

# **Remote Control Administrator's Guide**



## Special notice

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

## Edition notice

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

# Contents

<b>Chapter 1. Overview of the Remote Control system.....</b>	<b>14</b>
<b>Chapter 2. Set a secure environment.....</b>	<b>16</b>
Configure the server URL.....	16
HTTPS URL is enabled by default during installation.....	16
Enabling HTTP access.....	17
Disable the HTTP port.....	17
Enforce an HTTPS logon.....	18
Secure communication configuration.....	19
Protocol configuration after a server upgrade.....	23
Signed certificate management.....	24
Installing a certificate.....	24
Backing up your certificate file.....	26
Setting password rules.....	27
Lock user accounts.....	31
Automatic passphrase encryption.....	34
Enforcing strict HTTPS validation of certificates.....	39
<b>Chapter 3. Secure target registration.....</b>	<b>40</b>
Tokens for secure authentication of targets.....	40
How targets securely authenticate with the server.....	41
<b>Chapter 4. Configure SAML 2.0 authentication on the server.....</b>	<b>42</b>
Configuring the server for single sign-on during installation.....	43
Configuring the server for single sign-on after installation.....	43
<b>Chapter 5. Access the server web interface.....</b>	<b>47</b>
Logging on to the server.....	47
Getting a temporary logon password .....	47
Setting up email.....	48
Logging off.....	48
<b>Chapter 6. Using the Deployment Status Dashboard.....</b>	<b>49</b>
<b>Chapter 7. Unattended Target Support.....</b>	<b>55</b>
Unattended targets guidelines.....	56

Operating requirements.....	56
Enable unattended target support.....	57
Start Unattended Target sessions.....	58
Manage the Unattended Target environment.....	60
Security Features for the Unattended Targets.....	62
The Controller Instance ID.....	63
The Controller UUID.....	63
Two Factor Authentication via Mail.....	64
<b>Chapter 8. Unlocking user accounts.....</b>	<b>65</b>
<b>Chapter 9. Manage targets and target groups.....</b>	<b>66</b>
Manage Targets.....	66
Deleting a target .....	66
Assign targets to target groups.....	67
Creating target groups.....	71
Viewing Target Groups.....	73
Manage Target Groups .....	73
Viewing the members of a target group.....	74
Deleting a target group.....	74
Changing the details for a target group.....	75
Remove members from a target group.....	75
Assigning target groups to other target groups.....	77
Set permissions for a target group.....	78
Searching for target groups.....	78
Cleanup non-reporting targets.....	78
<b>Chapter 10. Manage users and user groups.....</b>	<b>79</b>
User account authorities and the functions available to each account.....	79
Creating user accounts.....	80
Viewing user accounts.....	81
Manage user accounts.....	81
Setting user account privileges.....	81
Modifying user details.....	82
Removing users .....	83

Unlocking user accounts.....	84
Viewing a list of previous sessions established by a user .....	84
Searching for users.....	85
Creating user groups.....	86
Assign users to groups.....	87
Assigning a user to a group when you create the user.....	87
Assigning a user to user groups.....	87
Assigning multiple users to user groups.....	88
Viewing user groups.....	89
Manage user groups.....	89
Viewing the members of a user group.....	90
Deleting user groups.....	90
Changing the details for a user group.....	91
Remove members from a user group.....	92
Assigning user groups to other user groups.....	93
Setting permissions for a user group.....	94
Searching for user groups.....	94
<b>Chapter 11. Server session policies.....</b>	<b>95</b>
<b>Chapter 12. How session policies are determined.....</b>	<b>115</b>
Set the policies and permissions for a remote control session.....	115
Values assigned for standard or normal permissions .....	116
Assign a higher priority value to policies.....	117
Creating a permission link.....	117
Deleting a permission link.....	119
How permissions are derived.....	120
Permissions set examples.....	122
Example 1: Standard priority 0 permissions.....	125
Example 2: Higher priority permissions.....	127
Example 3: Only relationship permissions are inherited.....	129
Example 4: No overrides Yes when priority values are the same.....	131
Example 5: Higher priority Yes overrides lower priority No.....	133
In summary.....	135

<b>Chapter 13. Starting a managed session by using an installed controller .....</b>	<b>136</b>
<b>Chapter 14. Manage permission sets for temporary access to targets.....</b>	<b>137</b>
Creating a set of permissions .....	137
Viewing sets of permissions .....	138
Modifying a defined set of permissions .....	138
Deleting permission sets.....	139
<b>Chapter 15. Requests for temporary access to targets.....</b>	<b>140</b>
Handle a request for temporary access to targets.....	140
Give users temporary access to target systems.....	140
Revoking requests for temporary access to target systems.....	144
Denying requests for temporary access to target systems.....	144
Delete requests for temporary access to target systems.....	145
View requests for temporary access to target systems.....	146
Viewing outstanding access requests.....	146
Viewing live access requests.....	146
Viewing all access requests.....	146
<b>Chapter 16. Generate custom reports .....</b>	<b>147</b>
Create a Custom Report.....	147
Creating a report by sorting and filtering.....	148
Creating a report by editing the SQL statement.....	149
Create a report by using the Edit SQL feature.....	150
Creating a report by adding tables and columns.....	152
Running a custom report.....	153
Viewing custom reports.....	153
Manage custom reports.....	154
Editing a custom report by using the <b>Edit Custom Report and Access</b> feature.....	154
Removing your access to a report.....	155
Deleting custom reports.....	156
<b>Chapter 17. Manage the home page for a user or group.....</b>	<b>157</b>
Create and set a home page.....	157
Setting a default home page as a user.....	158
Setting a home page for a group.....	158

Viewing the default home page list.....	159
Editing the default home page for a group.....	159
Reset the default home page.....	159
Resetting the default home page for a user .....	160
Resetting the default home page for a group.....	160
<b>Chapter 18. Adding tables and columns to queries.....</b>	<b>161</b>
Adding a database table to a query.....	161
Adding a database column to a query.....	161
<b>Chapter 19. Configuration and troubleshooting options in the Admin menu.....</b>	<b>162</b>
Editing the properties file.....	162
Use the LDAP wizard.....	163
Configure LDAP by using the LDAP configuration utility.....	163
Testing your LDAP connection.....	163
Configure LDAP using Secure LDAP.....	164
Configuring LDAP group search parameters.....	165
Configuring LDAP user search parameters.....	166
Setting the page size of LDAP search retrievals.....	170
Saving your LDAP configuration.....	171
Viewing the application log.....	171
Saving the application log for exporting.....	171
Import data into the database.....	171
Viewing the server status.....	171
Viewing the remote control gateways.....	172
Editing a remote control gateway.....	172
Deleting a remote control gateway.....	172
Creating a remote control gateway.....	172
Resetting the Application.....	173
Configuring the user acceptance window.....	173
Configure the user acceptance window for a peer to peer session.....	176
Uploading user acceptance window icons.....	178
Creating a set of permissions that can be applied to a group.....	178
Viewing the permissions sets.....	179



Creating a secure registration token.....	179
Viewing the list of secure registration tokens.....	179
Deleting secure registration tokens.....	180
Use rules to define target membership.....	180
Define when membership rules are applied.....	180
Creating rules.....	182
Viewing rules.....	184
Checking rules.....	184
Editing rules.....	184
Deleting rules.....	185
<b>Chapter 20. Ensure targets are registered correctly .....</b>	<b>186</b>
Find a perfect or best match for a target.....	186
Match on computer name.....	187
Match on GUID .....	188
<b>Chapter 21. Record the session on the target.....</b>	<b>190</b>
<b>Chapter 22. Set up for exporting recordings.....</b>	<b>191</b>
Setting up a Windows server for exporting recordings.....	191
Setting up a Linux server for exporting recordings.....	191
<b>Chapter 23. Audit log distribution.....</b>	<b>193</b>
<b>Chapter 24. Access targets on different networks .....</b>	<b>194</b>
Configure the gateway support.....	194
Configuring inbound connections.....	195
Configuring gateway connections.....	196
Configuring endpoint connections.....	197
Configuring tunnel connections.....	198
Configuring the targets to use tunnel connections.....	200
Configure gateways in IPv6 networks.....	200
Gateway setup example.....	202
Track connection requests.....	206
Logging gateway activity.....	206
Configuration file example.....	207
<b>Chapter 25. Editing the properties files .....</b>	<b>215</b>

Template of field information.....	216
trc.properties.....	216
common.properties.....	268
ldap.properties.....	280
log4j2.properties.....	287
appversion.properties.....	293
controller.properties.....	293
OnDemand properties file.....	299
<b>Chapter 26. Reduce the volume of target connections to the server.....</b>	<b>306</b>
<b>Chapter 27. Broker configuration.....</b>	<b>308</b>
Configuring the broker properties .....	308
Setting server connection parameters.....	308
Configuring the broker certificate.....	309
Configuring inbound connections to brokers.....	309
Configuring broker connections.....	310
Logging broker activity.....	312
Configuring optional parameters.....	313
Default configuration parameters.....	315
Broker setup examples.....	320
<b>Chapter 28. Managing brokers.....</b>	<b>325</b>
Registering a broker.....	325
Viewing registered brokers.....	325
Editing broker details.....	326
Deleting a broker.....	326
<b>Chapter 29. Certificate management.....</b>	<b>327</b>
Creating a self signed certificate.....	327
Configuring the keystore on the broker.....	329
Strict Certificate Verification on Broker Connections.....	330
Extracting the certificate from the keystore.....	330
Creating Certificate Authority signed certificates.....	331
Truststore configuration.....	333
Adding a certificate to the truststore.....	333

Viewing certificates in the truststore.....	334
Editing a trusted certificate.....	334
Deleting a trusted certificate.....	334
<b>Chapter 30. Migrating to a new certificate.....</b>	<b>335</b>
<b>Chapter 31. Configuring the session connection code.....</b>	<b>336</b>
<b>Chapter 32. Target registration before a remote control session.....</b>	<b>337</b>
<b>Chapter 33. Configure target properties.....</b>	<b>339</b>
Using a specific target IP address for connections.....	340
Specifying an IP address for a Windows target.....	340
Specifying an IP address for a Linux target.....	340
Joining or Disconnecting a session.....	341
Logging target activity.....	341
<b>Chapter 34. Importing data from other sources.....</b>	<b>343</b>
Configure LDAP .....	343
Setting up LDAP synchronization.....	343
Verifying connection information.....	345
Configuring connection credentials.....	346
Setting connection security.....	347
Setting user authentication properties.....	349
Importing Active Directory Groups.....	352
Testing the Connection.....	354
Verifying that the groups are imported.....	355
Sample LDAP Configuration File.....	355
Import data from csv files into the Remote Control database.....	360
Creating a csv file.....	360
Mapping data in a csv file to the Remote Control database.....	361
Viewing the list of defined Import Templates.....	364
Changing the details of an Import Template.....	364
Deleting Import Templates.....	364
Importing a csv file.....	365
<b>Chapter 35. Database table and column descriptions .....</b>	<b>366</b>
ASSET schema tables.....	366

COMMON schema tables.....	377
<b>Chapter 36. Troubleshooting and Help .....</b>	<b>394</b>
Recovering when the program is not running.....	394
Login failure.....	394
Log distribution task of the scheduler.....	394
Using log files to solve a problem.....	395
Obtaining the server log files.....	395
Obtaining the controller log files.....	396
Obtaining the target log files.....	397
Obtaining the gateway log files.....	399
Obtaining the broker log files.....	399
Obtaining the smart card feature log files.....	400
Obtaining the smart card Fixlet log files.....	400
Setting up the Trusted Sites zone.....	400
Targets unable to contact the server successfully and a session cannot be established with these targets.....	401
Remotely installed targets cannot contact the server.....	403
Extending the session timeout value.....	403
Gray screen on a Windows 2003 system.....	404
Files not visible during a file transfer session.....	406
Getting control of a mac OS target after the screen is locked.....	406
Issues with visualization of RC Server 10 with IE.....	406
Getting Help .....	407
Using the Documentation.....	407
Accessing the Remote Control product documentation.....	408
Broker troubleshooting and FAQs.....	408
<b>Appendix A. Gateway sample scenarios.....</b>	<b>411</b>
Overview.....	411
Scenario 1 - Several networks using Network Address Translation (NAT).....	412
Scenario 2 - Meshed Networks.....	415
Scenario 3 - Web hosting.....	417
<b>Appendix B. Properties for configuring logging activity .....</b>	<b>425</b>
<b>Appendix C. Support.....</b>	<b>427</b>

Notices.....cdxxviii

**Index.....**

# Chapter 1. Overview of the Remote Control system

The Remote Control system includes the following main components:

## Remote Control Target

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

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

## Remote Control Controller

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

## Remote Control Server

A web application that manages all the deployed targets that are configured for managed mode and to point to the Remote Control Server 's URL. You can deploy it on an existing WebSphere® server, or install it by using the installer package along with an embedded version of WebSphere®. The server listens for HTTP or HTTPS connections by default. When it is installed with the embedded WebSphere® option, WebSphere® it listens on ports 80 and 443. When it is deployed on top of an existing WebSphere® server, the Remote Control server listens on ports 9080 and 9443. The server requires a database server: embedded Derby, only for proof of concept deployments; DB2®, SQL Server, and Oracle are the supported options. Additionally, it can also be configured to synchronize and authenticate user and group data from an LDAPv3 server, such as Active Directory or Tivoli Directory Server. This deployment scenario has the same networking characteristics as peer-to-peer. Therefore, direct TCP connectivity is required between all the controllers and all the targets. However, the Remote Control server provides a method of centralized, and finer, policy control, where targets can have different policies that are determined by the user who is trying to start the remote control session. The Server also provides for centralized audit and storage of full session automatic recordings. In this scenario, the controller is

not a stand-alone application, but is started as a Java™ Web Start application from the Remote Control server's web interface to start the remote control session.



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

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

The following components can be used only in managed mode:

#### **Remote Control CLI tools**

CLI tools are always installed as part of the target component but you can also install them separately.

The CLI provides command-line tools for the following tasks:

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

#### **Remote Control Gateway**

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

#### **Remote Control Broker**

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

## Chapter 2. Set a secure environment

Set a secure environment when you are using Remote Control.

By default, Remote Control is configured for http access and https with a default self-generated certificate. Learn how to configure more advanced security parameters for your environment.

### Configure the server URL

Configure properties to allow the target to use a secure URL to communicate with the BigFix® Remote Control Server.

You can configure properties to allow the target to use a secure URL to communicate with the BigFix® Remote Control Server. You can also configure properties to enable secure access to the server.

### HTTPS URL is enabled by default during installation

During a new server installation, the following server properties in the `trc.properties` file are set to true by default:

#### **enforce.secure.web.access**

Forces all access to the web application to use HTTPS.

#### **enforce.secure.weblogon**

Forces all logons through the web portal to use HTTPS.



**Note:** Any attempt to access the logon page through HTTP is redirected to HTTPS, unless the HTTP port is disabled.

#### **enforce.secure.alllogon**

Forces logons through the server services interface to use HTTPS. For example, the BigFix® Remote Control Server CLI options.

To enable HTTP access, the properties can be modified after the installation is complete.

A new option in the server installer, **Force targets to use https**, is selected by default at installation time but you can clear the check box.

When the **Force targets to use https** check box is selected, the `url` property in the `trc.properties` file is set to use HTTPS

```
url=[HTTPS address]
```

Where `[HTTPS address]` is the server IP address that is used for HTTPS access.

This action forces the targets to always use HTTPS when they contact the server regardless of the value of `enforce.secure.endpoint.callhome` and `enforce.secure.endpoint.upload` in `trc.properties`.

When you clear the **Force targets to use https** check box, the following value is set for the `url` property:



`url=[regular HTTP address]`.

Where *[regular HTTP address]* is the server IP address that is used for HTTP access.

## Enabling HTTP access

During a new server installation, the option to use HTTPS in target to server communication is selected by default. You can also enable HTTP communication.

To use HTTP, in target to server communication complete one of the following steps.

- When you are using the server installer program, clear the **Force targets to use https** option.
- When you are installing the server by deploying the `trc.war` file in WebSphere® Application Server, the following properties in the `trc.properties` file must be modified after the installation:
  - Set the `url` property to the HTTP URL.
  - Set `enforce.secure.endpoint.callhome` to false.
  - Set `enforce.secure.endpoint.upload` to false.

Additionally, to enable HTTP logon and access to the web portal, complete the following steps:

1. After the server installation, edit the `trc.properties` file.
  - a. In the server UI click **Admin > Edit properties file**.
  - b. Select `trc.properties`.
  - c. Set `enforce.secure.web.access`, `enforce.secure.weblogon`, and `enforce.secure.allogon` to *false*.
  - d. Click **Submit**.
2. Edit the following file, where *[INSTALLDIR]* is the Remote Control server installation directory.

### Windows™ systems

```
[INSTALLDIR]\wlp\usr\server\trcserver\cookie.xml
```

### Linux™ systems

```
[INSTALLDIR]/wlp/usr/server/trcserver/cookie.xml
```

3. Set `<httpSession cookieSecure="false"/>` and save the file.
4. Click **Admin > Reset Application**.

## Disable the HTTP port

Enforcing HTTPS communication and web access and logon does not disable the HTTP port. If a user or a target attempts to access the server on port 80, they are redirected to HTTPS for logon or callhome. You can disable HTTP completely on the web server. To disable HTTP, set the **Server Port on Webserver** field in the installer screens, or the **HTTP port** field in the **Remote Control Server Installer Wizard**, to 0.

If you are deploying the `trc.war` file in WebSphere® Application Server, to disable the HTTP port, complete the following steps:

1. In the WebSphere Integrated Solutions console, expand **Servers > Server Types**.
2. Select **Websphere application servers**.
3. Select the application server on which Remote Control is installed.
4. On the **Configuration** tab, expand **Web Container Settings**.
5. Select **Web container transport chains**.
6. Click **HttpQueueInboundDefault** on port 80.
7. In General Properties, clear the **Enabled** check box.
8. Click **Apply**.
9. Click **Cancel**.
10. Click **WCInboundDefault** on port 80.
11. In General Properties, clear the **Enabled** check box.
12. Click **Save** directly to master configuration.
13. Restart the WebSphere server.

After you disable the HTTP port, if a user or a target attempts to contact the server on HTTP they are not redirected to HTTPS and an error is displayed:

**In Firefox**

```
Unable to connect.
Firefox can't establish a connection to the server at: [IP address of your server]
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure
that Firefox is permitted to access the Web.
```

**In Internet Explorer**

Internet Explorer cannot display the webpage.

## Enforce an HTTPS logon

You can configure properties to force logons from the server UI to use HTTPS, by editing the `trc.properties` file. In a new server installation, the following properties are all set to `True` by default.

```
enforce.secure.weblogon=
```


	<p>Logons from the BigFix® Remote Control Server UI use HTTPS. Logons that use HTTP through another tool or page are not prevented.</p> <p>HTTPS is not shown in the URL, but the logon page with USERID/PASSWORD is posted as HTTPS. The <b>secure.url</b> parameter is used. If this property is set incorrectly, the logon does not succeed. This value is the default value.</p> <p><b>False</b></p> <p>Log on by using HTTP or HTTPS, whichever is entered in the browser URL.</p>
--	---

```
enforce.secure.alllogon=
```




**Note:** The **secure.url** property must be set with a proper host name, not localhost.



## Secure communication configuration

You can use the following properties in `trc.properties` to control, how secure communications are enforced.

```
secure.url=
```



--	--

Field Description	Determines the URL that a target uses to contact the Remote Control server.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>If a call home is received by using HTTP, the request is redirected to the secure URL. The secure URL is also returned in the response from the server. Targets are forced to use the secure URL when they send heartbeats to the Remote Control server. This value is the default value.</p> <p><b>False</b></p> <p>Targets are not forced to use the secure URL when they send heartbeats to the Remote Control server.</p> <p> <b>Note:</b> From Remote Control V9.1.3, HTTPS secure communication is enforced by setting the <b>url</b> property in the <code>trc.properties</code> file to HTTPS when <b>Force targets to use https</b> is selected during installation. To ensure HTTP target communication, confirm that the <b>url</b> property is set to the HTTP URL in the <code>trc.properties</code> file. If the <b>url</b> property is set to HTTPS, the targets use HTTPS after they first contact the server.</p> <p> <b>Note:</b> When you change the value of this property, you must restart the Remote Control server service for the new value to take effect.</p>

```
enforce.secure.endpoint.upload=
```


base to provide the upload and validation URLs to the controller and target when the session starts. This value is the default value.

#### False

The server does not redirect to the secure URL if an upload or a validation request is received by using HTTP.



**Note:** From Remote Control V9.1.3, HTTPS secure communication is enforced by setting the **url** property in the `trc.properties` file to HTTPS when **Force targets to use https** is selected during installation. To ensure HTTP target communication, confirm that the **url** property is set to the HTTP URL in the `trc.properties` file. If the **url** property is set to HTTPS, the targets use HTTPS after they first contact the server.



**Note:** When you change the value of this property, you must restart the Remote Control server service for the new value to take effect.

The following examples consider scenarios that reflect different security requirements that you might have about communications with the Remote Control Server:

- Example 1: All endpoint and user communications with the server must be encrypted with SSL.

#### Configuration

- Set **secure.url** in the `trc.properties` file to contain the HTTPS URL.
- Set the three `enforce.secure` properties to true by editing the `trc.properties` file.
- The Target and CLI do not need to be explicitly configured to use the HTTPS URL, but doing so avoids the first redirection.

- Example 2: All user communications with the server must be encrypted with SSL. Endpoint communications that are not callhomes must be encrypted. For example, audit and recording uploads or validating session requests.

#### Configuration

- Configure the HTTP URL to be used by the call homes in the **url** property in the `trc.properties` file.
- Configure the HTTPS URL to be used by the users, endpoint uploads, and the API in the **secure.url** property.
- **enforce.secure.web.access** = true.
- **enforce.secure.endpoint.callhome** = false.

- **enforce.secure.endpoint.upload** = true.
  - Target and CLI tools are configured with the HTTP URL.
- Example 3: All user communications with the server must be encrypted with SSL. Endpoint communications do not need to be encrypted.

#### Configuration

- Configure the HTTP URL to be used by the endpoints call home and uploads in the `URL` property in the `trc.properties` file.
  - Configure the HTTPS URL to be used by the users and the API in the **secure.url** property.
  - **enforce.secure.web.access** = true.
  - **enforce.secure.endpoint.callhome** = false.
  - **enforce.secure.endpoint.upload** = false.
  - Target and CLI tools are configured with the HTTP URL.
- Example 4: No need for enforcement other than through the regular configuration options (**url** property and **ServerURL**).

#### Configuration

- **url** = http://localhost/trc.
- **secure.url** = https://localhost/trc.
- **enforce.secure.web.access** = false.
- **enforce.secure.endpoint.callhome** = false.
- **enforce.secure.endpoint.upload** = false.

