Contents/MacOS/trc_dsp.app/Contents/MacOS/trc_dsp`

More Information

The controller may show the gray screen or the following error message:

```
BigFix Remote Control is unable to control this target system because the display capture process failed to start
```

Also, the target log `C:\ProgramData\BigFix\Remote Control\trc_base.log` may show the following error:

```
2019.02.20-07:24:31.553 (GMT) ERROR [ 5012] GUI process didn't connect on time. Killing it
2019.02.20-07:24:31.553 (GMT) ERROR [ 5012] ERROR -19 starting GUI process
```

Appendix C. Support

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

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

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Index

A

add a token for secure target registration 100

application
- deployment 54

application server setup
- DB2 45
- mssql 51
- oracle 48

av exclusions
- linux 203
- windows 203

B

broker
- upgrading 173

broker requirements 26

broker support
- installing 95

C

command line tools
- installing
  - linux 92
  - windows 90

command-line tools
- installing 90

components
- installing 29

configuration
- server
  - enabling email 111

Configuring Microsoft Entra ID connection credentials 133

controller
- for mac
  - fixlet 86
  - pkg file 86
- installation
  - supported operating systems 87
- installing 84
  - linux 85
  - Windows 84
- pre-configuring 87
- upgrading 175

controller requirements 23

custom install
- target 78

D

data import
- LDAP 112
- Microsoft Entra ID 130

data source
- DB2
  - creating 47

MSSQL
creating
52
Oracle
creating
50
database
mssql
creating
35
mssql database
permissions
35
database authentication data
DB2
45
MSSQL
51
Oracle
48
database setup
DB2
30
oracle
31
default installation
server
36
deploying the war file
44
E
email
enabling
111
Enabling SP800-131A compliance on the CLI tools
158
environment guidelines
server
18
F
FIPS compliance
139
at target installation
145
linux target
enabling
146
server
enabling
139
target
after installation
146
target silent install
145
FIPS compliancy
controller
enabling
144
enabling on server
automated server installation
140
manual server installation
140
target
enabling
145
windows target
enabling
145
G
gateway
upgrading
172
gateway support
installing
93
linux
94
silent install
94
windows
93
getting started

28

I

installation
basic setup
13
firewall traversal
14
verifying
159
installation errors
DB2
161, 165
during installation
160
linux libstdc++.so.5 package
162
not enough memory
160
oracle
161
post installation
162
DB2 authentication failure
164
out of memory
163
welcome page not appearing
165
recovering
160
installation files
extracting to disk
97, 98
obtaining
29
installing
controller
84
target
55
target rpm file
76
Installing
server
29
installing a pre-configured controller component
87
installing broker support
95
Linux
95
Windows
95
installing gateway support
93
installing linux gateway support
94
installing the command-line tools
90
Installing the components
29
installing the Linux controller
85
Installing the Windows controller
84
Installing the Windows target
55
installing Windows gateway support
93

J

jdbc provider
MSSQL
creating
51
Oracle
creating
49

L

LDAP
configuration file
124
configuring
112
connection credentials

115
connection security
parameters
116
enabling
123
errors
123
groups
importing
121
ldap.security_athentication
116
SASL secure connection
116
SSL secure connection
117
synchronization
112
user authentication
118, 118
user search
120
verify imported groups
124
verifying a connection
114
linux components
restarting
109
starting
109
stopping
109
log files
location
160

M

MAC
203
mac controller
fixlet
86
installation
86, 86, 86
pkg file
86
mac target
deployment
fixlet
76
installation
76, 77
pkg file
77
managing the component services
109
manual install
application deployment
54
application server setup
45
database setup
30
Microsoft Entra ID
configuration file
136
configuring
130
connection credentials
133
enabling
135
errors
135
groups
importing
134
migrating from LDAP
135
synchronization
130
user authentication
133, 133

user search
134
verify imported groups
135
verifying a connection
132
MSSQL
FIPS compliancy
connection errors
168
mssql database
creating
35
N
NIST compliance
148
broker
enabling
158
cli
enabling
158
enabling
automated server installation
150
manual server installation
149
gateway
enabling
157
linux target
enabling
157
server
enabling
148
target
enabling
156
using the server installer
149
O
Obtaining the installation files
29
operating requirements
12
oracle database
out of bounds errors
167
Oracle database
creating
31
setting permissions
32
Overview
10
P
platform support
broker
26
controller
23
server
16
target
24
R
registration token
add after target installation
102
Linux target
adding
103
silent installation option
101
target installer option
101
target upgrade
102
Windows target
adding
101
requirements
12

S
secure target registration
enabling
99
rc.enforce.secure.registration
99
server
99
server installer
99
server environment guidelines
18
large environment
21
medium environment
20
small environment
19
server installation
BigFix
console
55
installer
36
war file
44
server installation types
18
server requirements
16
Setting up LDAP synchronization
112
Setting up Microsoft Entra ID synchronization
130
smart card
driver installation
104
target installer option
104
smart card reader driver
add by using the installer
104
Fixlet installation
106
remove by using the installer
104
silent installation
105
target upgrade
106
smartcard
certificate
installation Fixlet
107
certificates
downloading
107
SP800-131A compliance
148
broker
enabling
158
cli
enabling
158
linux
158
windows
158
controller
enabling
155
stand-alone
155
enabling
automated server installation
150
manual server installation
149
gateway
enabling
157
linux target
enabling

157
server
enabling
148
target
after installation
156
enabling
156
target silent installation
156
using the server installer
149
using the target installer
156
windows target
enabling
156
system requirements
broker
26
controller
23
gateway
25
server
16
target
24

T

target
for mac
pkg file
77
installing
Windows
55
modifying
Windows
177
smart card driver
104
smart card installer option
104
smart card silent installer option
105
uninstalling
Linux
170
Windows
170
upgrading
175
target install
custom install
windows
78
target installation
rpm file
76
target installer
add registration token
102
add smart card reader driver
104
registration token option
101
remove smart card reader driver
104
target properties
configuring
178
definitions
178
target requirements
24
target silent installer
registration token option
101
targets
not registering
166
targets
not visible on server

166
troubleshooting
installation errors
160
U
uninstalling
169
server
169
in WAS
169
using add remove programs
170
using installer
169
upgrading
controller
175
server
173
target
175
upgrading from previous versions
172
upgrading the broker
173
upgrading the gateway
172
using this guide
12
V
Verifying Microsoft Entra ID connection
132
W
war file deployment
database setup
30
websphere variables
db2
verifying
46
oracle
verifying
49
verifying
52
windows components
restarting
109
starting
109
stopping
109