## Protocol configuration after a server upgrade

When you upgrade by using the server installer program and select to keep existing properties, you must configure properties after installation if you change your protocol selection.



**Note:** From V9.1.3, HTTPS is enabled by default. If you do not keep existing properties during the upgrade and you clear the **Force targets to use HTTPS** option, you must configure properties after installation. For more information, see [Enabling HTTP access \(on page 17\)](#).

### Changing from HTTPS to HTTP

Your previous server installation is configured to use HTTPS and you clear **Force targets to use HTTPS** during the upgrade. To access and log on to the server UI by using HTTP, you must also complete the following steps after the upgrade.

1. Edit the `trc.properties` file and set **enforce.secure.allogon** to *false*.
2. Edit the following file, where `[INSTALLDIR]` is the Remote Control server installation directory.

#### Windows™ systems

```
[INSTALLDIR]\wlp\usr\server\trcserver\cookie.xml
```

**Linux™ systems**

```
[INSTALLDIR]/wlp/usr/server/trcserver/cookie.xml
```

3. Set `<httpSession cookieSecure="false"/>` and save the file.
4. Restart the server service.

**Changing from HTTP to HTTPS**

Your previous server installation is configured to use HTTP and you select the **Force targets to use HTTPS** option during the upgrade. To access and log on to the server UI by using HTTPS, you must also complete the following steps after the upgrade.

1. Edit the `trc.properties` file and set **enforce.secure.web.access**, **enforce.secure.weblogon**, and **enforce.secure.allogon** to `true`.
2. Edit the following file, where `[INSTALLDIR]` is the Remote Control server installation directory.

**Windows™ systems**

```
[INSTALLDIR]\wlp\usr\server\trcserver\cookie.xml
```

**Linux™ systems**

```
[INSTALLDIR]/wlp/usr/server/trcserver/cookie.xml
```

3. Set `<httpSession cookieSecure="true"/>` and save the file.
4. Restart the server service.

**Signed certificate management**

By default, Remote Control creates a self-signed certificate for the website.

You can change the default certificate by installing your own certificate. For more information about installing a certificate, see [Certificate management \(on page 327\)](#).

**Installing a certificate**

To install a certificate in Remote Control, you can either use an existing `P12` or `JKS` keystore or import an existing certificate into the existing keystore.

Any changes that are made to the certificate configuration are overwritten if you reinstall or upgrade the Remote Control server. Choose the appropriate method to install a certificate for Remote Control. You can also configure the SSL certificate by using the server installer. For more information about configuring the SSL certificate during installation, see the BigFix® Remote Control Installation Guide

To use an existing keystore, complete the following steps

If you want to use a keystore different than the default `.jks`, complete the following steps.



1. Edit the `ssl.xml` file.
2. Locate the `<keystore/>` parameter. Set appropriate values for your certificate keystore.

### ID

The default value is `defaultKeyStore`. You can change the value to an ID of your choice or keep the default value.

### Password

To apply custom certificate properly using AES-encoded password, do the following:

- a. Ensure the server is stopped.
- b. Open the `[installdir]\tools\env\env.xml` file.
- c. Copy the value reported in the value property of the `wlp.password.encryption.key` variable.

For example: From `<variable name="wlp.password.encryption.key" value="8f7008648eb308479c88f388e82000209a26" />`, copy  
`8f7008648eb308479c88f388e82000209a26`

- d. Run the following commands:

```
[installdir]\wlp\bin\securityUtility.bat encode --encoding=aes
--key=<encryption_key>
```

where `<encryption_key>` is the value copied in the previous step.



**Note:** On Linux, the `securityUtility` tool does not have the `.bat` extension. Therefore, use `securityUtility` instead of `securityUtility.bat`.

- e. Insert twice the password to be encrypted.
- f. Manually copy the resulting encrypted password in the XML file in `[installdir]\wlp\usr\servers\trcserver\ssl.xml`



**Note:** The encrypted password starts with "`{aes}`". For example,  
`{aes}AFLSwk76PovVwmQlVCULHEkkzRqPUgLoZVy33sMxPZf)`

- g. Restart the server.

### Location

Enter the absolute path to the existing keystore. The value can be the path to a `jks` file or a `p12` file.

### Type

Determines the type of keystore file. If you are using a `p12` file use `PKCS12`. If you are using a `jks` file, you do not need to define a type value.

3. Save the file.
4. Restart the Remote Control server.

## To generate a signed certificate

To generate a certificate, either self-signed or CA signed, see the instructions at the following links:

- [Creating a self signed certificate](#)
- [Creating Certificate Authority signed certificates](#)

## Backing up your certificate file

Back up your certificate file if you are upgrading your Remote Control server and you previously manually installed a certificate.

The following information applies only when you previously used the server installer to install the Remote Control server with an embedded WebSphere® Application Server 8.5 Liberty Profile.

If you are using the default keystore and `key.jks` file, back up the following file and directory.

Windows™ systems

```
\[installdir]\wlp\usr\servers\trcserver\resources\security\key.jks
```

Linux™ systems

```
/[installdir]/wlp/usr/servers/trcserver/resources/security/key.jks
```

Where `[installdir]` is the Remote Control server installation directory.

If the default keystore file is not in the default directory or you changed the default keystore password, also back up the `ssl.xml` file. The file is in the following directory.

Windows™ systems

```
\[installdir]\wlp\usr\servers\trcserver\ssl.xml
```

Linux™ systems

```
/[installdir]/wlp/usr/servers/trcserver/ssl.xml
```

Where `[installdir]` is the Remote Control installation directory.



**Note:** If your `key.jks` file is not in the default keystore directory, but is still within the Remote Control server installation directory you must back up the `key.jks` file.

## Setting password rules

You can use properties in the `trc.properties` file to create a set of password rules. The rules can define the type of passwords that can be created, how the passwords must be created, and whether the passwords must be periodically changed.

```
password.encrypt=
```

Modifiable Field	<b>password.encrypt</b>
Field Description	Determines whether passwords are encrypted in the database.
Possible Values	Yes or No
Value Definition	<p><b>Yes</b></p> <p>Passwords are encrypted in the database.</p> <p><b>No</b></p> <p>Passwords are not encrypted in the database.</p>

```
password.reuse=
```

Modifiable Field	<b>password.reuse</b>
Field Description	Determines whether users can reuse passwords.
Possible Values	Yes or No
Value Definition	<p><b>Yes</b></p> <p>Users can reuse passwords.</p> <p><b>No</b></p> <p>Users cannot reuse passwords.</p>

```
expire.new.password=
```

Modifiable Field	<b>expire.new.password</b>
Field Description	Determines whether users are required to set their own password after they receive the computer-generated password.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Users must set their own password after they receive the computer-generated password.</p> <p><b>False</b></p>

Users do not have to set their own password after they receive the computer-generated password.

```
password.timeout=
```

Modifiable Field	<b>password.timeout</b>
Field Description	Determines whether passwords expire.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords expire.</p> <p><b>False</b></p> <p>Passwords do not expire.</p>

```
password.timeout.period=
```

Modifiable field	<b>password.timeout.period</b>
Field Description	Defines after how many days passwords expire.
Possible Values	User-defined. The default value is 90.
Value Definition	User-defined integer

```
password.period=
```

Modifiable field	<b>password.period</b>
Field Description	Maximum number of days before a password can be reused.
Possible Values	User-defined
Value Definition	User-defined integer

```
password.check=
```

Modifiable Field	<b>password.check</b>
Field Description	Determines whether to enable password rule checking.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must follow certain rules. This value is the default value.</p>

	<p><b>False</b></p> <p>Passwords do not follow rules.</p>
--	---

```
password.must.have.non.numeric=
```

Modifiable Field	<b>password.must.have.non.numeric</b>
Field Description	Determines whether passwords must contain non-numeric characters.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must contain non-numeric characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not need to contain non-numeric characters.</p>

```
password.must.have.numeric=
```

Modifiable Field	<b>password.must.have.numeric</b>
Field Description	Determines whether passwords must contain numeric characters.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must contain numeric characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not have to contain numeric characters.</p>

```
password.must.have.non.alphanumeric=
```

Modifiable Field	<b>password.must.have.non.alphanumeric</b>
Field Description	Determines whether passwords must contain non-alphanumeric characters.
Possible Values	True or False
Value Definition	<b>True</b>

	<p>Passwords must contain non-alphanumeric characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not have to contain non-alphanumeric characters.</p>
--	--

`password.min.length=`

Modifiable Field	<b>password.min.length</b>
Field Description	Minimum length of a password.
Possible Values	User-defined. Default value is eight.
Value Definition	User-defined integer

`password.max.length=`

Modifiable Field	<b>password.max.length</b>
Field Description	Maximum length of a password.
Possible Values	User-defined. Default value is fifteen.
Value Definition	User-defined integer

`password.requires.mixedcase=`

Modifiable Field	<b>password.requires.mixedcase</b>
Field Description	The password must contain both lowercase and uppercase characters.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must contain both lowercase and uppercase characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not need to contain both lowercase and uppercase characters.</p>

`password.max.sequence=`

Modifiable Field	<b>password.max.sequence</b>
------------------	------------------------------

Field Description	Maximum length of a sequence of characters. For example, 1234.
Possible Values	User-defined. Default value is three.
Value Definition	User-defined integer

```
password.max.matching.sequential.chars=
```

Modifiable field	<b>password.max.matching.sequential.chars</b>
Field Description	Maximum number of sequential password characters that can match.
Possible Values	User-defined. The default value is two.
Value Definition	User-defined integer

```
password.max.previous.chars=
```

Modifiable field	<b>password.max.previous.chars</b>
Field Description	Maximum number of sequential password characters that can be reused in a new password.
Possible Values	User-defined
Value Definition	User-defined integer

## Lock user accounts

You can lock users accounts after a number of unsuccessful logons so that someone cannot guess a user name and password combination.

When an account is locked with a time period enabled, when the time period expires, a user can log on again with the correct password. However, if an incorrect password is entered another time, the account is locked again after a single attempt. If the account is locked and a user attempts to log on during the lockout period, the expiry time starts from the last attempt. Even when the attempt was made during a locked out phase. This is for security reasons, so that an administrator can see whether an attempt is being made to hack an account. The failed count is increasing and the last time of failure recorded. You can use the following properties to lock user accounts, set a period for the lock and specify computers that the locked account can be used on.

```
account.lockout=
```

--	--

Field Description	Lock a user account after a consecutive number of failed logons. Set to 0 to disable the function. The default value is 0.
Possible Values	User defined.
Value Definition	User-defined integer.

```
account.lockout.timeout=
```





Examples of usage:

**Example 1:**

**account.lockout** = 0.

**account.lockout.timeout** = X.

The account is not locked after unsuccessful logon attempts because **account.lockout**=0.

**Example 2:**

**account.lockout** = 3.

**account.lockout.timeout** =

After three successive failed logons for an account, the account is locked, and requires a reset. The reset can be made by an administrator account by editing the database or by using the server UI. This reset is a manual reset because **account.lockout.timeout** is not assigned a value.

**Example 3:**

**account.lockout** = 3.

**account.lockout.timeout** = 1HOUR .

After three successive failed logons for an account, the account is locked for a duration of 1 hour. However, it can be reset in the database or the serverUI by using an administrator account.

**Example 4:**

**account.lockout** = 3

**account.lockout.timeout** =


**account.lockout.allowlogonfrom**=1.1.1.1;

After three successive failed logons for an account, the account is locked, and requires a reset in the database or the server UI by using an administrator account. The user can also log on from a computer with the IP address set in **account.lockout.allowlogonfrom** and the lockout is ignored.

When a user account is locked, you can unlock the account by using the **Unlock locked userid** menu item. For more information, see [Unlocking user accounts \(on page 65\)](#).

When a user uses the forgotten password option on the logon page, a password is emailed to the registered user for the account. However, if the account is locked, it remains locked as a security precaution so that an attacker cannot have unlimited attempts to guess a password. You can use the property **account.lockout.reset.onemailpassword** to automatically unlock an account in this scenario.

```
account.lockout.reset.on.emailpassword=
```

Modifiable field	<b>account.lockout.reset.on.emailpassword</b>
Field Description	Determines whether a locked account is reset when the user selects the forgotten password check box on the logon screen.
Possible Values	True / False
Value Definition	<p><b>True</b></p> <p>The locked account is reset when the password reset email is received from the administrator.</p> <p><b>False</b></p> <p>The locked account is not reset when the forgotten password request is received</p> <p> <b>Note:</b> This property works with the forgotten password feature, therefore, email must be enabled in the system.</p>

## Automatic passphrase encryption

For security purposes, plain text passwords that are contained in the broker, gateway, target, and CLI component configuration, are now automatically encrypted. Use the **DisableAutomaticPassphraseEncryption** property to determine whether the passwords are automatically encrypted or not.

For the broker and gateway components, plain text passwords can be set within the **Passphrase** and **DefaultTLSCertificatePassphrase** parameters in the component configuration files. For the target, CLI and broker, the **ProxyURL** property value can contain a plain text password in the *userid:password* combination in the URL. The broker and gateway passwords and the *userid:password* combination are now automatically encrypted.

### **DisableAutomaticPassphraseEncryption=No**

Plain text passwords are automatically encrypted. This value is the default value.

### **DisableAutomaticPassphraseEncryption=Yes**

Plain text passwords are not automatically encrypted. For security reasons, it is recommended that you do not disable the automatic encryption.

## Setting the parameter value

You can set the **DisableAutomaticPassphraseEncryption** property value in the following places:

### **Broker component**

The broker configuration file `trc_broker.properties`.

Windows operating system. The file is in the following directory, depending on the version of Windows operating system that is installed:

`\Documents and Settings\All Users\Application Data\BigFix\Remote Control  
\Broker.`

`\ProgramData\BigFix\Remote Control\Broker.`

Linux operating system: `/etc.`

### Gateway component

The gateway configuration file `trc_gateway.properties.`

Windows operating system. The file is in the following directory, depending on the version of Windows operating system that is installed:

`\Documents and Settings\All Users\Application Data\BigFix\Remote Control  
\Gateway.`

`\ProgramData\BigFix\Remote Control\Gateway.`

Linux operating system: `/etc.`

### Target component

Windows operating system. In the target registry after the target is installed or as a parameter in a silent installation command.



**Note:** There is no option to disable the auto encryption when you install the target by using the installer program or the deployment Fixlet in the BigFix® console.

Linux operating system: `/etc/trc_target.properties.`

### CLI component

Windows operating system. In the target registry after the CLI component is installed.



**Note:** There is no option to disable the auto encryption when you install the CLI component by using the installer program or the deployment Fixlet in the BigFix® console.

Linux operating system: `/etc/trc_target.properties`



**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.

The following scenarios provide steps for the correct use of the parameter when you do not want to automatically encrypt the passwords. However, for security reasons, it is recommended that you do not disable the automatic encryption.

## New deployment scenario

When you install the components for the first time, and you do not want to automatically encrypt passwords, complete the following steps:

### Broker and gateway components

1. After you install the component, edit the relevant properties file.
2. Enter the plain text passwords in the relevant **Passphrase** and **DefaultTLSCertificatePassphrase** parameters.
3. Set **DisableAutomaticPassphraseEncryption=Yes**.
4. Save the file.
5. Start the component service.

The passwords are saved as plain text in the properties files.

### Target component

#### Windows operating system:

1. Set the following parameter values in the silent installation command:
  - Set **TRC\_PROXY\_USER\_ID** and **TRC\_PROXY\_PASSWORD** with plain text values.
  - Set **DISABLEAUTOMATICPASSPHRASEENCRYPTION=Yes**.
2. Run the installation command. For more information about running a silent target installation, see the *BigFix® Remote Control Installation Guide*.

#### Linux operating system:

1. Edit the `/etc/trc_target.properties` file.
2. Set a plain text `userid:password` combination in the **ProxyURL** property.
3. Set **DisableAutomaticPassphraseEncryption=Yes**.
4. Save the file.
5. Start the target service.

The `userid:password` combination in the proxy URL is saved as plain text.



**Note:** In the new deployment scenario, you must set the **DisableAutomaticPassphraseEncryption** property value to Yes before you start the component for the first time. Otherwise, the components automatically encrypt the passwords when they start. The components do not decrypt passwords after they are encrypted.

## Upgrade scenario

When you upgrade the components, and you do not want to automatically encrypt existing plain text passwords, complete the following steps:

### Broker and gateway components

1. Edit the current properties file.
2. Set **DisableAutomaticPassphraseEncryption=Yes**.
3. Upgrade the component.

The passwords are saved as plain text in the properties files.

### Target and CLI components

#### Windows operating system:

1. Edit the target registry and set **DisableAutomaticPassphraseEncryption=Yes**.
2. Upgrade the component.

#### Linux operating system:

1. Edit the `/etc/trc_target.properties` file and set **DisableAutomaticPassphraseEncryption=Yes**.
2. Save the file.
3. Upgrade the component.

The `userid:password` combination in the proxy URL is saved as plain text.

## Disable encryption after you start the components

The components do not decrypt passwords after they are encrypted. Therefore, to disable the automatic encryption and store plain text passwords after you start the components, complete the following steps. You must have the plain text passwords available for this scenario.

### Broker and gateway components

1. Edit the current properties file.
2. Set **DisableAutomaticPassphraseEncryption=Yes**.
3. Delete the encrypted passwords and replace them with the plain text passwords.
4. Restart the component.

### Target and CLI components

#### Windows operating system:

1. Edit the target registry and set **DisableAutomaticPassphraseEncryption=Yes**.
2. Modify the **ProxyURL** property and set the *userid:password* combination to a plain text value.
3. Restart the component.

#### Linux operating system:

1. Edit the current `/etc/trc_target.properties` file and set **DisableAutomaticPassphraseEncryption=Yes**.
2. Modify the **ProxyURL** property and set the *userid:password* combination to a plain text value.
3. Save the file.
4. Restart the component.

The *userid:password* combination in the proxy URL is saved as plain text.



**Note:** After passwords are encrypted, if you set `DisableAutomaticPassphraseEncryption` to `Yes` and restart the components, the passwords are not affected. The components do not decrypt the passwords and they can still use the encrypted password to unlock the keystore or access the proxy.

#### More information

- Keywords or commands are not available to decrypt the passphrases after they are encrypted.
- The encryption uses an encryption key that is derived from a value unique to the underlying system. The encryption key is never stored. The key is derived from the unique system value every time the component is started. Hence, it is not possible to copy an encrypted passphrase or a configuration file with encrypted passphrases from one system to another system. The component on the other system is unable to use the encrypted passphrase because it is encrypted with a different key.
- The system-unique value that is used to create the encryption key can be changed. For example, by reinstalling the operating system. If a component configuration with encrypted passphrases is restored from a backup after the operating system is reinstalled, the component is unable to use the encrypted passphrases to open the keystore because they are encrypted with a different key. It is recommended that the plain text passphrase is backed up separately. For example, by using a secure password vault. Do not store the backup passphrase together with the backup keystore.
- Encrypted passphrases are prefixed with the string `{aes-128-gcm}`. However, the passphrase that is configured in a gateway **inbound** and **inbound6** connection is encrypted with a different algorithm. It is prefixed with the string `{pbkdf2-hmac-sha256}`.
- The encryption algorithm is AES in GCM mode with a 128-bit encryption key.
- The key derivation algorithm is PBKDF2-HMAC-SHA256 with a 128-bit salt.

## Enforcing strict HTTPS validation of certificates

You can configure Remote Control to enforce strict HTTPS validation of certificates. All HTTPS connections from the target, broker, CLI, and controller are verified and the connection fails if the certificate is not trusted.

To enable strict validation of HTTPS certificates by the Remote Control components, the following settings must be enabled:

### Controller component in managed mode

1. In the Remote Control server UI select **Admin > Edit properties file**.
2. Select **common.properties**.
3. Set **https.strict validation** to *true* and click **Submit**.
4. Select **Admin > Reset Application**.

### Target or CLI

1. Set the **HTTPSStrictValidation** property to Yes in the following locations.

#### Windows operating system.

Edit the target registry and go to `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`

#### Linux operating system.

Edit the `/etc/trc_target.properties` file.

2. Restart the target service.

### Broker component

1. Edit the `trc_broker.properties` file.
2. Set **HTTPSStrictValidation** to Yes.
3. Save the file and restart the broker service.

After configuration, the components use the system truststore to verify HTTPS connections to the server. If the server certificate is issued by a certificate authority (CA) trusted by your operating system, the components work automatically. If the CA that is used by the server is not trusted by the operating system, it can be added by using the standard operating system certificate management methods.

## Chapter 3. Secure target registration

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

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

The feature is controlled by the **rc.enforce.secure.registration** property in the `trc.properties` file. Use the following values to configure the property.

### **true**

Secure target registration is enabled. Secure tokens are used to authenticate a target when it contacts the server. The default value is *true*.

### **false**

Secure target registration is disabled.

## Tokens for secure authentication of targets

Two types of token are used as part of the implementation for secure target registration in Remote Control.

The secure target registration property must also be enabled. For more information, see [Secure target registration \(on page 40\)](#).

The tokens are generated by the Remote Control server.

### **Registration token**

A token that is used to authenticate a target when it initially contacts the server. The token is used for new target registrations and also when you reinstall a target whose details are still in the database.

You can create a token in the server UI and specify a validity period for the token. For more information about creating a registration token, see [Creating a secure registration token \(on page 179\)](#).

### **Endpoint token**

A token that is sent to a target after it registers with the server. The target stores the token and uses it for all subsequent callhomes to the server. The token is also saved in the target details in the database.

To allow the target details to be updated, the token in the database must match the token that is stored on the target. The Endpoint token is valid until the target entry is deleted from the database. For more information about how the tokens are used to authenticate the targets, see [How targets securely authenticate with the server \(on page 41\)](#).



**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.

## How targets securely authenticate with the server

After you enable the secure authentication property, you can enable targets to securely register or update their details in the Remote Control database.

### New registrations

For a new target or an existing target to contact the server after the secure registration feature is enabled, use the following process to implement secure authentication:

- Create a secure registration token on the Remote Control server. Copy the token data and keep it confidential. For more information about how to create a token, see [Creating a secure registration token \(on page 179\)](#).
- Distribute the token when you install the target. For more information, see the *BigFix® Remote Control Installation Guide*.

The target uses the registration token when it contacts the server. The server verifies that the token matches an existing token on the server. If the token is valid, the new target is registered in the server or the details of the existing target are updated. The response from the server to the target provides an endpoint token. The target uses the endpoint token in subsequent callhomes to the server.



**Note:** The registration token in the property `RegistrationToken` which is contained in the registry key (Windows) or in the configuration file (UNIX) is deleted as soon as the target registers to the server and obtains the endpoint token.

### Updates to target entries after they register

When a target contacts the server after it registers, the following process is used to implement secure authentication:

- When the target contacts the server, it sends the endpoint token.
- If the target details on the server contain the same endpoint token, the target details are updated in the database. If the tokens do not match, the target details are not updated.

# Chapter 4. Configure SAML 2.0 authentication on the server

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

Configure the server to support SAML 2.0 authentication by using a SAML 2.0 identity provider (IdP).

After configuration, SAML 2.0 support enables web-based Single Sign-On (SSO) authentication. Logged in users are automatically redirected to the web-based components that support SAML 2.0 authentication without having to log in again.

For the SAML SSO to work properly with the Remote Control server, the users must exist in the server database. The users can be added manually or by using an LDAP server. For more information about configuring LDAP, see [Configure LDAP \(on page 343\)](#). The LDAP server can also be configured by using the LDAP Configuration wizard. For more information, see [Configure LDAP properties by using the LDAP wizard \(on page 163\)](#). The IdP administrator is responsible for the configuration of the LDAP identity provider. If LDAP is enabled, the IdP must be configured to authenticate the users by using the same backend LDAP server as Remote Control.

You can configure the server for SSO by using the server installer program. This method is the recommended method. You can also configure for SSO after you install the server.

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

For more information, see [SAML 2.0 Web Browser Single-Sign-On](#).



**Note:** The default Remote Control configuration supports a service provider (SP) initiated login flow, where the user initiates the login process by first accessing the product interface. Remote Control also supports an Identity Provider initiated login flow, where the user initiates the login process by accessing the Identity Provider interface first. To enable support for an Identity Provider initiated login, update the `sso.xml` file and include the `useRelayStateForTarget` and the `targetPageUrl` to the `samlWebSso20` section as given below:

```
<samlWebSso20 id="defaultSP" keyStoreRef="samlKeyStore" httpsRequired="true"
useRelayStateForTarget="false"
targetPageUrl="https://Server_FQHN/trc/ssologon.do"
signatureMethodAlgorithm="SHA256"/>
```

where `Server_FQHN` is your server host name.

## Configuring the server for single sign-on during installation

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

When you install the Remote Control server by using the installer program, you can select options to configure Single-Sign-On (SSO). To enable SSO, complete the following steps:

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

### Enable SSO

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

### Metadata XML file

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

### Algorithm used to sign SAML messages

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

### Advanced parameters (optional)

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

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

The first time that you enable SSO, a new default SAML certificate keystore is created. For future upgrades, you can select the regeneration option to create a new default certificate keystore.

The current keystore is deleted and the new one is saved. When you select this option, you must reestablish the connection between the SP and the IdP after the server restarts.

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

## Configuring the server for single sign-on after installation

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

You must create a keystore with a single self-signed certificate (or CA signed certificate) before you start the configuration. Select a **Key Size** of 2048 and select sha256 for the **Signature Algorithm**. The keystore file can be a

.p12 or .jks file. Do not save the file to the server installation directory because that might conflict with the server self-signed certificate. Set a long validity period for the keystore. For more information about creating a keystore file, see [Creating a self signed certificate \(on page 327\)](#).



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

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

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

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

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

**Windows™ operating system**

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

**Linux™ operating system**

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

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

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

**[hostname:port]**

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

**[samlKey.file]**

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

**[yourkeystorepassword]**

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

**[filetype]**

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

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

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

In a default configuration, the following values are used:

**AssertionConsumerService URL**

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

**Service Provider (SP) metadata URL**

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

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

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

**Windows™ operating system**

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

**Linux™ operating system**

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

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

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

4. Get the SAML metadata XML file from the Identity Provider (IdP).

How this file is obtained varies, depending on the IdP. Rename the file to `idpMetadata.xml` and copy it to the following directory on the server:

**Windows™ operating system**

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

#### Linux™ operating system

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

5. Edit the `common.properties` file and set `sso.enabled` to `True`.

The file is in the following directory:

#### Windows™ systems

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

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

#### Linux™ systems

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

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

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

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



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

# Chapter 5. Access the BigFix® Remote Control Server web interface

After you install the BigFix® Remote Control Server software and the BigFix® Remote Control Target software, you can log on to the server application. For more information about installing and configuring the server and target software, see the [Remote Control Installation Guide](#)

## Logging on to the Remote Control server

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

1. In a web browser type

`http://SERVERNAME/trc.`

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

2. Enter a valid ID and password.

Invalid or missing IDs and passwords generate an error message.

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

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

3. Click **Logon**.

The BigFix® Remote Control Server UI is displayed.

## Getting a temporary logon password

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

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



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

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

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

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

4. Log on with your ID and temporary password.

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

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

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

## Setting up email

By editing the `trc.properties` file, you can enable the email function.

To use the email function, a mail server must be installed and set up. By editing the `trc.properties` file, you can enable the email function by editing the following variables:

### **email.enabled**

Set to true to enable email function.

### **smtp.server**

Set to the address of the mail server.

### **smtp.authentication**

Set to true if you want the SMTP server to authenticate with the SMTP ID and password. Set to false if no authentication is required.

### **smtp.userid**

User ID for the SMTP server.

### **smtp.password**

Password for the SMTP server.

## Logging off from the Remote Control server

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

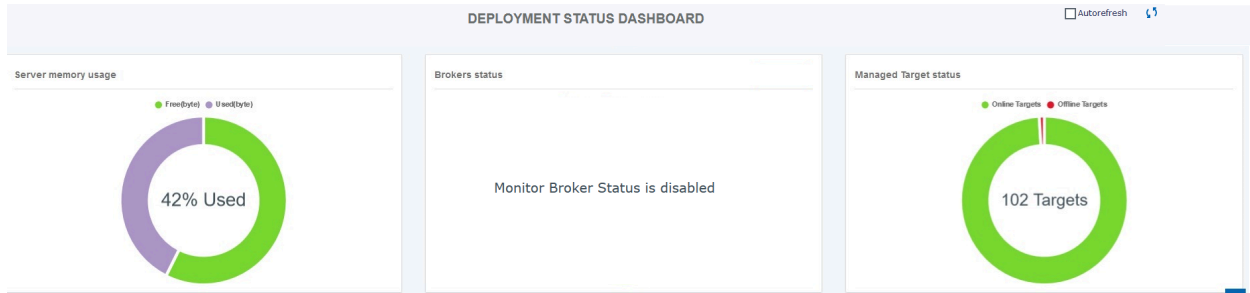


# Chapter 6. Using the Deployment Status Dashboard

The Deployment Status Dashboard provides a quick view of the system and brokers health status.

To access the dashboard, from the Remote Control Server web interface menu select **Admin > Deployment Status Dashboard**.

By default, the Dashboard shows Server Memory status and Managed Targets status.

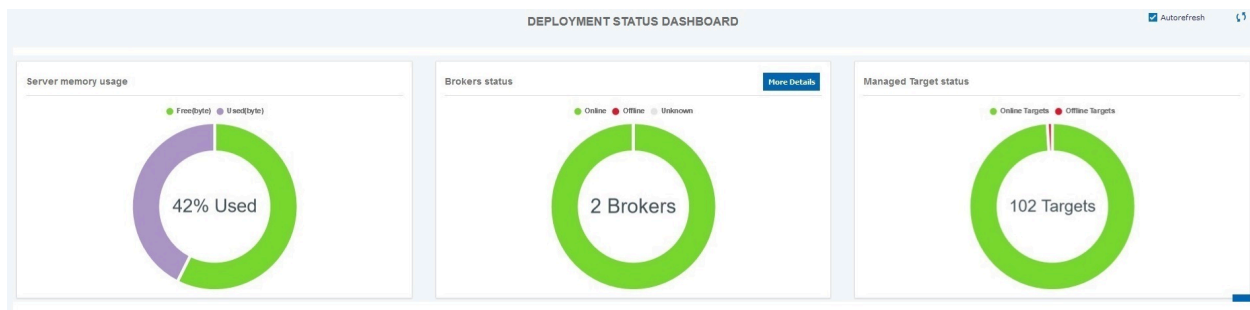


You can also activate the following additional components.

- [Broker Status Monitor \(on page 49\)](#)
- [Broker Status Control \(on page 50\)](#)
- [On Demand Target Activity Monitor \(on page 50\)](#)
- [Broker Activity History Control \(on page 51\)](#)
- [Unattended Target Activity Monitor \(on page 52\)](#)
  
- [Application Errors Monitor \(on page 53\)](#)

## Broker Status Monitor

The Broker Status Monitor component on the Deployment Status Dashboard shows the status of the Brokers.



The broker status can be:

- **Online:** The broker has contacted the server in the last `rc.dashboard.broker.heartbeat.minutes`.
- **Offline :** The broker has not contacted the server in the last `rc.dashboard.broker.heartbeat.minutes`.
- **Unknown:** The broker has not yet contacted the server after a server restart.

### Activate the Broker Status Monitor

To activate the Broker Status Monitor component on the Deployment Status Dashboard on the Remote Control Server:

1. From the Remote Control Server web interface menu, select **Admin > Edit Properties File** and then select **trc.properties**.
2. At the bottom of the page, in the **Status Dashboard - Configure the Broker Status Monitor** section, set the property **rc.dashboard.show.broker.status** to `True`.
3. At the top of the page, click **Submit**.
4. From the Remote Control Server web interface menu, select **Admin > Reset Application**.

### Update the Brokers configuration

- For Brokers of version higher than 10.0.0.0514, restart the broker.
- For Brokers of earlier version:
  1. Update the `trc_broker.properties` file of each broker by adding the following line:

```
HeartBeatTimeout = number_of_minutes
```

where `number_of_minutes` is the value that was set in

```
rc.dashboard.broker.heartbeat.minutes.
```

2. Restart the broker.

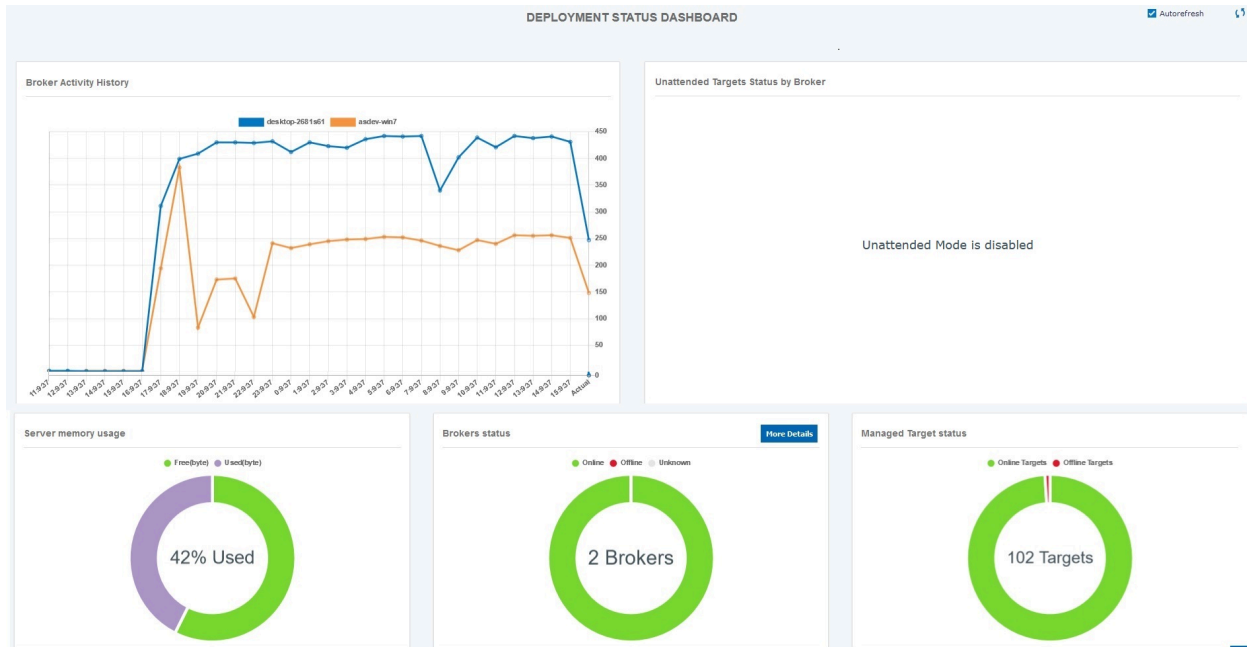
### Broker Status Control

The Broker Status Control component shows the status of the broker as known to the server.

The status of the broker is determined from the fact that the brokers contact the server at `rc.dashboard.broker.heartbeat.minutes` intervals. If the server does not receive a contact from the broker after the defined interval, it flags the broker status as *Offline*.

### On Demand Target Activity Monitor

The On Demand Target Activity Monitor enables to view the broker activity related to On Demand Targets activity over time.



### Activating the On Demand Target Activity Monitor

To activate On Demand Target Activity Monitor on the Remote Control Server:

1. From the Remote Control Server web interface menu, select **Admin > Edit Properties File > trc.properties**.
2. At the bottom of the page, in the **Status Dashboard - Include OnDemand Activity in Broker Trend** section, set the property `rc.dashboard.show.ondemand.trend` to True.
3. At the top of the page, click **Submit**.
4. From the web interface menu, select **Admin > Reset Application**.

**!** **Important:** If the On Demand Target Activity Monitor is used along with other dashboard features, you need to configure `rc.dashboard.broker.mapping` to avoid brokers duplication on the dashboard page. This property defines a mapping between the broker IP address as seen by the server and the hostname of the broker. For example: "10.14.75.67,eolo;10.14.75.62,harlock". Refer to the property description in the *edit trc.property* web page for more information on how to configure the parameter.

### Broker Activity History Control

- When the Unattended Target support is not activated, this control shows how many OnDemand sessions are established by each broker in the given time interval. The default time interval is 60 minutes.
- When the Unattended Target support is activated, the OnDemand session counts are added to the incoming heartbeats (only if OnDemand Target Activity Monitor has been activated).

## Unattended Target Activity Monitor

When the Unattended Target support is activated, the dashboard shows the real-time status of the broker activity trend related to this type of target over time and the status of the reporting targets by broker.

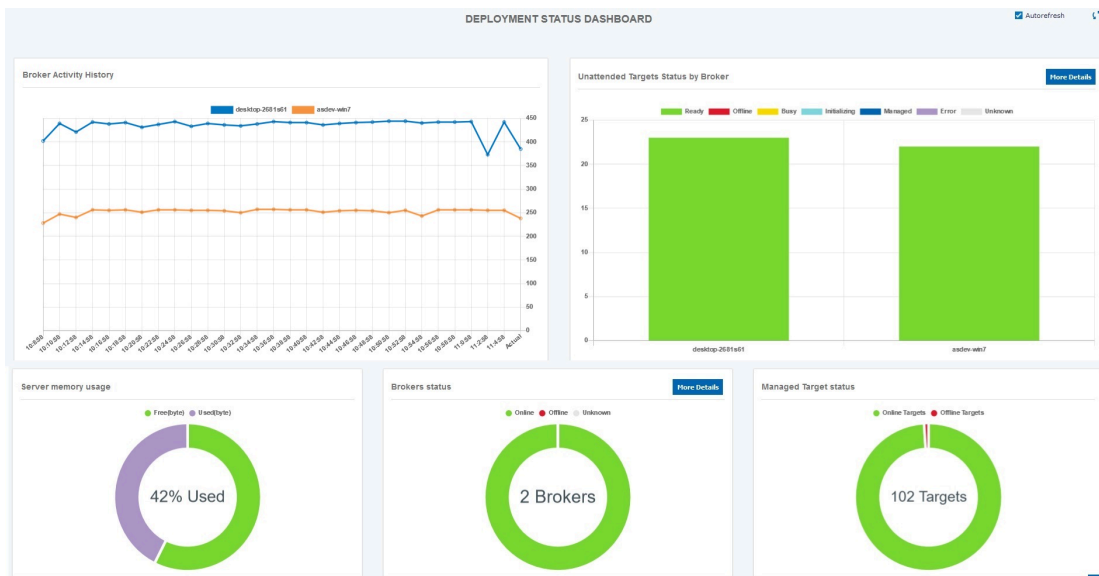
### The Broker Activity History Control

This control shows how many heartbeats are received by each broker in the given time interval.

The time interval corresponds to the value of the `rc.unattended.heartbeat.interval.minutes` property.

### The Unattended Target Status Control

This control shows the real time status of Unattended targets.



The status can be:

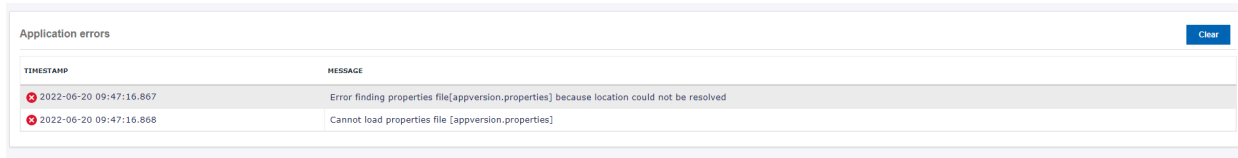
- - **Ready** The target is ready.
  - **Offline** The target is offline.
  - **Initiating** The target is about to start a Remote Control Session.
  - **Busy** The target is in a Remote Control Session.
  - **Managed** The target once registered as Unattended has reverted to Managed.
  - **Unknown** The target that has not contacted the Server after a Server restart.
  - **Error** The target is in error status.

You can get a list of targets in Offline, Busy, Unknown and Error status by clicking on the More Details button on the control.

You can also exclude specific target status from the view by clicking the corresponding status icon on the control legend.

## Application Errors Monitor

The Application Errors Monitor component allows to monitor error conditions on the Remote Control Server Application.



The table shows the last 100 errors that occurred on the server application in chronological order. You can clear the data in the table by clicking the "Clear" button at the top right corner of the box.

## Additional Dashboard Controls

The following additional options can be used to control the Dashboard behavior.

You can specify these options from the "Status Dashboard - Tuning options" section of the trc.property file.

### Dashboard Preload at System Start Up

The dashboard operates on real time data. After the server is restarted, the Unattended Target Status Control and the Broker Status Control are empty and updated as real time data start to flow into the server. This is the default behavior.

Alternatively, it is possible to preload this controls at Server Start up. In this case the Unattended Target status and the Broker status will appear as "Unknown" until the targets and brokers have contacted the Server.

To activate the preload at Server start up set the **rc.dashboard.preload.on.startup** property to True.

A Server Restart is needed for this property to take effect.

### Trend Controls Interval and Data Points

When activating Trends Control the system selects predefine values for the rc.dashboard.trend.intervals.number and the rc.dashboard.trend.intervals.minutes properties. Those properties define how many data points are shown on the trend control and how many minutes a data point represents. Default Values when monitoring OnDemand Activity are as follows:

Property	Value	Meaning
rc.dashboard.trend.intervals.number	30	30 datapoint of 60 minutes each.
rc.dashboard.trend.intervals.minutes	60	Provides a 30 hour coverage.

Default Values when monitoring Unattended Activity are as follow:

Property	Value	Meaning
rc.dashboard.trend.intervals.number	30	30 datapoint of 2 minutes each.
rc.dashboard.trend.intervals.minutes	2 <sup>1</sup>	Provides 1-hour coverage.

To override default values, specify the desired values in `trc.properties`.

### Refreshing the Status Dashboard view

You can manually refresh the Status Dashboard by clicking the refresh icon on the page title bar.

Alternatively you can click the **Autorefresh** checkbox for a 20 seconds automatic page update.

1. The default value is the value of the `rc.unattended.heartbeat.interval.minutes` property.

# Chapter 7. Unattended Target Support

The Unattended Target Support feature allows you to take remote control sessions of targets that are connected through a broker, without the need to provide a connection code. In strict remote control terminology, an unattended target is a managed target that performs [Call Home \(on page 60\)](#) through a broker.

## Managed target

A managed target is a target that registers itself to the Remote Control server, and it contacts the Remote Control server directly (or through Gateways) to perform the call home. A controller requires a direct network connection (or through Gateways) with the target to establish a Remote Control Session. By this definition managed targets exist only within the corporate network.

## Unattended target

An unattended target is a target that registers itself to the Remote Control Server, but unlike a managed target it contacts the Remote Control Server through a Broker. A controller does not use a direct network connection with the target to establish a Remote Control Session as the session is established through the Broker. By this definition an unattended target can exist either inside or outside of the corporate network and the session can be established from either inside or outside of the corporate network.

## Types of target operating modes

The following table summarizes the major differences between the different types of target operating modes.

The term *inside* refers to the Corporate Network accessed either from the corporate facilities or via VPN. The term *outside* refers to outside of the Corporate Network.

	Managed	Unattended	ODT / Broker
<b>Components Location</b>			
Target	Inside	Inside or outside	Inside or outside
Controller Inside	Yes	Yes	Yes
Controller Outside	No	Lite Web Portal	Lite Web Portal
<b>Session Establishment</b>			
Requires User at the target system to Initiate a Session	No	No	Yes to enter the Connection Code
Require User at the target system to Accept Incoming Session	Yes or No Configurable	Yes or No Configurable	Yes or No Configurable

User / Target Group Policy	Yes	Yes	Yes
<b>Other</b>			
Server Contact	Direct	Through a Broker	Through a Broker
Server Contact Frequency	Configurable	Configurable	At Session Time

## Unattended targets guidelines

Unattended targets are useful if you need to establish a session with a target in some specific scenarios.

The following are the scenarios where the Unattended targets are useful:

- A managed target can be connected from the office, connected from home via the VPN, or connected only via the Internet. If you require a managed target to always be reachable regardless of the connection situation, you can configure that managed target as an unattended target.
- A target that permanently presents outside of the corporate network.
- A target that permanently presents inside of the corporate network and that must be reachable from outside of the corporate network.
- An Unattended Target can initiate the session in any mode. The users have to review the session permissions and confirm that the Unattended Target Active sessions are permitted in the configuration section.

From the product function prospective, there is no difference between managed targets and unattended targets. When operated within the corporate network, unattended targets provide some advantages in deployment and configuration of Remote Control Gateways.



**Note:** The initial session mode for an unattended session is set to Active. Review the session permissions and make sure that Active sessions are allowed in the configuration section. If the permission configuration does not include the Active session mode, then the initial session mode can become unpredictable when the session is established. This unpredictability is dependent on the other session permissions and the status of the unattended target connection with the server.

## Operating requirements

Unattended Target Support requires that all components (Server, Broker, Target, and Controller) are at Remote Control Fix Pack 5 (build 10.0.0.0514) or higher.

If you are upgrading from an earlier version of the Remote Control product and plan to use Unattended Targets you must upgrade in the following order:



1. Server
2. Brokers
3. Controllers

Targets can then be upgraded or installed afresh before the Unattended Mode configuration is applied.

Older targets that are not operated in Unattended Mode work with the rest of the infrastructure upgraded at Fix Pack 5 or higher.

If you do not plan to use Unattended Targets, the standard upgrade order applies depending on the Remote Control Version that you are currently using.

For security reasons, the use of pre-installed controllers is enforced when operating on Unattended Targets.

## Enable unattended target support


This topic describes how to enable Unattended Target Support.

Once the Server, the Broker, and the Controllers have been deployed, you can activate the Unattended Target Support as follows:

### Activating Unattended Target Support

To activate the Unattended Target Support feature on the Remote Control Server, complete the following steps:

1. From the Remote Control Server web interface menu, select **Admin > Edit Properties File** and then select **trc.properties**.
2. At the bottom of the page, in the **Unattended Target - Enable and configure Unattended target support** section, set the property **rc.unattended.enable** to True.
3. In the same section, select the preferred initial session mode when starting an Unattended session from the **Controller Target List**.
4. At the top of the page, click **Submit**.
5. From the Remote Control Server web interface menu, select **Admin > Reset Application**.

 **Important:** Once the server has been reset, you must restart the Broker services.

### Configuring Targets

A Managed Target is configured to operate in Unattended mode using the BigFix Remote Control Target Wizard on the BigFix Console.

If you need to deploy an Unattended Target, deploy the target as a Managed Target first and then configure it as Unattended Target using the BigFix Remote Control Target Wizard.

To configure the Target, perform the following steps:

1. Uncheck the checkbox at the top of the page to deselect all properties.
2. Select **BrokerList** and insert the list of Brokers.
3. Select **BrokerCertsUpload** and add the Brokers Certificates.
4. Configure the **UnattendedInternetAccess** to the desired value. The property `UnattendedInternetAccess` is configured to determine the mode of operation of the target. The value can be:
  - **Never**: This is the default value of the property, and it is equivalent to not specifying the property in the target configuration. If this value is set, the target operates as Managed Target. If it is configured with a **BrokerList** and **BrokerCertsUpload**, it allows you to enter the connection codes to establish a Broker Session.
  - **Always**: If this value is set, the target always operates in Unattended mode. When operating in this configuration, it is not possible to enter the connection code. In addition, the **AllowP2P** is assumed to be Never. The target connects the server only via the brokers indicated in the **BrokerList**.

When configuring the target with **UnattendedInternetAccess = Always** also consider the following values.

- Select **AllowP2P** and set it to Never.
  - Select **PortToListen** and set it to 0.
  - **Auto**: If this value is set, the target determines the operating mode (Managed or Unattended) depending on how the target reached the server.
    - The target tries to perform Call Home using the `ServerURL`. If this connection is successful, the target operates as a Managed Target.
    - If the `ServerURL` connection is not successful, the target tries to connect via the brokers in the **BrokerList**. If the connection is successful, the target operates as an Unattended Target.
5. Click **Create Configuration Task** and deploy the task to the intended targets.

## Start Unattended Target sessions

Learn how to start an Unattended Target session.

### Start Session from the Server Interface

You can start an Unattended Target session from the Server Interface, as you do for a Managed Target.

To do that, select the Unattended Target and then select **Start Session**.

### Start Session from Controller Target List

You can operate on a list of Unattended targets from the controller. This mode of operation is possible from the Server interface and from the Lite Web Portal.

#### From the Server Interface

From the Remote Control Server web interface menu select **Targets > Start Unattended Session**.

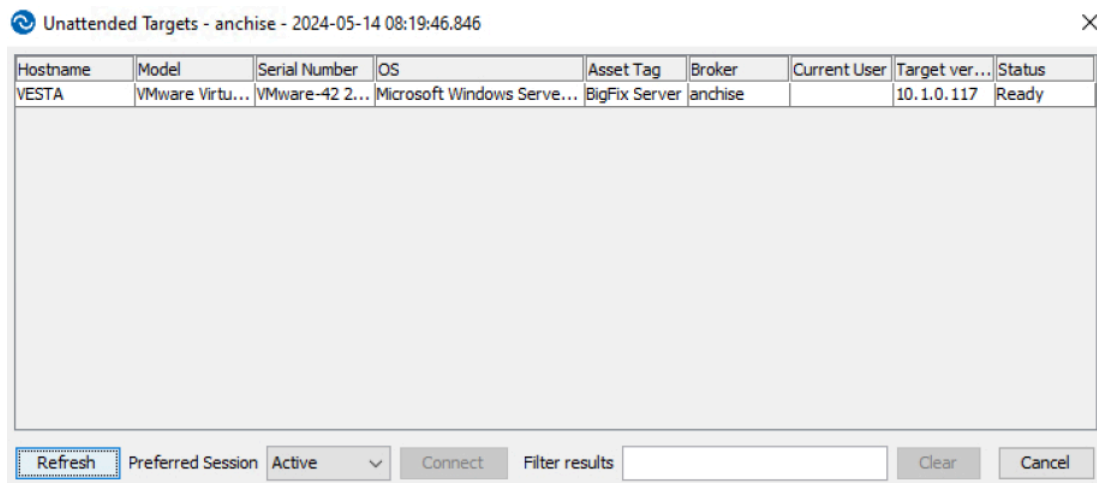
#### From the Lite Web Portal Interface

Unattended target support from the Lite Web Portal must be explicitly activated as follows:

1. From the web interface menu select **Admin > Edit Properties File**, and then select **ondemand.properties**.
2. At the bottom of the page, set the property **liteweb.portal.unattended.enable** to `True`
3. At the top of the page, click **Submit**
4. From the web interface menu, select **Admin > Reset Application**. When this support is enabled, a new tile is shown in the Lite Web Portal page.

### The Controller Target List

Once the controller is started, the Controller Target List is shown. The list shows only the targets that the user is authorized to see based on user group membership.



- The title bar shows the Broker the controller is connected to and the timestamp of the last update.
- The **Refresh** button retrieves a new list of targets from the Server.
- The **Preferred Session** permits the user to choose the session mode.
- To search the list of targets, enter text in the **Filter results** text box and press **Enter**.
- Press the **Clear** button to cancel the search and return to the full list.
- The **Cancel** button closes the Target List and Disconnects from the Controller.
- You can retrieve the list of targets again by clicking on the Controller Connect Icon after clicking **Cancel** or after a Session is established.
- To start a session, select the target and click the **Connect** button. The Connect is enabled only if the target is in Ready status.
- This target status shows the real time status of Unattended targets. The status can be:
  - **Ready** The target is ready.
  - **Offline** The target is offline.
  - **Initiating** The target is about to start a Remote Control Session.
  - **Busy** The target is in a Remote Control Session. When in session the field **Current User** shows the user that is in session with the target.

- **Unknown** The target that has not contacted the Server after a Server restart.
- **Error** The target is in error status.

## Manage the Unattended Target environment

Learn how to manage the Unattended Target environment.

### The Unattended Status Cache

The information about the Target Heartbeat and the Unattended Target Status is stored on a volatile cache on the server for performance reasons. The actual Unattended Target Status is visible from the Target Status page (after selecting the single target), from the [Deployment Status Dashboard \(on page 49\)](#) from the Server log file or from the Target List on the Controller.

The volatile nature of the cache implies that if you restart, the server starts to populate with real-time information as they are processed on the server.

You can set the `rc.dashboard.preload.on.startup` option to preload the cache at server startup. In this case, the status of the preloaded target appears as *Unknown* until the target reaches the server again.

### Call Home v/s Heartbeat

A Managed Target performs a Call Home every `rc.heartbeat_timeout` minutes.

An Unattended Target perform a Call Home every `rc.heartbeat_timeout` minutes and a Heartbeat (also named Pulse) every `rc.unattended.heartbeat.interval.minutes`.

The target asset information is updated on Call Homes. That information includes `LAST_UPDATE` time stamp, `IP_ADDRESS` LIST, `BROKER`. For an Unattended Target, this information indicates the last Call Home information.

The information about the target Heartbeat and the Unattended Target Status is stored on a volatile cache on the Server.

An Unattended Target can be recognized by the presence of a broker in the `BROKER` column of the **All Target View**.

### Heartbeat Interval and Offline Grace

An Unattended Target contacts the server every `rc.unattended.heartbeat.interval.minutes` to report its status and to check if there is any pending session request.

When you initiate a Remote Control Session with an Unattended Target, the `rc.unattended.heartbeat.interval.minutes` also indicates the maximum amount of time you need to wait before the session is established.

The target heartbeat contact is used by the server to determine the target status. The property `rc.unattended.heartbeat.offline.grace` indicates how many missing target heartbeats are allowed before the target is considered *Offline*.

## Controlling Unattended Session Timeout

It is possible to control the timeout value of the Unattended Target sessions.

When starting sessions from the **Start Session** entry from the Remote Control Server, the controller must be started within 15 minutes (the same as in standard Managed sessions). You can control this timeout value using the `rc.unattended.controller.token.minutes` property.

When operating via the target list (from the **Start Unattended Session** either via the Remote Control Server or via the Lite Web Portal), the controller is authorized to operate for 60 minutes from the initial session request. If the controller is closed, a new start session is required. You can control this timeout value using the `rc.unattended.targetlist.token.minutes` property.

To define a value for the `rc.unattended.targetlist.token.minutes`, you must consider the operating environment (either via portal or via server interface) as well as what other security feature you are planning to adopt. Using a higher timeout value requires less session restart. If [Controller UUID \(on page 63\)](#) or [Two Factor Authentication \(on page 64\)](#) is used, you must consider increasing this timeout value.

## Target Groups

Unattended Targets can be assigned to a `Target Group` during initial registration or at every `Call Home` in accordance with the same rules that apply for Managed Targets.

If you are using rules based on IP address and you have indicated `rc.tmr.at.registration`, `rc.tmr.at.every.callhome`, or `rc.tmr.at.triggered.callhomes` and the `UnattendedInternetAccess` is set to `Auto`, the target might change its group depending on target location. Review your rules and ensure the targets are assigned to the desired group.

## Using the Asset Tag

You can use the `Target Asset Tag` to add notation to a target or a group of targets to make it easier to search for targets.

You can set the Asset Tag using the **BigFix Remote Control Target Wizard** on the BigFix Console.

## Controlling Log Content

As you operate with an increasing number of targets, the log information that is produced can be impractical.

You can set the Broker log level to 1.

In addition, the following properties are available in the **Unattended Target - Log control** section of the `trc.properties` to control logging functions.

- Set `rc.unattended.log.incoming.heartbeat` to `False` to prevent every Unattended Target heartbeat to produce a log entry.
- Set `rc.unattended.log.heartbeat.trend` to `True` to produce a periodic summary in the **Server Log File** on how many heartbeats were received in the last `rc.unattended.heartbeat.interval.minutes` interval. The same information is available in graphical form from the [Deployment Status Dashboard \(on page 49\)](#).

The `rc.unattended.log.cache.report` produces a periodic summary in the [Server Log File](#) on the `Status of Targets` as known to the server. On each periodic summary, a list of targets for each status is included in the summary based on the status of the respective property in the **Unattended Target - Log cache entries at cache report** section.

## Debug Options

The following properties are available in the **Unattended Target - Tuning and debug options** section of the `trc.properties`.

You must use those properties following the indication of the HCL Support Team.

The `rc.unattended.force.guid.check` enables extensive verification of target information at Heartbeat time. This option must be used if **Targets in Error** status are noticed.

The `rc.unattended.log.timing.records` and `rc.unattended.log.timing.completed` provide processing time information on the [Server Log File](#) to collect performance information. The produced log file must be provided to the HCL Support team for investigation.

## Monitoring the Unattended System Health

When the Unattended Target Support is enabled, the [Deployment Status Dashboard \(on page 49\)](#) provides a real-time status view of the targets and broker status that is based on the `Unattended Status Cache`.

Targets when performing the Heartbeat connect to the server through all the Brokers that are listed in the `BrokerList`. The target connects the first broker that responds to the request. Operating with more than one broker hence produces a load balancing and redundancy effect.

## Security Features for the Unattended Targets

The following table shows a summary of the security features that are available when operating on Unattended Targets in different usage scenarios.

**Prerequisite:** Security features require Server, Controller, and Broker to be at version 10.0.0.0518 or higher.

Security Feature	Start Session from Server	Target List from Server	Target List form Portal
<a href="#">Controller Instance ID (on page 63)</a>	Yes	Yes	Yes
<a href="#">Controller UUID (on page 63)</a>	N/A	Configurable	Configurable
<a href="#">Two Factor Authentication via Mail (on page 64)</a>	N/A	N/A	Configurable

Where:

- **Yes** means the security feature is available and always effective.
- **N/A** means the security feature is not available in the indicated usage scenario.

- **Configurable** means the feature is not activated by default.
  - When Operating on Unattended Target List via the Lite Web Portal (with **liteweb.portal.unattended.enable** set to true) at least one Configurable security feature must be defined. If none is selected the Server will enforce the Controller UUID verification.

## The Controller Instance ID

This feature is always enabled when operating on Unattended Targets. Every time the Controller is started, controller generates a temporary and unique Controller Instance ID that is bound to the session being established. Only one Controller Instance ID can be bound to a session. Subsequent attempts to re-initiate the same session by re-starting the controller throws the error “the Controller Instance ID is invalid for the session.” The Controller Instance ID is not visible to the user.

## The Controller UUID

When enabled, this function provides an additional level of authorization for operating on the Unattended Target Lists from the Controller.

Each controller provides a unique Universally Unique Identifier, named Controller UUID.

When this security feature is enabled, the Controller UUID of the Controller that is about to start the session must be listed among the authorized Controller UUID for the user.

To activate the feature on the Remote Control Server:

1. From the web interface menu select **Admin > Edit Properties File**, and then select **trc.properties**
2. At the bottom of the page, in the **Unattended Target - Security Options** section, set the property **rc.unattended.check.controller.uuid** to True.
3. At the top of the page click **Submit**.
4. From the web interface menu select **Admin > Reset Application**

To find the Controller UUID in the controller:

1. From the Controller menu bar select the **Configure Controller > Configure**.
2. At the bottom of the page, you find the **Controller UUID**. Copy this value and use it to update your user information on the Server Interface or provide this value to your system administrator.



**Note:** This field appears editable to allow copying, but do not edit it. If the field is edited it has no effect.

To update the user detail on the Server Interface:

1. As an Administrator user from **All Users list**, select **Edit User**.
2. A User can edit its own information from the **My Details** option available from the User Icon on the web interface menu.

3. Insert the Controller UUID in the **User Controller UUIDs:** field. More than one Controller UUID can be added using the “,” separator.
4. Click **Submit** at the bottom of the page.

### Additional Options

- The generation of the Controller UUID is based on unique machine information.
- Setting the property `rc.unattended.force.customized.uuid` to `True` introduces a personal pass code element in the computation of the UUID.
- The personal or custom pass code is user defined.
- When the controller is started, the user is asked to input a personal pass code that is used in the computation of the Controller UUID along with other elements. Every time the controller is started, the user must insert the same personal pass code to compute the same Controller UUID.
- The same personal passcode used in different controller machines creates different Controller UUID.

## Two Factor Authentication via Mail

This feature is only available when operating from the Lite Web Portal, and it requires the configuration of an SMTP server in the Remote Control Server.

When the user asks to initiate Unattended Remote Control sessions from the Lite Web Portal, an email with a One-Time Authentication Code is sent to the User email address. Once the controller is started, the user is asked to insert connection code received by mail. Activate the feature on the Remote Control Server.

### To activate the feature:

1. From the web interface menu select **Admin > Edit Properties File**, and then select `trc.properties`
2. At the bottom of the page, in the **Unattended Target - Enable two factor authentication for Lite Web Portal Access**, set the property `rc.unattended.twofactors.mail.active` to `True`.
3. At the top of the page click **Submit**.
4. From the web interface menu, select **Admin > Reset Application**

#### Additional Options:

- The length of the generated Authentication Code is controlled by the `broker.code.length` property.
- You can customize the validity of the token by setting `rc.unattended.twofactors.token.minutes`.



# Chapter 8. Unlocking user accounts

When a user account is locked, you can unlock the account by using the **Unlock locked userid** feature.

When a user logs on to the Remote Control server with an incorrect password, their user account is locked if the number of failed logon attempts exceeds the limit. The value that is assigned to the **account.lockout** property in the `trc.properties` file defines the limit. For more information about this property, see [trc.properties \(on page 216\)](#).

To unlock the user account for one or more users, complete the following steps:

1. Choose the appropriate method to unlock users.
  - a. To unlock users by using the search utility.
    - Click **Users > Search**.
    - Enter the user information to be used in the search.
    - Click **Submit**.
    - Select the user and go to step 2 ([on page 65](#)).
  - b. To unlock users by using the **All Users** report.
    - Click **Users > All users**.
    - Select the users.
2. Choose the appropriate action to unlock the users.
  - Click **Users > Unlock locked userid**.
  - Select **Unlock locked userid** from the Action list on the left.

The user account for the selected users is unlocked and they are able to make another logon attempt.

If the **account.lockout** property is enabled in the `trc.properties` file, the following extra user information is also displayed on the **Change details** window. For more information about editing user details, see [Modifying user details \(on page 82\)](#).

### Last failed logon

Shows the date and time of the last failed logon attempt by this user.

### Failed logons

Shows the number of failed logons since the last successful logon or since the user's account was unlocked by an administrator.

### Account locked

Displays Yes or No depending on whether the user's account is locked because the limit of consecutive failed logons is reached. The limit is defined by the **account.lockout** property in the `trc.properties` file.

# Chapter 9. Manage targets and target groups

In the Remote Control system, targets are endpoints that you install the target component on. The target component identifies the computers to the BigFix® Remote Control Server to receive connection requests, and pass information to and from the server. For more information about installing the target component, see the *BigFix® Remote Control Installation Guide*.

The targets periodically report back to the BigFix® Remote Control Server to indicate to the server that they are still active and, in particular, when their state changes. For example, when a user logs on, when a remote control session is taking place, or when the system powers on or shuts down.

When a target is first installed and made known to the server, it is automatically assigned to the default target group and given a default set of policies. You can decide which set of policies and permissions must be assigned to the target by making it a member of any relevant target groups. Target groups are created and assigned specific permissions that are combined with user group permissions to determine what the target users can do during remote control sessions.



**Note:** Only a user with Administrator authority sees the **Target Groups** menu.

## Manage Targets

The following actions are available for Administrators to use on targets. For more information about the features that all users can use on targets, see the *BigFix® Remote Control Console User's Guide*

### Delete Target

Use this feature to delete one or more targets from the BigFix® Remote Control Server.

### Manage Group Membership

Use this feature to add a target to a target group.

## Deleting a target

You can remove targets from the BigFix® Remote Control Server by using the **Delete target** option.

- If the target is still active and the BigFix® Remote Control Target service is running, it can report back to the server again. Its details are uploaded to the server, to be displayed in the **All Targets** list.
- If it does report back, any policies or permissions that were set previously are reset and it is no longer a member of any previously assigned target groups.

If you remove the target Software or stop the **Remote Control - Target** service on the target, prevents it from uploading details again.

To delete one or more targets complete the following steps:

1. Choose the appropriate method to delete targets:
  - a. To delete a target by searching for targets, complete the following steps:
    - i. Click **Targets > Search**
    - ii. In the search field, enter information about the target.
 

For example : serial number, computer name, model number, IP address
    - iii. Click **Submit**.
    - iv. Select the targets from the list and go to step 2 ([on page 67](#))
  - b. To delete a target by using the **All Targets** report, complete the following steps:
    - i. Click **Targets > All targets**.
    - ii. The list of all defined targets is displayed.
    - iii. Select the targets.
2. Choose the appropriate action to delete the target.
  - From the **Targets** menu, select **Delete target**.
  - Select **Delete target** from the Actions list on the left.
3. On the **Confirm deletion** window, click **Submit**.

The targets are deleted. Use the **delete.target.auth** property in the `trc.properties` file to change the user authority that is required to use the delete option. For more information about this property, see [Editing the properties files \(on page 215\)](#).

## Assign targets to target groups

When targets are registered in the server, they are assigned to target groups. The policies and permissions that are set for the groups are used to determine what the target members can or cannot do during a remote control session.

For more information about creating target groups, see [Creating target groups](#). For more information about how policies and permissions are granted for remote control sessions, see [How policies are determined for a remote control session](#).

Targets can then be assigned to target groups using the following methods.

### The Default Target Group

By default the default target group name is **DefaultTargetGroup**. You can change the default target group name changing the **default.group.name** property in the `trc.properties` file on the server.

The target is assigned to the default target group when the other available methods are not used or when they do not assign the target to any group.

### The Manage group membership Feature

You can use the **Manage group membership** feature to add targets to target groups thus making them members of the selected groups. This action must be performed after a new target is made known to the server.

## The Target Group Label Parameter

You can also assign targets to target groups by using the **GroupLabel** target parameter thus letting the target define the target groups it belongs to. This assignment can occur during initial target registration or during subsequent target triggered callhomes. To enable the GroupLabel processing during initial target registration set the **allow.target.group.override** to Yes. To enable the GroupLabel processing during triggered call homes the **allow.override.at.triggered.callhomes** to Yes. Both properties are in the trc.properties file on the server.

When a managed target deployment occurs from the BigFix console it is not possible to define the GroupLabel parameter. In this case you can:

- Deploy the target as Peer to Peer and then use the Target Configuration Wizard and make the target managed setting the GroupLabel as desired. In this case set target.group.override to Yes.
- The default GroupLabel value "DefaultTargetGroup" indicates that the Default Target Group as defined on the server is to be used. However if the GroupLabel property includes the DefaultTargetGroup in a list of groups like "DefaultTargetGroup;MyOtherGroup", the DefaultTargetGroup will be considered as a target group.
- Deploy the target as Managed and then use the Target Configuration Wizard to set the GroupLabel as desired. In this case set allow.override.at.triggered.callhomes to Yes.



### Note:

- It is not possible to remove a target group membership by removing the target group from the GroupLabel parameter even if the allow.override.at.triggered.callhomes is set to Yes. Use the **Manage group membership** feature to change the Target Group assignment in this case.
- You could leverage BigFix Relevance language as in this example to define the target group membership.

```
If {distinguished name of local computer of active directory contains
    "OU=Group1,DC=PROD,DC=HCLPNP"}
    "GroupLabel"="TESTGroup1"
else
    "GroupLabel"="DefaultGroup;OtherGroup"
Endif
```

## The Target Membership Rules

You can also assign targets to target groups by creating **target membership rules**. The rules can be used to automatically assign targets to specific groups when they contact the Remote Control server. For more information about target membership rules, see [Use rules to define target membership](#).



**Note:** If you define rules and the target group override function is also enabled, the target is assigned to the target groups that are defined for both options.

## Assigning a target to target groups

After a target has registered with the BigFix® Remote Control Server, you can assign it to one or more target groups. When the target takes part in a remote control session, the policies and permissions that are defined for these groups are considered when the final session policies are derived. For more information about how policies are set for a session, see [How policies are determined for a remote control session \(on page 115\)](#).

To add a target to one or more target groups, complete the following steps:

1. Choose the appropriate step to select a target:
  - a. Select the target by using the search utility
    - Click **Targets > Search**
    - In the search field, type in some specific or non-specific information about the target
 

for example : serial number, computer name, model number, IP address
    - Click **Submit**.
    - Select the target.
  - b. Select the target by using the **All targets** report.
    - i. Click **Targets >All targets**.
    - ii. Select a target.
2. Select **Manage Group Membership** from the **Actions** list on the left.
3. From the group list, select the target groups that you want to add the target to.
 

Any groups with a + sign can be expanded to select sub groups also.
4. Click **Submit**.

The target is now a member of the selected target groups.

## Assigning multiple targets to target groups

You can assign multiple targets to target groups and also change their current group membership.

For example, targets used by the one department might need to be in the same target group. You can select all of these targets and assign them to the relevant target group or groups at the same time, which is more efficient than assigning each target individually.

Assign multiple targets to target groups by using one of the following options that can be used when you define the group tree hierarchy.

**replace**

The selected targets become members of the group or groups that you select within manage group membership. Their membership to any other groups is replaced by the target groups that are selected here.

For example: Target1 and target2 are members of targetgroup1 and targetgroup2. Select these targets from the target list and then select **Manage Group Membership**. From the list of groups that are displayed, select targetgroup3 and the replace option. Target1 and target2 are no longer members of targetgroup1 or targetgroup2 and are only members of targetgroup3.

#### **add**

The selected targets are now also members of the group or groups that you select within manage group membership.

For example: In the example that is used in the replace option, if targetgroup3 is selected with the add option, target1 and target2 are now members of targetgroup1, targetgroup2, and targetgroup3.

#### **delete**

The selected targets are removed from the groups that you select within manage group membership.

For example: Target1 and target2 are members of targetgroup1 and targetgroup2. Select these targets from the target list and then select **Manage Group Membership**. Select targetgroup2 from the group list in manage group membership along with the delete option. Target1 and target2 are still members of targetgroup1 but are no longer members of targetgroup2.

---

To assign multiple targets to one or more target groups, complete the following steps:

1. Choose the appropriate method for selecting the targets
  - a. Select the targets by using the search utility
    - Select **Targets > Search**.
    - Type in some relevant information for retrieving the target data.
    - Click **Submit**.
    - Select the targets.
  - b. Select the targets by using the **All targets** report.
    - Click **Targets > All targets**.
    - Select the relevant targets from the list.
2. Select **Manage Group Membership** from the **Actions** list on the left.
3. From the group list, select the relevant target groups.

Any groups with a + sign can be expanded to select sub groups also.
4. Select one of the following options:
  - **replace current group membership**
  - **add to current group membership**
  - **delete from current group membership**
5. Click **Submit**.

The group membership for the selected targets is defined by the option that is selected in step 4 (on page 70).

## Creating target groups

Use target groups to assign similar policies and permissions to multiple targets. The policies are effective during remote control sessions.

For more information about starting remote control sessions, see the *BigFix® Remote Control Installation Guide*. When a new target is defined in the BigFix® Remote Control Server, it automatically becomes a member of the default target group. However, the Administrator must assign the target to relevant target groups.

A target can be a member of multiple groups. Policies and permissions are defined for a target group when it is created. A permissions link must be created between the target group and a user group. The policies and permissions that are defined in the permission link and any other links that are defined in the group hierarchy, are used to derive the set of policies for the session. For more information about deriving session policies, see [How policies are determined for a remote control session \(on page 115\)](#).

To create target groups, complete the following steps:

1. Click **Target Groups > New Target group**.  
The **Edit Target Group** window is displayed. Define the target group name and select the policies and permissions that are relevant for the target group.
2. Type in a name for the target group,  
For example, *testtargets*.
3. **Optional:** Type in a description for the target group.
4. For **Heartbeat interval**, type in the number of minutes that the target members of this group wait before they contact the BigFix® Remote Control Server.
5. Use **Lock target on disconnect** to determine whether the target computers that belong to this target group are locked automatically when a remote control session ends.

### Set to Yes


The target is locked when a remote control session with it ends.

### Set to No


The target is not locked when a remote control session with it ends.

6. Select the value for **Automatically reset the console after a Remote Desktop console session:**

Value	Description
Never	Do not apply the workaround.
At session start	Reset the Windows® session when a remote control session is started.


Value	Description
	 <b>Note:</b> The Windows® session takes a couple of minutes to initialize and the controller user sees a blank desktop until the initialization is complete.
After console is logged out	Reset the Windows® session when the Remote Desktop user logs out.

For more information about this attribute, see [Gray screen on a Windows 2003 system \(on page 404\)](#) .

 **Note:** The attribute is not set to any value by default.

7. Select the value for **Allow Remote Control connections to Remote Desktop sessions:**

Value	Description
No	Does not allow the controller to connect to a running Remote Desktop session in the target. The default value is no.
Yes	The controller follows the active session when connecting to a target, even if the active session is a Remote Desktop session.
Not set	Uses the generic value defined in the <code>follow.active-session</code> property located in the <code>trc.properties</code> file. The default value is no.

 **Note:** This feature is available in Remote Control v9.1.2 IF0002 and later versions.

8. Select the permission settings for the target group.

The settings are classed as the standard or normal set for the group. On initial display, the screen shows the default values for the permissions that you can accept or change to your own requirements

The Permission settings for the group can be defined in the following ways:

- To **accept the given default** permission settings, click **Submit**.
- To **assign an already defined set** of standard or normal permissions, select the template name from the pull-down
  - The Policy list is populated with the values saved for the selected permission set.
  - Click **Submit**.



- To **define a new standard set** of permissions complete the following steps
  - a. Click **Edit Settings**, the policy values are now available for selection.
  - b. For each Policy in the list, select the permission or enter a value



**Note:** For more information about server policies, see [Server session policies \(on page 95\)](#).

#### **Yes**

The policy is valid for members of this target group and therefore its value is considered when the permissions are combining in Manage Permissions.

#### **No**

The policy is not valid for members of this target group but its value is also considered when the permissions are combined in Manage Permissions.

#### **Not Set**

No value is set and therefore it is not considered when the permissions are combined in Manage Permissions because this option is overridden by all others. For more information about how permissions are assigned, see [How policies are determined for a remote control session \(on page 115\)](#).

- c. The new permissions set can be saved in the following ways:
  - **Save existing template**

Select this option to save the changes to the template name that is displayed in the template list.
  - **Save as new template named**

Select this option to save the changes to a new template.
- d. Click **Submit**.

## Viewing Target Groups

When target groups are created, you can view a list of all defined groups. To view all target groups click **Target Groups > All target groups**.

The list of all defined Target Groups is displayed.

## Manage Target Groups

After you create target groups, you can use the following features to manage the target groups.

- View the members of a target group.
- Delete target groups.

- Change the details for a target group.
- Remove members from a target group.
- Set permissions for a target group.
- Assign target groups to other target groups.
- Search for target groups.

## Viewing the members of a target group

To see which targets are assigned to a target group, use the List Members function.

To list all members of a selected target group, complete the following steps:

1. Choose the appropriate method for selecting a target group.
  - a. Select the target group by using the search utility.
    - Click **Target Groups > Search**.
    - Enter relevant information to find the target group and click **Submit**.
    - Select the target group.
  - b. Select the target group by using the **All Target groups** report.
    - Click **Target groups > All target groups**.
    - Select the target group.
2. Select **List members** from the Action list on the left.

The list of members for the selected target group is displayed, showing target groups and targets that are members of the selected group.

## Deleting a target group

You can remove target groups that are no longer required by using the **Delete target group** function.

To delete one or more target groups, complete the following steps:

1. Choose the appropriate method for selecting the groups.
  - a. Select a group by using the search utility.
    - Click **Target Groups > Search**.
    - Enter relevant information to find the target group and click **Submit**.
    - Select the target group.
  - b. Select a group by using the **All Target groups** report.
    - Click **Target groups > All Target groups**.
    - Select the target groups.
2. Select **Delete Group** from the **Actions** list on the left.
3. On the **Confirm deletion screen** click **Submit**.

The target groups are deleted.

## Changing the details for a target group

After you create a target group, you can change the details or policies and values for the group by using the **Edit Group** function.



**Note:** If the policy values are changed for a group, the new policies are valid for this group only when any new permissions links, between this target group and a user group, are created in manage permissions. Any existing links that are already defined for the target group, keep the policy values that were set for the group when the link was created. For more information about creating permissions links, see [How policies are determined for a remote control session \(on page 115\)](#).

To edit a target groups details, complete the following steps:

1. Choose the appropriate method for selecting the group.
  - a. Select the group by using the search utility.
    - Click **Target Groups > Search**.
    - Enter relevant information to find the target group and click **Submit**.
    - Select the target group.
  - b. Select the group by using the **All Target groups** report.
    - Click **Target groups > All target groups**.
    - Select the target group.
2. Select **Edit Group** from the **Actions** list on the left.
3. Change the relevant information. For more information about the requirements for target groups, see [Creating target groups \(on page 71\)](#).
4. Click **Submit**.

The updated groups details are saved.

## Remove members from a target group

After targets or target groups are assigned to target groups, you can remove them from the group.

Removing members from a target group can be done in two ways.

- Remove one member from a Target Group.
- Remove all members from a Target group.

### Removing one member from a target group

To remove one member from a target group, complete the following steps:

1. Choose the appropriate method for selecting a member:

a. Select the member by using the search utility.

To select a target member.

- Click **Targets > Search**
- In the search field, type in some specific or non-specific information about the target

for example : serial number, computer name, model number, IP address

- Click **Submit**.
- Select the target.

To select a target group member.

- Click **Target Groups > Search**.
- Enter relevant information to find the target group and click **Submit**.
- Select the target group.

b. Select the member by using a report.

To select a target member.

- Click **Targets > All targets**.
- Select the target.

To select a target group member.

- Click **Target Groups > All Targets Groups**.
- Select the target group.

2. Select **Manage Group Membership** from the **Actions** list on the left.
3. Clear the check box of the groups that you want to remove the target or target group from.
4. Click **Submit**.

The target is no longer a member of the selected target group.



**Note:** You can confirm the removal by selecting the **List Members** option for the selected target group. For more information, see [Viewing the members of a target group \(on page 74\)](#).

## Removing all members from a target group

To remove all members from a target group, complete the following steps:

1. Choose the appropriate method for selecting the target group.

a. Select the group by using the search utility.

- Click **Target Groups > Search**.
- Enter relevant information to find the target group and click **Submit**.
- Select the target group.

- b. Select the group by using the **All target groups** report.
  - Click **Target groups > All target groups**.
  - Select the target group.
2. Select **Remove all members** from the **Actions** list on the left.
3. Click **Submit** to confirm.

All members are removed from the selected target group.



**Note:** You can confirm the removal by selecting the **List Members** option for the selected target group. For more information, see [Viewing the members of a target group \(on page 74\)](#).

## Assigning target groups to other target groups.

Use the **Manage Group Membership** function to assign target groups to other target groups thus creating a group hierarchy. Target groups are assigned the permissions and policies of the direct target groups they are a member of. These permissions are known as their standard or normal set of permissions. For more information about how policies and permissions are granted by the Policy Engine, see [How policies are determined for a remote control session \(on page 115\)](#).

To add target groups to target groups, complete the following steps:

1. Choose the appropriate method for displaying the target groups.
  - a. Select the group by using the search utility.
    - Click **Target Groups > Search**.
    - Enter relevant information to find the target group and click **Submit**.
    - Select the target group.
  - b. Select the group by using the **All target groups** report.
    - Click **Target groups > All target groups**.
    - Select the target group.
2. Select **Manage Group Membership** from the **Actions** list on the left.
3. Select the target groups that you want to add the target groups to. Some target groups in the list might have a plus sign in front of their name which can be expanded to show other target groups. If you selected multiple target groups in step 1 ([on page 77](#)), select one of the following options.
  - **replace current group membership**
  - **add to current group membership**
  - **delete from current group membership**

For more information about the options, see [Assigning multiple targets to target groups \(on page 69\)](#).
4. Click **Submit**.

The target groups are assigned to the selected target groups.

## Set permissions for a target group

Use the manage permissions option to create a permissions link between a user group and a target group. This link defines the policies and permissions that are granted in a remote control session between user and target members of these groups. For more information about this function and how the policies and permissions are determined for a remote control session, see [How policies are determined for a remote control session \(on page 115\)](#).

## Searching for target groups

You can use the **Search** utility to find specific target groups or find a target group by using non-specific information. To search for a target group, complete the following steps:

1. Click **Target Groups > Search**.

Enter the target group information in the input field. You can enter all or part of the target group name, or description that is associated with the target group. For the quickest search, type the target group name into the **Search Target groups** field. Otherwise, type part of the name or description.

2. Click **Submit**.

- If any matching target groups are found, the following information is displayed
  - If the target group name is entered, the details for that target group are displayed.
  - If non-specific information is entered, a list of any target groups with this information as part of their details is displayed.



**Note:** The information that is entered is not case-sensitive - Test matches with test.

- If no matching target groups are found, a message is displayed and the target group list is blank.



**Note:** If nothing is entered in the input field and you click **Submit**. The list of all target groups is displayed.

## Cleanup non-reporting targets

As the number of targets present in the database is a factor to determine license compliance, it is important to clean up the database periodically and remove non-reporting targets.

Remote Control automatically removes offline targets from the database. By default, the cleanup process runs every 24 hours. Cleanup is hooked to `dbcleaner` process and controlled by the `target.offline.max.age` property in `trc.properties`. With this property, you can configure the target cleanup to run automatically or indicate for how long a given offline target can be kept in the database.

When the value is set to 0, no offline target cleanup is performed. The properties indicate in days for how long a target that is no longer calling home is kept in the database.

If you want to perform automatic offline target cleanup specify a value that suites your deployment.

# Chapter 10. Manage users and user groups

BigFix® Remote Control Server is designed to accommodate three types of user authorities: user, super user, and administrator. Various BigFix® Remote Control Server functions can be carried out by each user account type. The administrator has the most comprehensive privileges.

## User account authorities and the functions available to each account

Three types of user accounts can be created in the Remote Control server UI. The user accounts are user, super user, and administrator.

The administrator account has the most authority. Administrators can do more advanced tasks. All types of authority can take part in remote control sessions, taking over and controlling target systems and are known as controller users. A user with administrator authority can also access server admin functions and is known as a Server Admin User.

The following table illustrates each user account and highlights the authority that is given to each account.

User Account	Types of functions
<b>User</b>	<p>The most limited account. A user with user authority can do the following actions:</p> <ul style="list-style-type: none"><li>• Log on to the web application.</li><li>• View all targets available for control.</li><li>• Create or view lists of favorite targets.</li><li>• Start a remote control session.</li><li>• View target status or information.</li><li>• View their own user and group details.</li><li>• View information for<ul style="list-style-type: none"><li>◦ Sessions that they started. For example, session history, session details, recording details, audit logs.</li><li>◦ Defined groups.</li><li>◦ Recently accessed targets.</li></ul></li><li>• Search for targets.</li></ul>
<b>SuperUser</b> (User+)	<p>Can do the same tasks as a user and also more advanced functions, such as generating specialized reports.</p> <p>A user with SuperUser authority can do the following extra actions:</p> <ul style="list-style-type: none"><li>• Create and run various reports about users, sessions, targets, and server.</li></ul> <p>However, a SuperUser is limited to viewing their own user details only. They are also limited to viewing the session details only for sessions that they started.</p>

User Account	Types of functions
<b>Administrator</b> (User +, Super User+)	<p>Can do the same tasks as a user and super user and also more advanced functions. Unlike the user and super user, they are not limited to just viewing their own details but can view details for all users. Also, responsible for maintaining and modifying user and target groups and for managing permissions that are granted to those groups. A user with administrator authority can do the following extra actions:</p> <ul style="list-style-type: none"> <li>• Edit and delete targets.</li> <li>• Create, delete, and manage users.</li> <li>• Create, delete, and manage user groups.</li> <li>• Create, delete, and manage target groups.</li> <li>• Create and run various reports on users, sessions, targets, and server.</li> <li>• Various types of data import. For example, from LDAP or by using import templates</li> <li>• Property file editing.</li> <li>• Search for targets and users.</li> <li>• View the application log and server status.</li> </ul>

## Creating user accounts

To create a new user, complete the following steps:

1. Click **Users > New**

The **Add User** screen is displayed.



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

2. Type in the relevant information for the new user.



**Note:** The fields that are marked with a star are mandatory fields.

### User ID

Type in a unique ID for the user.

### Email address

Type in a valid email address for the user.

### Forename

Type in a given name for the user.

### Surname



Type in a surname for the user.

### Password

Type in a unique password that conforms to your defined password rules and then retype the password for confirmation. Password rules are defined in the `trc.properties` file. For more information about the file, see [trc.properties \(on page 216\)](#).



**Note:** The password fields are not available when LDAP authentication is enabled.

3. From the Authority list, select the authority level to assign to the new user. For more information about user account authorities, see [User account authorities and the functions available to each account \(on page 79\)](#).
4. Select the groups that the new user is a member of.
5. Click **Submit**.

The user details are saved.

## Viewing user accounts

After user accounts are created, you can view the list of all users.

To view all users click **Users > All Users**.

The **All Users** pane displays the list of users who are defined in the system.

## Manage user accounts

After you create users you can use the following features to manage the users.

- Set user account privileges.
- Modify user details.
- Remove users.
- Unlock user accounts.
- View a list of sessions by a user.
- Search for users.

## Setting user account privileges

As an administrator you can set the authority for other user accounts. The privileges that are given to a user depend on the operations the user needs to accomplish. For information about the types of user accounts and the functions that are associated with each account, see [User account authorities and the functions available to each account \(on page 79\)](#).

To set the authority level of a user account, complete the following steps:

1. Choose the appropriate method for displaying the user.
  - a. To select the user by using the search utility.
    - i. Click **Users > Search**.
    - ii. The Search User screen is displayed
    - iii. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.
    - iv. Click **Submit**.
  - 5) Select the user.
  - b. To select the user by using the **All User** report.
    - Click **Users > All users**
    - Select the user.
2. Select **Edit User** from the **Actions** list on the left.
3. From the **Authority** list, select the authority level to assign to the account.
4. Click **Submit**.

## Modifying user details

After you create a user, you can modify the users details. To change the details, select the user from the **All Users Report** or by using the search utility. Use the **Edit user** option to make the required changes. If many users are defined in the system, you can search to find a user more quickly.

To modify a users detail, complete the following steps:

1. Choose the appropriate method for displaying the user.
  - a. To select a user by using the search utility.
    - i. Click **Users > Search**.
    - ii. The Search User screen is displayed
    - iii. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.
    - iv. Click **Submit**.
  - 5) Select the user.
  - b. To select the user by using the **All User** report.
    - Click **Users > All users**
    - Select the user.
2. Select **Edit User** from the **Actions** list on the left.



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

### 3. Change the relevant information

For more information about the requirements for the **Edit Details** screen, see [Creating user accounts \(on page 80\)](#). The following extra user information is also displayed if the **account.lockout** property in the `trc.properties` file is enabled.

#### Last failed logon

Shows the date and time of the last failed logon attempt by this user.

#### Failed logons

Shows the number of failed logon attempts made by the user.



**Note:** If this user account was previously locked due to the number of allowed failed logon attempts being exceeded, the failed logons number denotes the number of failed attempts since the account was unlocked.

#### Account locked

Displays **Yes** or **No**. If set to Yes, the users account is locked because the limit of consecutive failed logons is reached. The limit is defined by the **account.lockout** property in the `trc.properties` file.



**Note:** The User ID is unique and therefore cannot be changed.

### 4. Click **Submit**

The amended user details are saved.

## Removing users

After users are created, you can remove them if they are no longer required. Use the **Delete user** function to remove them. Use the search utility for a quicker search, if there are many users in the database.

To remove one or more users, complete the following steps:

1. Choose the appropriate method for displaying the users.
  - a. To remove users by using the search utility.
    - i. Click **Users > Search**.
    - ii. The Search User screen is displayed

- iii. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.
  - iv. Click **Submit**.
- 5) Select the users.
- b. To select users by using the **All Users** report.
    - Click **Users > All users**.
    - Select the users.
2. Select **Delete User** from the **Actions** list on the left.
  3. On the **Confirm deletion screen** click **Submit**.

The users are deleted.

## Unlocking user accounts

When a user logs on to Remote Control with an incorrect password, their user account is locked if the number of failed logon attempts is exceeded. The limit is determined by the value that is assigned to the **account.lockout** property in the `trc.properties` file. For more information about the property, see [trc.properties \(on page 216\)](#). After the user account is locked, you can unlock the account by using the **Unlock locked userid** function.

To unlock the user account for one or more users, complete the following steps:

1. Choose the appropriate method for selecting the users.
  - a. To unlock users by using the search utility.
    - i. Click **Users > Search**.
    - ii. The Search User screen is displayed
    - iii. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.
    - iv. Click **Submit**.
  - 5) Select the users.
  - b. To select the user by using the **All User** report.
    - Click **Users > All users**
    - Select the user.
2. Select **Unlock locked userid** from the **Actions** list on the left.

The selected users are unlocked and they are able to log on.

## Viewing a list of previous sessions established by a user

You can view a list of all previous sessions for one or more selected users by using the **Session history** function.

To view a list of previously established sessions by specific users, complete the following steps:

1. Choose the appropriate method for displaying the users.
  - a. To select a user by using the search utility
    - i. Click **Users > Search**.
    - ii. The Search User screen is displayed
    - iii. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.
    - iv. Click **Submit**.
  - 5) Select the user.
  - b. To select a user or users by using the **All Users** report.
    - Click **Users > All users**.
    - Select the required users.
2. Select **Session history** from the **Actions** list on the left.

The **Session History** screen displays the sessions by the selected users. The most recent session is first in the list.

## Searching for users

You can use search for users and view a summary list in the search results. To search for a user, complete the following steps.

1. Click **Users > Search**.
  2. The Search User screen is displayed
  3. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.
  4. Click **Submit**.
- Any users that match the search criteria are shown. To view the details for any of the users, click their name in the search results.
    - If the email address was entered, the summary details for that user are shown.
    - If non-specific information was entered, a list of any users with this information as part of their details is displayed. For example, if you typed Scot, a list of users with Scot somewhere in their details is listed.

```
Users with Forename - Scot
Email - ascot@example.com
```



**Note:** The information that is entered is not case-sensitive. Scot can also match with scot.

- If no matching users are found, a message is displayed and the user list is blank

## Creating user groups

You can create groups of users in BigFix® Remote Control Server. User groups are used for grouping users to give them the same permissions and access during an Remote Control, remote control session.

For more information about remote control sessions, see the *BigFix® Remote Control Controller User's Guide*. When you create a new user they automatically become a member of the DefaultGroup. You can also assign the user to other user groups.



### Note:

1. A user can be a member of multiple groups.
2. The policies and permissions that you select when you create a user group are not the set of policies that are applied when a member of the group starts a session. You must also create a permissions link between the user group and a target group. For more information about policies and permissions for a session, see [How policies are determined for a remote control session \(on page 115\)](#).

To create a user group, complete the following steps:

1. Click **User Groups > New User group**
2. Type in a name for the user group.
3. **Optional:** Type in a description for the user group.
4. Select the permission settings for the user group.

These settings are classed as the standard or normal set for the group. The default values for the permissions are displayed. Accept or change the permissions to your own requirements.

You can define the permission settings for a group in various ways.

- To **accept the given default** permission settings click **Submit**.
- To **assign an already defined set** of standard or normal permissions, select the template name from the pull down.
  - The policy list is populated with the selected permission set values.
  - Click **Submit**.
- To **define a new standard set** of permissions:
  - a. Click **Edit Settings**.
  - b. For each policy in the list, select the relevant permission or enter a value.



**Note:** For more information about the policy definitions and default and possible values for the policies, see [Server session policies \(on page 95\)](#).

### Select Yes.

This policy is valid for members of this user group. Therefore, its value is considered when the permissions are combined in **Manage Permissions**.

**Select No.**

This policy is not valid for members of this user group. However, its value is also considered when the permissions are combined in **Manage Permissions**.

**Select Not Set.**

No value is set. Therefore, its value is not considered when the permissions are combined in **Manage Permissions**. For more information about how permissions are assigned, see [How policies are determined for a remote control session \(on page 115\)](#).

c. You can save the new permissions set in multiple ways.

- **Save existing template**

Select this option if you want to save the changes to the template name that is displayed in the template list.

- **Save as new template named**

Select this option if you want to save the changes to a new template. Enter a name for the new template.

d. Click **Submit**.

## Assign users to groups

When user groups are created, you can add users to the groups in multiple ways.

- Assign the user to a group when you create the user.
- Select one or more users and use the **Manage Group Membership** option.

### Assigning a user to a group when you create the user

When you create a new user, a list of all user groups is displayed on the **Add user** screen. You can select the groups that the new user must be made a member of. For more information about creating users, see [Creating user accounts \(on page 80\)](#).

### Assigning a user to user groups

To add a user to user groups complete the following steps:

1. Choose the appropriate method for displaying the user.
  - a. Select the user by using the search utility.
    - i. Click **Users > Search**.
    - ii. The Search User screen is displayed

iii. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.

iv. Click **Submit**.

5) Select the user.

b. Select the user by using the **All Users** report.

- Click **Users > All users**.
- Select the user.

2. Select **Manage Group Membership** from the **Actions** list on the left.

3. Select the user groups that the user must be assigned to.

Any groups with a + sign can be expanded to select sub groups also.

4. Click **Submit**.

The user is a member of the selected groups.

## Assigning multiple users to user groups

You can assign multiple users to user groups. Users who work in the same department can be in the same user group. You can select all of the users and assign them to the relevant user groups at the same time, which is more efficient than assigning each user individually. Assign multiple users to user groups by using one of the following options when you define the group tree hierarchy.

### replace

The selected users become members of the groups you select within manage group membership. Their membership to any other groups is replaced by the user groups that are selected here.

```
For example: user1 and user2 are members of usergroup1 and
usergroup2.

Select the users from the user list. Select manage group
membership From the list of groups that are displayed,
select usergroup3 and the replace option. user1 and user2 are no longer
members of usergroup1 or usergroup2 and are only members of usergroup3.
```

### add

The selected users are now also members of the groups that you select within manage group membership.

```
For example: in the example used in the replace option, if
usergroup3 is selected with the add option, user1 and user2 are now
members of usergroup1, usergroup2 and usergroup3.
```

### delete

The selected users are removed from the groups that you select within manage group membership.



```

For example:user1 and user2 are members of usergroup1 and
usergroup2.

Select these users from the user list, then select manage group
membership. Select usergroup2 from the group list along with the delete
option. user1 and user2 are still members of usergroup1 but are no
longer members of usergroup2.

```

To assign multiple users to one or more user groups complete the following steps:

1. Choose the appropriate method for selecting multiple users
  - a. Select by using the search utility.
    - Select **Users > Search**.
    - Type in some relevant information for retrieving the user data.
    - Click **Submit**.
    - Select the users.
  - b. Select by using the **All users** report.
    - Click **Users > All users**.
    - Select the users.
2. Select **Manage Group Membership** from the **Actions** list on the left.
3. Select the user groups.
 

Any groups with a + sign can be expanded to select sub groups also.
4. Select one of the following options:
  - **replace full group membership**
  - **add to current group membership**
  - **delete from current group membership**
5. Click **Submit**.

The group membership for the multiple users is defined by the option that is selected in step 4 ([on page 89](#)).

## Viewing user groups

After you create user groups, you can view a list of all groups.

To view all user groups click **User Groups > All User groups**.

The **All User Groups** screen is displayed.

## Manage user groups

After you create user groups, you can use the following features to manage the user groups.

- View the members of a user group.
- Delete user groups.
- Change the details for a user group.
- Remove members from a user group.
- Set permissions for a user group.
- Assign user groups to other user groups.
- Search for user groups.

## Viewing the members of a user group

Use the **List Members** function to view a list of users and users groups that are members of a specific user group.

To list all members of a selected user group, complete the following steps:

1. Choose the appropriate method for displaying the user group
  - a. Select the user group by using the search utility.
    - i. Click **User Groups > Search**.
    - ii. Enter all or part of the user group name or description that is associated with the user group.  
For the quickest search, type the user group name.
    - iii. Click **Submit**.
    - iv. Select the user group.
  - b. Select by using the **All User Groups** report.
    - i. Click **User groups > All User Groups**.
    - ii. The list of all defined user groups is displayed.
    - iii. Select the user group.
2. Select **List members** from the **Actions** list on the left.

The list of members for the selected user group is displayed. The list includes user groups and users that are members of the group.

## Deleting user groups

To delete one or more user groups, complete the following steps:

1. Choose the appropriate method for displaying the user groups.
  - a. Select the user group by using the search utility.
    - i. Click **User Groups > Search**.
    - ii. Enter all or part of the user group name or description associated with the user group. For the quickest search, type the user group name.
    - iii. Click **Submit**.
    - iv. Select the user groups.

- b. Select the user group by using the **All User groups** report.
  - i. Click **User groups > All user groups**.
  - ii. Select the user groups.
2. Select **Delete User group** from the **Actions** list on the left.
3. On the **Confirm deletion** window, click **Submit**.

The user groups are deleted.

## Changing the details for a user group

You can use the **Edit Group** function to edit the details or policies and values for the selected user group.



**Note:** If the policy values are changed for a group, the new policies are valid for this group only when any new permissions links, between this user group and a target group, are created in manage permissions. Any existing links that are already defined for the user group, keep the policy values that were set for the group when the link was created. For more information about creating permissions links, see [How policies are determined for a remote control session \(on page 115\)](#).

To edit a user groups details, complete the following steps:

1. Choose the appropriate method for selecting the user group.
  - a. Select the user group by using the search utility.
    - i. Click **User Groups > Search**.
    - ii. Enter all or part of the user group name or description that is associated with the user group.  
For the quickest search, type the user group name.
    - iii. Click **Submit**.
    - iv. Select the user group.
  - b. Select by using the **All User groups** report.
    - i. Click **User groups > All User Groups**.
    - ii. The list of all defined user groups is displayed.
    - iii. Select the user group.
2. Select **Edit Group** from the **Actions** list on the left.  
For more information about the requirements for the **Edit Group** screen, see [Creating user groups \(on page 86\)](#).
3. Change the relevant information.
4. Click **Submit**.

The amended user group details are saved.

## Remove members from a user group

When users or user groups are assigned to user groups you can also remove them from the group.

Removing members from a user group can be done in multiple ways.

- Remove one member from a user group.
- Remove all members from a user group.

### Removing one member from a user group

To remove one member from a user group, complete the following steps:

1. Choose the appropriate method for selecting a user.
  - a. Select the user by using the search utility.
    - i. Click **Users > Search**.
    - ii. The Search User screen is displayed
    - iii. Enter the user information in the input field. For the quickest search, type the users's email address in the **Search Users** field. You can also type all or part of the name or any other detail that is known.
    - iv. Click **Submit**.
  - b. Select the user by using the **All Users** report.
    - i. Click **Users > All users**.
    - ii. Select the user.
2. Select **Manage Group Membership** from the **Actions** list on the left.
3. Clear the check box of the user group that you want to remove the user from.
4. Click **Submit**.

The user is no longer a member of the selected user group. Use the **List Members** function on the selected user group to confirm the removal. For more information, see [Viewing the members of a user group \(on page 90\)](#).

### Removing all members from a user group

To remove all members from a user group, complete the following steps:

1. Choose the appropriate method for selecting a user group:
  - a. Select the user group by using the search utility
    - i. Click **User Groups > Search**.
    - ii. Enter all or part of the user group name or description that is associated with the user group.  
For the quickest search, type the user group name.
    - iii. Click **Submit**.
    - iv. Select the user group.

- b. Select the user group by using the **All User groups** report.
  - i. Click **User groups > All User Groups**.
  - ii. The list of all defined user groups is displayed.
  - iii. Select the user group.
2. Select **Remove all members** from the **Actions** list on the left.
3. Press **Submit** to confirm.

All members are removed from the selected user group.



**Note:** Use the List Members function on the selected user group to confirm the removal. For more information, see [Viewing the members of a user group \(on page 90\)](#).

## Assigning user groups to other user groups

Use the **Manage Group Membership** function to make user groups members of other user groups to create a group hierarchy. User groups are assigned the permissions and policies of the user groups they are a member of. These permissions are known as the standard or normal set of permissions. For more information about how policies and permissions are granted, see [How policies are determined for a remote control session \(on page 115\)](#).

To add user groups to user groups, complete the following steps:

1. Choose the appropriate method for displaying the user group.
  - a. Select the user group by using the search utility.
    - i. Click **User Groups > Search**.
    - ii. Enter all or part of the user group name or description that is associated with the user group.  
For the quickest search, type the user group name.
    - iii. Click **Submit**.
    - iv. Select the user group.
  - b. Select the user group by using the **All User Groups** report.
    - i. Click **User groups > All User Groups**.
    - ii. The list of all defined user groups is displayed.
    - iii. Select the user group.
2. Select **Manage Group Membership** from the **Actions** list on the left.
3. Select the user groups that you want to add the selected user groups to. Some user groups in the list might have a plus sign in front of their name, which can be expanded to show other target groups. If you selected multiple target groups, select one of the following options.
  - **replace current group membership**
  - **add to current group membership**
  - **delete from current group membership**

For more information about the options, see [Assigning multiple users to user groups \(on page 88\)](#).

4. Click **Submit**.

The user group is now a member of the selected user groups.

## Setting permissions for a user group

Use the **Manage Permissions** function to create a permissions link between a user group and a target group. This link is used to define the policies and permissions that are granted in a remote control session between user and target members of these groups. For more information about this function and how the policies and permissions are determined for a remote control session, see [How policies are determined for a remote control session \(on page 115\)](#).

## Searching for user groups

You can use the Search utility to find specific user groups or find a user group by using non-specific information. To search for a user group, complete the following steps:

1. Click **User Groups > Search**.

The Search User Group screen is displayed.

Enter the user group information to be used in the search. Type all or part of the user group name or description that is associated with the user group. For the quickest search, type the user group name into the **Search User groups** field. You can also type all or part of the user group name or any other detail that is known.

2. Click **Submit**

- If any matching user groups are found, the following information is displayed
  - If the user group name is entered, the details for that user group are displayed.
  - If non-specific information is entered, a list of any user groups with this information as part of their details is displayed.



**Note:** The information that is entered is not case-sensitive - Test matches with test.

- If no matching user groups are found, a message is displayed and the user group list is blank.



**Note:** If nothing is entered in the input field and you click **Submit**. The list of all user groups is displayed.

# Chapter 11. Server session policies

You can configure the following session policies on the BigFix® Remote Control Server to determine what actions and features are available during a remote control session. The policies can be configured initially when you create a user or target group. However, the permission links set up between the user and target groups determine what policies and permissions are finally derived for the session.

For more information about groups and policies, see the following sections.

- [Creating user groups \(on page 86\)](#)
- [Creating target groups \(on page 71\)](#)
- [How policies are determined for a remote control session \(on page 115\)](#)

## Policy list definitions

### Security policies

#### Reboot

To send a restart request to the target computer, so that it can be restarted remotely. Determines whether **Reboot** is available as a session mode option on the start session screen. For more information about session types, see the *BigFix® Remote Control Controller User's Guide*.

##### Set to Yes.

**Reboot** is shown as an option on the start session screen.

##### Set to No.

**Reboot** is not shown as an option on the start session screen.

#### Allow multiple Controllers

To enable collaboration so that multiple controllers can join a session. Determines the availability of the collaboration option on the controller window. For more information about collaboration sessions that involve multiple participants, see the *BigFix® Remote Control Controller User's Guide*.

##### Set to Yes.

The collaboration icon is available for selection in the controller window.

##### Set to No.

The collaboration icon is not active in the controller window.

#### Allow local recording

To 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*.

##### Set to Yes.

The record option is available for selection in the controller window.

**Set to No.**

The record option is not active in the controller window.

**Set target locked**

Determines whether the local input and display is locked for all sessions. Therefore, the target user cannot use the mouse or keyboard on the target while in a remote control session.

**Set to Yes.**

The target screen is blanked out when the session is started, 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.

**Set to No.**

The target screen is not blanked out when the session is started and the target user is able to interact with the screen.

**Allow input lock**

Determines whether the 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.

**Set to Yes.**

The **Enable Privacy** option is available in the **Perform Action in target** menu in the controller window. For more information about the controller window functions, see the *BigFix® Remote Control Controller User's Guide*.

**Set to No.**

The **Enable Privacy** option is not available in the **Perform Action in target** menu in the controller window.

**Connect at Logon**

Determines whether a session can be started when no users are logged on at the target.

**Set to Yes.**

Session is started with the target.

**Set to No.**

Session is not started and the following message is displayed. `Session rejected because there is no user logged to confirm the session`

**Use Encryption**

Determines whether to encrypt the data that is being transmitted.

**Disable Panic Key**

Determines whether the Pause Break key can be used by the target user to automatically end the remote control session.



**Set to Yes.**

The target user cannot use the Pause Break key to automatically end the remote control session.

**Set to No.**

The target user can use the Pause Break key to automatically end the remote control session.

**Enable On-screen Session Notification**

Determines whether a semi-transparent overlay is shown on the target computer to indicate that a remote control session is in progress. Use this policy when privacy is a concern so that the target user is clearly notified when somebody is remotely viewing or controlling their computer.

**Set to Yes.**

The semi-transparent overlay is shown on the target screen with the text **Remote Control**. The type of remote control session that is in progress is also displayed. The overlay does not intercept keyboard or mouse actions, therefore the user is still able to interact with their screen.

**Set to No.**

The overlay is not shown on the target computer.



**Note:** This policy is only supported on targets that have a Windows® operating system installed.

**Allow input lock with visible screen**

This property works along with **Allow input lock** and on its own. Use **Allow input lock with visible screen** to lock the target users mouse and keyboard during a remote control session.

**Set to 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.

**Set to No.**

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.

**Display screen on locked target**

Works along with **Set target locked**, which you can use to enable privacy mode at session startup. You can use **Display screen on locked target** to determine whether the target user can view their screen or not during a remote control session, when privacy mode is enabled.

#### Set to Yes.

In privacy mode, the target screen is visible to the target user during the session, but their mouse and keyboard control is locked.

#### Set to No.

In privacy mode, the target screen is not visible to the target user and the privacy bitmap is displayed during the session. The target users mouse and keyboard input is also disabled.



**Note:** For **Display screen on locked target** to take effect set **Set target locked** to Yes.

### Denied Program Execution List

To specify a list of programs that a controller user cannot run on the target during an active session with the target. These programs must be entered as a comma-separated list. The following points must be noted.



#### Note:

1. This feature works only on the following operating systems
  - Windows® 2000, all editions
  - Windows® XP, 32-bit editions only
  - Windows® Server 2003, 32-bit editions only
2. The programs can be entered with or without a path defined.

```
For example  
c:\notepad.exe or notepad.exe are both acceptable.
```

3. Any program with a space in its name must be enclosed in double quotation marks.

```
my prog.exe should be entered as "my prog.exe"
```

4. If you enter any of the Remote Control specific programs in the list, for example `trc_dsp`, `trc_base` or `trc_gui`, they are ignored.
5. If any of the programs that are listed are already running on the target when the session is started, they continue to run. However, any new instances of the program are not started.

### Inactivity timeout

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 0.

## Auditing

### Force session recording

All sessions are recorded and the session recordings are uploaded and saved to the server.

#### Set to Yes.

A recording of the session is saved to the server when the session ends. A link for playing the recording is also available on the session details screen.

#### Set to No.

No recording is stored and therefore no link is available on the session details screen.

## Local Audit

Use to create a log of auditable events that take place during the remote control session. The log is created on both the controller and target computer.

#### Set to Yes.

The `trcaudit` log file is created and stored on the controller computer in the home directory of the currently logged on user.

The log can be viewed on a Windows target computer by using the event viewer. To access the Application Event Viewer click **Start > Control Panel > Administrative Tools > Event Viewer > Application**. On a Linux target, the events are stored in the messages file that is in the `/var/log` directory.

#### Set to No.

No log is created or stored on the controller or target computer.

## Force session audit

A log of auditable events is automatically stored on the server. Determines the visibility of these events on the session details screen.

#### Set to Yes.

Controller and target events that took place during the session are displayed on the session details screen.

#### Set to No.

Controller and target events are not displayed on the session details screen.

### Keep session recording in the target system

Determines whether a copy of the session recording that was done on the target and successfully uploaded to the BigFix® Remote Control Server is also saved on the target system. The location of the saved recording is determined by the location that is set in the target property **RecordingDir**.



**Note:** This policy is only valid if **Record the session in the target system** is set to Yes.

#### Set to Yes.

If **Record the session in the target system** is set to Yes and the session recording is successfully uploaded to the BigFix® Remote Control Server, a copy of the recording is also saved on the target system.

#### Set to No.

If **Record the session in the target system** is set to Yes and the session is recorded, a copy of the recording is not saved on the target system.

### Record the session in the target system

Determines whether the session recording is done on the target system instead of the controller, when the **Force session recording** policy is also set to Yes.

#### Set to Yes.

The session is recorded on the target and uploaded to the BigFix® Remote Control Server.



**Note:** However, if **Force session recording** is set to No, the session is not recorded.

#### Set to No.

The session is recorded on the controller and uploaded to the BigFix® Remote Control Server.

### Control

#### Enable high quality colors

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**.

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.

### Allow registry key lookup

Determines the availability of the Enter key item in the **Registry keys** menu on the controller window, during a guidance and active session.

#### Set to Yes.

The **Enter key** option is available in the **Registry keys** menu. Use the **Enter key** option to enter a registry key and lookup the value that is defined for it on the target. For more information about the **Registry keys** menu, see the *BigFix® Remote Control Controller User's Guide*.

#### Set to No.

The Enter key option is not available and the controller user cannot find out the values of the targets registry keys.

### View registry key list

Determines the availability of the defined registry keys list in the **Registry keys** menu on the controller window.

#### Set to Yes.

The list of up to 10 registry keys, which can be defined in the `trc.properties` file, is visible in the **Registry keys** menu. The controller user can select one to view the value for it on the target. For more information about editing the properties files, see [Editing the properties files \(on page 215\)](#).



**Note:** If you set this policy to Yes, you must make sure that you define registry keys in the `trc.properties` file. Otherwise, if you click the menu item, nothing is shown.

#### Set to No.

The defined list of registry keys is not visible in the **Registry keys** menu.

### Enable user acceptance for system information

Use this policy to display the user acceptance window on the target computer when the controller user selects to view the target system information.

#### Set to Yes.

When the controller user clicks the system information icon in the controller window, the user acceptance window is displayed. The target user must accept or refuse the request to view the target system information. 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.

**Set to No.**

The target system information is displayed automatically when the controller user clicks the system information icon.

**Enable user acceptance for file transfers**

Use this policy to display the user acceptance window on the target computer when the controller user wants to transfer a file from the target to the controller system.

**Set to Yes.**

The acceptance window is displayed in the following two cases. The target user must accept or refuse the file transfer.

- If the controller user selects **pull file** from the file transfer menu on the controller window.



**Note:** The target user must select the file that is to be transferred, after they accept the request.

- If the controller user selects **send file to controller** from the **Actions** menu in the target window

**Set to No.**

The acceptance window is not displayed and files are transferred automatically from the target to the controller system when requested.

**Enable user acceptance for mode changes**

Use this policy to display the user acceptance window on the target computer when the controller user selects a different session mode.

**Set to Yes.**

The user acceptance window is displayed each time the controller user selects a new session mode. The target user must accept or refuse the request.

**Set to No.**

The user acceptance window is not displayed and the session mode is changed automatically.

**Enable user acceptance for incoming connections**

Use this policy to display the user acceptance window on the target computer when a remote control session is requested. The target user must accept or refuse the session.




**Note:** This policy works along with **Acceptance Grace Time** and **Acceptance timeout action**.

**Set to Yes.**

The acceptance window is displayed and the target user has the number of seconds defined for **Acceptance Grace time** to accept or refuse the session.

 **Note:**

1. The target user can also select a different session mode on the **User Acceptance** window.
2. The target user can hide any running applications by choosing the **Hide applications** option on the acceptance window. For more information about hiding applications, see the *BigFix® Remote Control Controller User's Guide*.

 **Note:** The "Allow to show/hide selected windows during the session" feature has been deprecated for all versions above Windows 7.

3. When set to Yes, the **Acceptance Grace time** must be > 0 to give the target user time to accept or refuse the session

**Accept**

The session is established.

**Refuse**

The session is not started and a message is displayed.

**Set to No.**

The session is started automatically and the **User Acceptance** window is not displayed on the target.

**Run post-session script**

Determines whether a user-defined script is run after the remote control session finishes.

**Set to Yes.**

When a remote control session ends, the user-defined script is run. Complete the following steps to set up the scripts.

The script must be given the following name.

```
post_script. {ext}
```

Where {ext} is `.cmd` on a Windows™ system and `.sh` in UNIX™ or Linux™ systems.

The script must be placed in the following directory on the target.

**Windows™ systems.**

```
\%SYSTEMROOT%\scripts
```

Where *SYSTEMROOT* is the relevant Windows™ operating system directory.

**UNIX™ or Linux™ systems.**

```
/etc/scripts
```



**Note:** This directory must be owned by root and have the permissions 700 so that root can read, write, or execute. All other users must have no permissions. Otherwise, the script does not run and it fails. The success or failure of the execution of this script is logged in the audit log by the target.

**Set to No.**

No script is run after the session.

**Run pre-session script**

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. This policy is connected to **Pre-script fail operation**. The outcome of running the script and the continuation of the session is determined by the value that is set for **Pre-script fail operation**.

**Set to Yes.**

When a Remote Control Session is requested, the defined script is run before the controller user has access to the target.

Defining Pre and Post scripts.

The script development is free from any constraint. Except for the need to allow them to run unattended and to use exit codes that can be correctly interpreted by Remote Control. Pre-scripts and post-scripts are supported on the following operating systems.

- Windows® (XP, 2003, Vista, 7)
- Linux® (SLES, RHLE)

When you develop scripts, you must adhere to the following rules:

- Define the scripts as batch files on a Windows® system (with extension `.cmd`) and as shell files on a Linux® system (with extension `.sh`).
- On Windows® systems, the scripts must be named `pre_script.cmd` and `post_script.cmd`. On Linux systems,™ they must be named `pre_script.sh` and `post_script.sh`.



- Copy the scripts into a directory that is called `scripts` that is in the installation directory of the Remote Control target. Make sure that they are executable just by root to avoid security exposures in Linux®.



**Note:** This directory must be owned by root and have the permissions 700 so that root can read, write, or execute. All other users must have no permissions. Otherwise, the script does not run and it fails. The success or failure of the execution of this script is logged in the audit log by the target.

- The pre-script and post-scripts are run with system privileges and without validation to protect them from unauthorized access.



**Note:** The installer creates the script directory with access just for administrators and **localsystem** on a Windows® system and for read/write/execute just for root on a Linux® system.

- Ensure that the scripts end within 3 minutes. If they run for longer, they cannot return a valid execution code. The administrator at the controller is notified that the timeout elapsed and an error occurred. The execution code indicates whether the script did run.
- Define a non-negative (greater than or equal to 0) exit code for the script to indicate that the script ran with success. Define a negative exit code to indicate that it ran with errors. Whenever an error occurs a message is reported to the controller. The exit code is shown and session fails to start.

### Environment Variables

You can use the following environment variables in the pre-script and post-script.

**RC\_TIVOLI\_ADMIN\_NAME= Tivoli\_administrator\_name.**

Where `Tivoli_administrator_name` specifies the Tivoli® administrator name on the controller as provided by the server.

**RC\_TIVOLI\_ADMIN\_LOGIN = Tivoli\_administrator\_name.**

Where `Tivoli_administrator_name` specifies the Tivoli® administrator name on the controller as provided by the server.

**RC\_ACTION=action.**

Where *action* specifies the following actions:

**0**

No actions.

**1**

Remote Control (Active, Guidance, or Monitor)

**2**

File Transfer.

**3**

Chat

**4**

Reboot

**RC\_GRACE\_PERIOD= *duration*.**

Where *duration* specifies the number of seconds to wait for the target user to respond before an activity starts or times out.

**RC\_PROCEED\_IF\_TIMEOUT= *timeout*.**

Where *timeout* determines whether to start a session if the target user does not respond within the grace period. Possible values are,

**1**

Starts the session if the grace period times out.

**0**

Cancels the session if the grace period times out.

**RC\_STARTUP\_STATE = *startup\_state* .**

Where *startup\_state* specifies the initial state of a Remote Control action. Possible values are,

**0**

The action is started in monitor state (Monitor or Guidance).

**1**

The action is started in active state (Active).

**RC\_CHANGE\_STATE= *change\_state***

Where *change\_state* determines whether the target user can change the state during a remote control session. Possible values are,

**0**

Not enabled.

**1**

Enabled (user can change from Active to Monitor/Guidance or vice versa).

**Set to No.**

No script is run before the session.

#### **Allow automatic session handover**

Determines whether a collaboration session is automatically handed over to another participant when the master controller loses connection to the broker. The policy applies only to collaboration sessions that you start through a broker. For more information about session resilience, see the *BigFix® Remote Control Controller User's Guide*.

##### **Set to Yes.**

If the master controller does not reconnect to the broker within 3 minutes, session control automatically passes to another participant. However, if user acceptance is enabled, the target user must accept or refuse the new master controller.

##### **Set to No.**

If the master controller does not reconnect to the broker within 10 minutes, the session terminates. This value is the default value.

#### **Allow clipboard transfer**

Determines the availability of the **clipboard transfer** icon in the controller session window. For more information about this feature, see the *BigFix® Remote Control Controller User's Guide*.

##### **Set to Yes.**

The clipboard transfer icon is available for use in the controller window. The controller user can transfer the clipboard content between the controller and the target.

##### **Set to No.**

The clipboard transfer icon is not available for use in the controller window.

#### **Allow session handover**

The master controller in a collaboration session can use this feature to hand over control of the session to a new controller. Determines the availability of the **Handover** option on the collaboration control panel. For more information about the handover function, see the *BigFix® Remote Control Controller User's Guide*.

##### **Set to Yes.**

The **Handover** option is displayed in the **Collaboration control panel**.

##### **Set to No.**

The **Handover** option is not displayed in the **Collaboration control panel**.

#### **Enable user acceptance for collaboration requests**

Use this policy to display the user acceptance window on the target computer when another controller requests to join a collaboration session. For more information about joining a collaboration session, see the *BigFix® Remote Control Controller User's Guide*.

##### **Set to Yes.**

The user acceptance window is displayed on the target computer after the master controller accepts to share the session for collaboration. The target users response determines whether the additional controller is allowed to join the session.

**Accept**

The additional controller joins the collaboration session.

**Refuse**

A refusal message is displayed on the controller and the additional controller cannot join the collaboration session.

**Timeout**

If the target user does not respond to the user acceptance within the time that is defined in **Acceptance Grace Time**, a refusal message is displayed to the additional controller. The additional controller does not join the collaboration session.

**Set to No.**

The user acceptance window is not displayed on the target computer. After the master controller accepts to share the session for collaboration, the additional controller joins the session.

**Stop screen updates when screen saver is active**

Stops the target from sending screen updates when it detects that the screen saver is active.

**Set to Yes.**

While the screen saver is active on the target system, the target stops transmitting screen updates. A simulated screen saver is displayed on the controller computer so that the controller user knows that a screen saver is active on the remote screen. The controller user can close the screen saver by pressing a key or moving the mouse.

**Set to No.**

No simulated screen saver is displayed in the session window. The target screen is displayed as normal and the target continues to transmit screen updates.

**Enable user acceptance for local recording**

Use this feature to display the user acceptance window when a controller user clicks the record icon on the controller window. The target user can accept or refuse the request to make a local recording of the remote control session.

**Set to Yes.**

When the controller user clicks the record icon on the controller window, a message dialog 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.

#### **Set to No.**

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.

#### **Hide windows (Deprecated)**



**Note:** The "Allow to show/hide selected windows during the session" feature has been deprecated for all versions above Windows 7.

Determines whether the **Hide windows** check box is displayed on the user acceptance window when **Enable user acceptance for incoming connections** is also set to Yes.

#### **Set to Yes.**

The **Hide windows** check box is displayed on the user acceptance window.

#### **Set to No.**

The **Hide windows** check box is not displayed on the user acceptance window.

#### **Remove desktop background**

Determines whether a desktop background image can be removed from view during a remote control session.

#### **Set to Yes.**

The desktop background image on the target is not visible during a remote control session.

#### **Set to No.**

The desktop background image on the target is visible during a remote control session.

#### **Lock color quality**

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**.

### **Set to No.**

The color quality can be changed during the session. The **Performance settings** icon is enabled in the controller window.

### **Pre/post - script fail operation**

Action to take if the pre-script or post-script execution fails. A positive value or 0 is considered a successful run of the pre-script or post-session script. A negative value, script that is not found or not finished running within 3 minutes is considered a failure.

#### **Abort**

If the pre-script or post-script run is a fail, the session does not continue.

#### **Proceed**

If the pre-script or post-script run is a fail, the session continues.

### **Acceptance timeout action**

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**.

#### **Abort**

Session is not established. This value is the default value.

#### **Proceed**

Session is established.

### **Acceptance Grace Time**

Sets the number of seconds to wait for the target user to respond before a session starts or times out. Used along with **Enable User Acceptance for incoming connections**.



**Note:** If **Enable user acceptance for incoming connections** is set to Yes, Acceptance Grace Time must be set to a value >0 to give the target user time to respond.

## **Configuration**

### **File Transfer**

Determines whether File Transfer is available as a session mode on the start session window so that files can be sent or received during the session. For more information about File Transfer session mode, see the *BigFix® Remote Control Controller User's Guide*.

#### **Set to Yes.**

File Transfer is available as a session mode in the start session window.

#### **Set to No.**

File Transfer is not available as a session mode in the start session window.

**Allow chat in session**

Determines whether chat functions are available while in a remote control session and the also the availability of the chat icon in the controller window. For details of the Chat function, see the *BigFix® Remote Control Controller User's Guide*.

**Set to Yes.**

Chat icon is available for selection in the controller window.

**Set to No.**

Chat icon is disabled in the controller window.

**Active**

Determines whether the target system can take part in active sessions. Also determines whether Active is available as a session mode on the start session window. For more information about the Active session mode, see the *BigFix® Remote Control Controller User's Guide*.

**Set to Yes.**

Active is available as a session mode in the start session window.

**Set to No.**

Active is not available as a session mode in the start session window.

**Guidance**

Determines whether the target system can take part in guidance sessions. Also determines whether Guidance is available as a session mode on the start session window. For more information about the Guidance session mode, see the *BigFix® Remote Control Controller User's Guide*.

**Set to Yes.**

Guidance is available for selection as a session mode in the start session window.

**Set to No.**

Guidance is not available for selection as a session mode in the start session window.

**Monitor**

Determines whether the target system can take part in monitor sessions. Also determines whether Monitor is available as a session mode on the start session window. For more information about the Monitor session mode, see the *BigFix® Remote Control Controller User's Guide*.

**Set to Yes.**

Monitor is available for selection as a session mode in the start session window.

**Set to No.**

Monitor is not available for selection as a session mode in the start session window.

**Chat**

Determines whether the target system can take part in chat only sessions. Also determines whether Chat is available as a session mode on the start session window. For more information about the Chat session mode, see the *BigFix® Remote Control Controller User's Guide*.

**Set to Yes.**

Chat is available as a session mode in the start session window.

**Set to No.**

Chat is not available as a session mode in the start session window.

**Command**

Determines whether the target system can take part in Command sessions. Also determines whether Command is available as a session mode on the start session window. For more information about the Command session mode, see *BigFix® Remote Control Controller User's Guide*.

**Set to Yes.**

Command is available as a session mode in the start session window.

**Set to No.**

Command is not available as a session mode in the start session window.

**File Transfer Actions**

Determines the actions that can be carried out on a file during a File Transfer session. If no value is set, the file transfer action is determined by the **default.rc\_def\_ft\_actions** property in the `trc.properties` file.

**Set to Send.**

You can transfer files only to the target during a File Transfer session.

**Set to Pull.**

You can transfer files only from the target during a File Transfer session.

**Set to Both.**

You can transfer files to and from the target during a File Transfer session.

**Allow file transfer in session**

Controls the transfer of files while in an Active session. Its value determines the availability of the **Send file / Pull file** options in the **File Transfer menu** within the **Controller** window. For more information about transferring files, see the *BigFix® Remote Control Controller User's Guide*.

**Set to NONE.**

The Send file and Pull file options are not available for selection. No file transfers can be initiated.

**Set to BOTH.**



The Send file and Pull file options are available. Files can be transferred to the target and transferred from the target. This value is the default value.

**Set to PULL.**

Only the Pull file option is available. Files can be transferred only from the target.

**Set to SEND.**

Only the Send file option is available. Files can be transferred only to the target.

**Policy List Values**

**Table 1. Policy acceptable and default values.**

<b>Policy</b>	<b>Possible values.</b>	<b>Default value.</b>
Reboot	yes   no	yes
Allow multiple controllers	yes   no	yes
Allow local recording	yes   no	yes
Set target locked	yes   no	no
Allow input lock	yes   no	yes
Connect at logon	yes   no	yes
Use encryption	yes   no	yes
Disable Panic Key	yes   no	no
Enable on-screen session notification	yes   no	no
Allow input lock with visible screen	yes   no	no
Display screen on locked target	yes   no	no
Denied Program Execution List	blank	blank
Inactivity timeout	number of seconds	0
Force session recording	yes   no	no
Local audit	yes   no	yes
Force session audit	yes   no (live audit on server)	yes
Keep session recording in the target system	yes   no	no
Record the session in the target system	yes   no	yes
Enable high quality colors	yes   no	no
Allow registry key lookup	yes   no	no
View registry key list	yes   no	no

**Table 1. Policy acceptable and default values. (continued)**

<b>Policy</b>	<b>Possible values.</b>	<b>Default value.</b>
Enable user acceptance for system information	yes   no	no
Enable user acceptance for file transfers	yes   no	no
Enable user acceptance for mode changes	yes   no	no
Enable user acceptance for incoming connections	yes   no	no
Run post-session script	yes   no	no
Run pre-session script	yes   no	no
Allow automatic session handover	yes   no	no
Allow clipboard transfer	yes   no	yes
Allow session handover	yes   no	yes
Enable user acceptance for collaboration requests	yes   no	no
Stop screen updates when screen saver is active	yes   no	no
Enable user acceptance for local recording	yes   no	no
Hide windows	yes   no	no
Remove desktop background	yes   no	no
Lock color quality	yes   no	no
Pre / post -script fail operation	abort   proceed	abort
Acceptance timeout action	abort   proceed	abort
Acceptance Grace Time	number of seconds	45
File transfer	yes   no	yes
Allow chat in session	yes   no	yes
Active	yes   no	yes
Guidance	yes   no	yes
Monitor	yes   no	yes
Chat	yes   no	yes
Command	yes   no	no
File transfer actions	pull   send   both	both
Allow file transfer in session	none   pull   send   both	both

## Chapter 12. How policies are determined for a remote control session

When a remote control session is requested, a number of factors must be considered when the permissions and policies are determined for the session. The policies and permissions for the various entities that are involved in the session are considered. These entities are user, user groups to which the user belongs, target, and target groups to which the target belongs. The different sets of policies must be resolved following rules of precedence. The result is a single set of policies and permissions for each session.

Users and targets are assigned to groups that have policies and permissions defined. The permissions that are defined in these groups are known as their standard or normal set of permissions.

Due to the group hierarchy that can be set up, users and targets can be members of groups. User groups and target groups can also be members of other groups. Therefore, when a remote control session is requested, the following permissions are considered when the policies are determined for the session.

- The permission sets that are defined for immediate user to target group relationships.
- The permission sets that are defined for relationships between parent and grandparent groups.

When all required user and target groups are created and their membership is defined, you must create relationships between the user and target groups. The relationships determine the policies and permissions that are applied during a remote control session. Use the **Manage Permissions** function to create these links between the groups.



**Note:** It is important to set up the groups and relationships in a way that does not lead to unexpected policy values.

### Set the policies and permissions for a remote control session

Creating permissions links between user groups and target groups is a fundamental part of the Remote Control application. These links are used to determine which policies and permissions are applied to a remote control session. When a user group or target group is created, a set of permissions is defined for the group. The permissions are known as the standard or normal set. Use **Manage Permissions** to create a permissions link to combine the standard set of policies for the user group and standard set of policies for the target group. This standard permissions link has policies set to priority 0. You can then enable or disable the relevant policies. The standard permissions can also be overridden by selecting a 1 or 5 priority value to create a new set of permissions. The new set is valid only for the particular user group and target group combination that is selected. Therefore, avoiding the requirement for setting up a user and target group permissions link for every relationship needed.



**Note:** After you create a permissions link between a user group and target group, the only way to change the policies for a session between members of these two groups is to edit this link. Editing the policies, through the **Edit group** function, has no effect on the policies and permissions that are defined in the existing link in



**Manage Permissions.** It affects only the policies that are considered for the group when any new permissions links are created.

## Values assigned for standard or normal permissions

When you select a user group and a target group to set up a permissions link, the following rules govern which values are applied automatically in manage permissions.

### Policy is set to **Yes** for the session.

- Applied when both the user group and target group have a policy value, in their standard permissions template, set to **Yes**.
- Applied if one group has a policy value in their standard permissions template set to **Yes** and the other group set to **Not Set**. Standard Yes overrides Not Set

### No

Applied when either group has a **No** policy value set in their standard permissions.

```
For example : user group UG1
```

```
Guidance policy set to Yes
```

```
Monitor policy set to Yes
```

```
Reboot policy set to No
```

Members of UG1 can start **Guidance** and **Monitor** sessions but are not allowed to restart the target.

```
For example : target group TG1
```

```
Guidance policy set to Yes
```

```
Monitor policy set to Not Set
```

```
Reboot policy set to Yes
```

Members of TG1 can accept **Guidance** and **Monitor** sessions and are allowed to accept a Reboot request.

Therefore, the following policy values, are automatically applied to the standard permissions set when UG1 and TG1 are selected on the **Manage Permissions** screen.

UG1 ↔ TG1

**Table 2. Standard Permissions**

	UG1	TG1	Manage Permissions set
Guidance	Yes	Yes	Yes

**Table 2. Standard Permissions (continued)**

	UG1	TG1	Manage Permissions set
Monitor	Yes	Not Set	Yes
Reboot	No	Yes	No

## Assign a higher priority value to policies

Use the **Manage Permissions** function to apply a higher priority to policy permissions, to override the standard permissions set. Therefore, avoiding the requirement of having to set up a user group and target group permissions combination for every relationship needed. When the policies for a session are being determined, higher priority permissions override standard permissions if multiple permissions sets are found within the group hierarchy. Multiple values that can be assigned to policies.

### 0

This value is the standard or normal value that is automatically assigned to the policies when a link is created between a user group and a target group.

### 1

This value can be used to override any priority 0 policies when there are multiple permissions sets to be considered for a session.

If there is a group hierarchy and one of the permissions links has a policy set to priority 0 No, the policy is set to No when a session is established. To set the policy to Yes, for the session, select priority 1 Yes in the permissions link. A priority 1 Yes overrides a priority 0 No.

### 5

This value overrides all other priority values when there are multiple permissions sets to be considered for a session.

## Creating a permission link

After you create user groups and target groups, create a link between them to define a set of policies to be considered when a remote control session is requested between the user and target members of these groups.

To create this link, complete the following steps:

1. Click **Target groups > All Target groups** or use the search facility. For more information, see [Searching for target groups \(on page 78\)](#)
2. Select the target group.  
For example, DefaultTargetGroup.
3. Click **Manage Permissions**.  
The Manage Permissions screen is displayed.
4. Choose the appropriate method for creating the permissions link.

The first time you create a link between two groups, use the **Group Browser** option. You can use the **Existing profile** option to edit an already defined link.

Using the **Group Browser** option.

- Click the selector button next to user group. Select the user group from the list. For example, DefaultGroup.
- Click the selector button.
- Click the selector button next to target group. Select the target group from the list. For example, DefaultTargetGroup.
- Click the selector button.

Using the **Existing profile** option.

- Select **Existing Profile**
- Select the user to target group link from the list.
- Click the selector button.

The set of permissions is displayed. The selected values are derived from the combination of standard policies that are defined for the selected user and target group.

5. To enable all of the policies, click the **Enabled?** check box. To enable specific policies, click the enabled check box next to each policy.

Clear the check box next to each policy that you do not want.



**Note:** All required policies must be enabled before you save the permissions link. Any policy that is not enabled loses its current value when the permissions link is saved. You must reassign a value to the policy if it is enabled, within the permissions link, in the future.

6. Set the priority for each enabled policy.

**0**

This value is the lowest priority and is automatically assigned when you create the permissions link.

**1**

This value overrides a priority 0 policy when the policies and permissions are being determined for a remote control session.

**5**

This value is the highest priority. It overrides any existing 0 and 1 priority policy when the policies and permissions are being determined for a remote control session.

7. Set or enter a value for the enabled properties.

For definitions and values for the policies, see [Server session policies \(on page 95\)](#).

**Set to Yes**

The policy is in effect during a remote control session depending on the priority that is set for it.

#### **Set to No**

The policy is not in effect during a remote control session depending on the priority that is set for it.

8. You can create a schedule to define when the set of policies is valid. To create a schedule for the policies, go to step 9 (on page 119) otherwise click **Submit** and the policies are now active.
9. From the - Repeat Schedule - list, select the relevant options. Click **Submit**.

#### **Once Only**

Policies are only valid from the start date and start time until the end date and end time.

- a. Type in a Start date, in the format *yyyy-mm-dd* or select the calendar icon to select the date.
- b. Type in a Start time in the format *hh:mm:ss*.
- c. Type in an End date, in the format *yyyy-mm-dd* or select the calendar icon to select the date.
- d. Type in an End time in the format *hh:mm:ss*.

#### **Daily**

Policies are valid every day between the selected start time and the end time from the start date until the end date.

- a. Type in a Start date, in the format *yyyy-mm-dd* or select the calendar icon to select the date.
- b. Type in an End date, in the format *yyyy-mm-dd* or select the calendar icon to select the date.
- c. Type in a Start time in the format *hh:mm:ss*.
- d. Type in an End time in the format *hh:mm:ss*.

#### **Weekly**

Policies are valid every week on the selected days, between the selected start time and end time from the start date until the end date.

- a. Type in a Start date, in the format *yyyy-mm-dd* or select the calendar icon to select the date.
- b. Type in a Start time in the format *hh:mm:ss*
- c. Type in an End date, in the format *yyyy-mm-dd* or select the calendar icon to select the date.
- d. Type in an End time in the format *hh:mm:ss*.
- e. Select the days.

## Deleting a permission link

After you create permissions links, you can delete them by completing the following steps:

1. Click **Target groups > All Target groups** or use the search function to search for target groups. For more information about searching for target groups, see [Searching for target groups \(on page 78\)](#).
2. Select the target group. For example, DefaultTargetGroup.
3. Click **Manage Permissions**.
4. Click **Existing Profile**.
5. Select the link from the **Existing Profile** list.
6. Click x, to the right of the existing profiles list.
7. On the **Confirm deletion** screen click **Submit**.

The selected permissions link is deleted.



**Note:** It is the link between the user group and target group that is deleted, the policies and permissions that are set specifically for the user group and target group are not affected when the permissions link is deleted.

## How permissions are derived

When a request for a remote control session is initiated, all of the groups to which the user and target belong to are determined. The following statements can be true for the groups.

- No grandparent group present: Any parent groups that are found for the user and target have user or target members only.
- Grandparent group present: Due to the group hierarchy that is created through manage group membership, any parent groups that are found also have user group, and target group members.

The next thing that is determined is, which permissions links are created between any of these groups. The permissions for the session are derived from using the following set of rules.

Rule 1: No grandparent group. There can be 2 scenarios.

**The user and target are members of a single user group and target group only.**

The policies for the session are set from the one permissions link that is defined for their parent user group and target group combination.

**User and target are also members of other user and target groups.**

The policies for the session are derived from comparing the multiple permissions links that are defined for any parent user group and target group combinations.

Rule 2: Grandparent group.

The policies for the session are derived from comparing multiple permissions links. The links that are defined for any parent user group and target group combinations, and any permissions links that are defined for any grandparent groups are all considered.



Where multiple permissions links are present within the group hierarchy, the value and priority that is set for each enabled policy, within each link, is checked. The following rules for the priority values, determine what is applied to the session policy.

**Priority 5 No**

If a policy in any of the relevant permissions links has this value set, the session policy is set to priority 5 No. This value overrides all other values.

**Priority 1 No**

This value is set for the session policy if there are no priority 5 values set in any existing permissions links.

**Priority 0 No**

This value is set for the session policy if there are no priority 1 or 5 values set for any of the existing permissions links.

**Priority 5 Yes**

This value is set for the session policy if there are no priority 5 No values set for any of the existing permissions links. Priority 5 Yes overrides any lower priority No.

**Priority 1 Yes**

This value is set for the session policy if there are no priority 5 values, or priority 1 No values set for any of the existing permissions links.

**Priority 0 Yes**

This value is set for the session policy if there are no higher priority values set or a priority 0 No set for any of the existing permissions links.

## Set non-binary policies

The non-binary policies work differently from the binary policies. You must enter a value for the policy.

- Denied Program Execution List
- Inactivity timeout
- Pre Script Fail Operation
- Acceptance Timeout Action
- Acceptance Grace Time
- Allow File Transfer in Session

- If there are multiple permission links that have different values for the non-binary policies, the final set of policies inherit one of the values, but it is not defined which one.
- If a non-binary policy is not enabled in any permissions links in the group hierarchy, the default value that is defined in the `trc.properties` file is assigned. For more information about the properties file, see [trc.properties \(on page 216\)](#).



**Note:** If non-binary policies are enabled in the group hierarchy but no values are assigned to them, the values that are defined in `trc.properties` are not assigned. Therefore, if you enable a non-binary policy you must also assign a value to it.

## Permissions set examples

The following examples show how the permissions are determined for a session that involves the following entities.

4 user groups U1 – U4

5 target groups T1 – T5

Users X and Y

Targets A and B

The following steps create the users, targets, user groups, and target groups that are used in the examples. The examples show how policies and permissions are derived for a session.

1. Create users X and Y.
  - a. Click **Users > New**.
  - b. Enter relevant details for user X and click **Submit**.
  - c. Repeat the steps to create user Y.
2. Create the required user group U1 to U4.
  - a. Click **User groups > New user group**.
  - b. Type in the group name. For example, U1.
  - c. Click **Submit** to accept the default template.
  - d. Repeat the steps to create groups U2, U3, and U4.
3. Assign user or user group members to the user group.
  - a. Make user X a member of group U3.
    - a. Click **Users > Search**.
    - b. Type in the user ID or some other relevant information for user X.
    - c. Select user X and click **Manage Group Membership**.

- d. In the user group list, select U3 then click **Submit**.



**Note:** Make sure that U3 is the only user group that is selected.

- Make user Y a member of group U4
  - a. Click **Users**.
  - b. Click **Search** then type in the user ID or some other relevant information for user Y.
  - c. Select user Y then click **Manage Group Membership**.
  - d. In the user group list, select U4 then click **Submit**.



**Note:** Make sure that U4 is the only user group that is selected.

- Make groups U3 and U4 members of U2
  - a. Click **User groups**.
  - b. Click **Search** then type in U.
  - c. Click **Submit**.
  - d. Select U3 and U4 then click **Manage Group Membership**.
  - e. In the user group list, select U2.



**Note:** Make sure that U2 is the only user group that is selected.

- f. Select **add to current group membership**.
- g. Click **Submit**.

- Make U2 a member of U1
  - a. Click **User groups**.
  - b. Click **Search** then type in U2.
  - c. Click **Submit**.
  - d. Select U2 then click **Manage Group Membership**.
  - e. In the user group list, select U1 then click **Submit**.

#### 4. Create the required target groups T1 to T5

- a. Click **Target groups > New target group**.
- b. Type in the group name. For example, T1.
- c. Click **Submit** to accept the default template.
- d. Repeat the steps to create groups T2, T3, T4, and T5.

#### 5. After the target software is installed on target A and target B and the targets contact the server, assign target or target group members to target groups.

- Make target A a member of group T4
  - a. Click **Targets**.
  - b. Click **Search** then type in the serial number or some other relevant information for target A.
  - c. Select target A then click **Manage Group Membership**.
  - d. In the target group list, select T4 then click **Submit**.



**Note:** Make sure that T4 is the only target group that is selected.

- Make target B a member of group T5
  - a. Click **Targets**.
  - b. Click **Search** then type in the serial number or some other relevant information for target B.
  - c. Select target B then click **Manage Group Membership**.
  - d. In the target group list, select T5 then click **Submit**.



**Note:** Make sure that T5 is the only target group that is selected.

- Make group T4 and T5 members of T2
  - a. Click **Target groups**.
  - b. Click **Search** then type in T.
  - c. Click **Submit**.
  - d. Select T4 and T5 then click **Manage Group membership**.
  - e. In the target group list, select T2.



**Note:** Make sure that T2 is the only target group that is selected.

- f. Select **add to current group membership**.
- g. Click **Submit**.

- Make T2 and T3 members of T1
  - a. Click **Target groups**.
  - b. Click **Search** then type in T.
  - c. Click **Submit**.
  - d. Select T2 and T3 then click **Manage Group Membership**.
  - e. In the target group list, select T1.

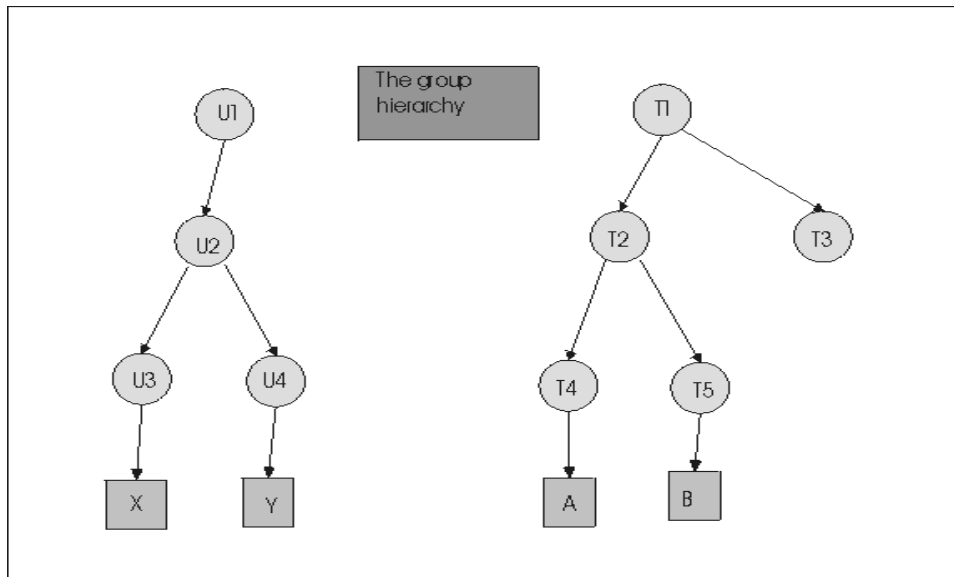


**Note:** Make sure that T1 is the only target group that is selected.

- f. Select **add to current group membership**.
  - g. Click **Submit**.
6. Create permissions links between specific user and target groups. Remembering to enable all relevant policies. Create the links in the following examples.

The following figure shows the group hierarchy that is created.

Figure 1. Group tree diagram



### Example 1: Standard priority 0 permissions

When the groups are created, a standard permissions template is defined for U1 and T1. To change any values for the group, use the **Edit group** action. In this example, edit the values for user group U1. Set **Chat** to Yes and everything else to No. In target group T1, Chat and Monitor are set to Yes and everything else is set to No.

Edit user group U1

1. Click **User groups**.
2. Select **Search**
3. Type in U1 in the input field.
4. Click **Submit**.
5. Select U1 and click **Edit group**.
6. Click **Edit Settings**.
7. Select **Yes** for Chat. Select **No** for everything else.
8. Select **Save as new template named** and type in **AllowChat** for the template name.
9. Click **Submit**.

### Edit target group T1

1. Click **Target groups**.
2. Select **Search**.
3. Type in T1 in the input field.
4. Click **Submit**.
5. Select T1 and click **Edit group**.
6. Click **Edit Settings**.
7. Select **Yes** for Chat and Monitor. Select **No** for everything else.
8. Select **Save as new template named** and type in **AllowChatMonitor** for the template name.
9. Click **Submit**.

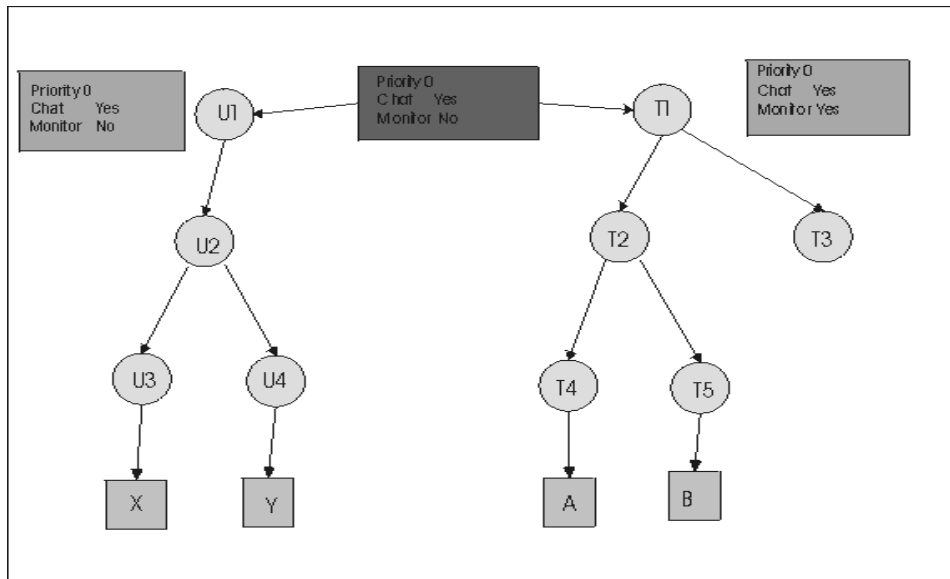
Within **Manage Permissions** when a relationship is created between U1 and T1, all enabled policies are set to priority 0. The reason for the priority 0 value is because there are no higher priority permission values enabled.

### Create the Permissions link

1. Click **Target groups > All target groups**.
2. Select T1.
3. Click **Manage Permissions**.
4. The Manage Permissions screen is displayed.
5. Click the **Group Browser** button if not selected.
6. Click the selector button next to user group then select U1.
7. Click the selector button.
8. Click the selector button next to target group then T1.
9. Click the selector button.
10. The set of permissions and their selected values, which are derived from the combination of standard policies that are defined for U1 and T1, is displayed.
11. Click the **Enabled** check box to make the policies available.
12. Click **Submit**

The following figure shows the group hierarchy and permissions links

Figure 2. Standard priority 0 permissions



Determine session permissions for example 1

User X is a member of group U3, U2, and U1

User Y is a member of group U4, U2, and U1

Target A is a member of group T4, T2, and T1

Target B is a member of group T5, T2, and T1

Using [Figure 2: Standard priority 0 permissions \(on page 127\)](#) and the policy engine process, there are parent and grandparent groups. However, there is only one permissions link defined in the group hierarchy between U1 and T1. Therefore, the policies and values within this link are assigned for a remote control session. The resultant permissions set allows users X and Y to initiate Chat only sessions with targets A and B.



**Note:** Monitor is set to No because the priority 0 No value that is set for group U1 overrides the priority 0 Yes value that is set for group T1.

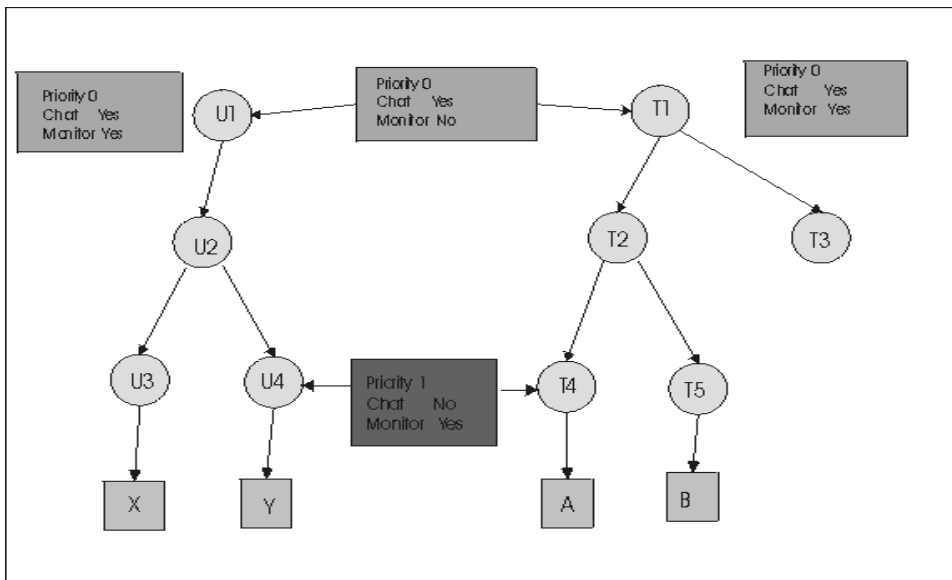
## Example 2: Higher priority permissions

When groups U4 and T4 are created, the default template is accepted as the standard set of permissions. Create a relationship in **Manage Permissions** between U4 and T4 and select a higher priority No for Chat and higher priority Yes for Monitor.

Create the Permissions link

1. Click **Target groups > All target groups**.
2. Select T4
3. Click **Manage Permissions**.
4. The Manage Permissions screen is displayed.
5. Click the **Group Browser** button if not selected.
6. Click the selector button next to user group then select U4. Group list must be expanded.
7. Click the selector button.
8. Click the selector button next to target group then T4. Group list must be expanded.
9. Click the selector button.
10. The set of permissions and their selected values, which are derived from the combination of standard policies that are defined for U4 and T4 is displayed.
11. Click the **Enabled** check box to make all of the policies available.
12. Set priority 1 for Chat and select No, set priority 1 for Monitor, and select Yes. Set Guidance, Active, and File transfer to No.
13. Click **Submit**.

Figure 3. Higher priority permissions



Determine Permissions for example 2.

User X is a member of group U3, U2, and U1.

User Y is a member of group U4, U2, and U1.

Target A is a member of group T4, T2, and T1.

Target B is a member of group T5, T2, and T1.



Using [Figure 3: Higher priority permissions \(on page 128\)](#) and the policy engine process, there are parent and grandparent groups and multiple permissions links defined in the group hierarchy. The following permissions are applied for each example session.

#### Session with user X and target A

The only permissions link considered for user X and target A is the one between U1 and T1. User X is not a member of U4. Therefore, user X can start a Chat session with target A but not a Monitor session.

#### Session with user X and target B

Only the link between U1 and T1 is considered as user X is not a member of U4 and target B is NOT a member of T4. Therefore, user X can start a Chat session with target A but not a Monitor session.

#### Session with user Y and target A

There are two permissions links to be considered this time: U1 to T1 and U4 to T4. Therefore, user Y can start a Monitor session with target A but not a Chat session. The priority 1 value set in the link between U4 to T4 overrides the priority 0 value set in the link between U1 and T1.

Priority 1 No overrides priority 0 Yes.

Priority 1 Yes overrides priority 0 No.

#### Session with user Y and target B

The only permissions link that is considered for these two entities is the one between U1 and T1. Target B is not a member of T4. Therefore, user Y can start a Chat session with target B but not a Monitor session.



**Note:** The same explanation applies if the priority values that are set in the U4↔T4 link are set to 5. Priority 5 overrides priority 1. Priority 1 overrides 0.

## Example 3: Only relationship permissions are inherited

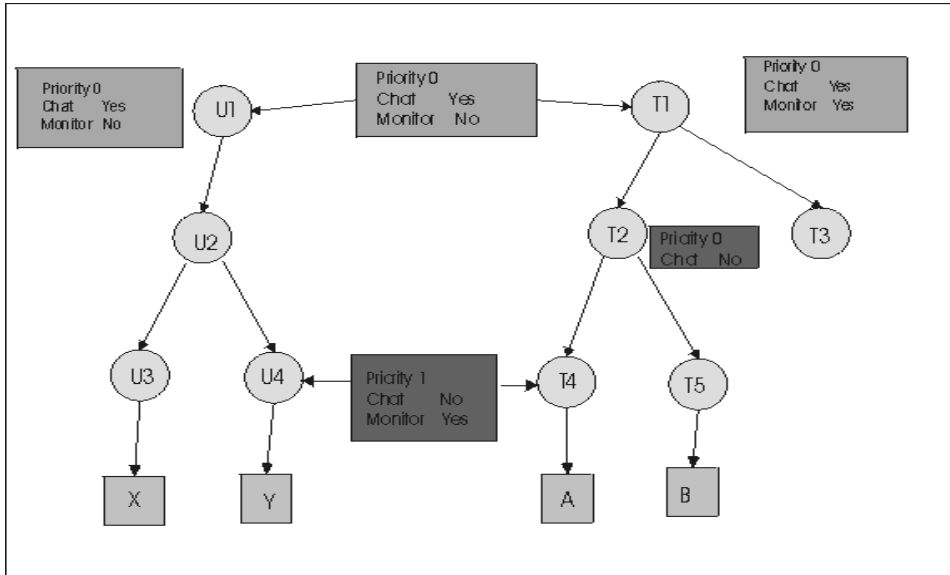
Edit the target group T2 and change the standard permission value for Chat to No.

Edit target group T2

1. Click **Target groups > Search**.
2. Type in T2 in the input field.
3. Click **Submit**.
4. Select T2 and click **Edit group**.
5. Click **Edit Settings**.
6. Select **No** for everything, including Chat.
7. Select **Save as new template named** and type in `NoChat` for the template name.
8. Click **Submit**.

In [Figure 4: Only relationship permissions inherited \(on page 130\)](#) there are parent and grandparent groups, and there are multiple permission links defined in the group hierarchy. The following permissions are applied for each example session.

Figure 4. Only relationship permissions inherited



### Determine permissions for example 3

User X is a member of group U3, U2, and U1.

User Y is a member of group U4, U2, and U1.

Target A is a member of group T4, T2, and T1.


Target B is a member of group T5, T2, and T1.

#### Session with user X and target A

The only permissions link that is considered for these two entities is the one between U1 and T1. User X is not a member of U4. Therefore, user X can start a Chat session with target A, but not a Monitor session.

Priority 1 No overrides priority 0 Yes.

Priority 1 Yes overrides priority 0 No.

 **Note:** The standard permissions for group T2 have Chat set to priority 0 No. This value overrides standard Yes. However, because there is no permission link with T2 and any other group, its values are not considered. It is the policy values in permissions links only that are inherited.

**Session with user X and target B**

Only the link between U1 and T1 is considered. User X is not a member of U4 and target B is not a member of T4. Therefore, user X can start a Chat session with target B but not a Monitor session. The T2 permissions are not considered in this example.

**Session with user Y and target A**

There are 2 permissions links to be considered. U1 to T1 and U4 to T4. Therefore, user Y can start a Monitor session with target A. The priority 1 value in the link between U4 to T4 overrides the priority 0 value in the link between U1 and T1. Group T2 policies and permissions are not considered as there are no permissions links set up between it and any other groups.

**Session with user Y and target B**

The only permissions link that is considered for these 2 entities is the one between U1 and T1. Target B is not a member of T4. The value of priority 0 No in the standard set for T2 would override the U1 to T1 priority 0 Yes if T2 was linked to another group. As it is not, the value is not considered. Therefore, user Y can start a Chat session with target B, but not a Monitor session.

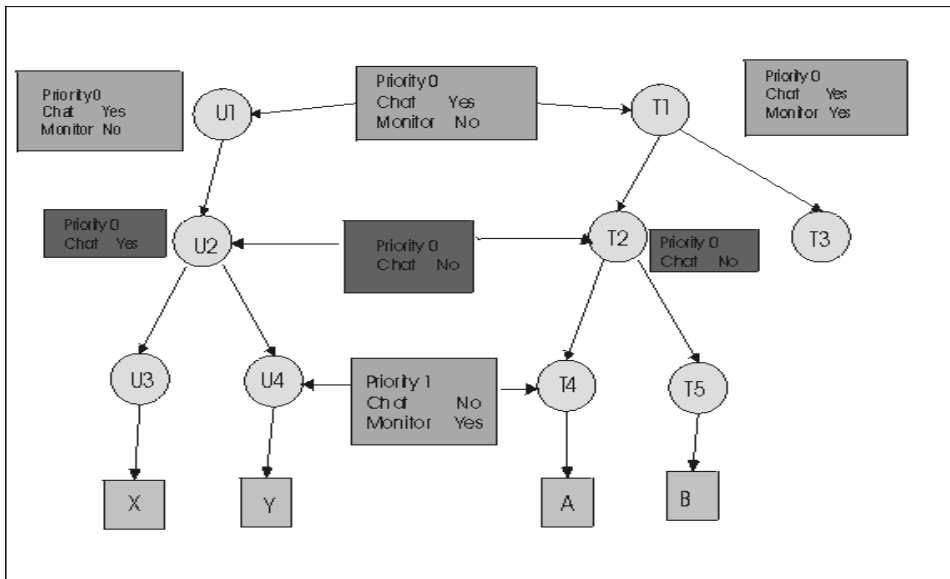
**Example 4: No overrides Yes when priority values are the same**

Create a link in **Manage Permissions** between groups U2 and T2 with priority 0 permissions and Chat set to No.

Create the Permissions link.

1. Click **Target groups > All target groups**.
2. Select T2.
3. Click **Manage Permissions**.
4. The Manage Permissions screen is displayed.
5. Click the **Group Browser** button.
6. Click the selector button next to user group then select U2. Group list needs to be expanded.
7. Click the selector button.
8. Click the selector button next to target group then T2.
9. Click the selector button.
10. The set of permissions and the values, that are derived from the combination of standard policies for U2 and T2 are displayed.
11. Make the policies available by clicking the **Enabled** check box.
12. Set the value for Chat to `priority 0 No`, Monitor to `priority 0 Yes` and Guidance, Active and File Transfer to Yes
13. Click **Submit**

Figure 5. No overrides Yes when priority values are the same



Determine permissions for example 4

User X is a member of group U3, U2, and U1.

User Y is a member of group U4, U2, and U1.

Target A is a member of group T4, T2, and T1.

Target B is a member of group T5, T2, and T1.

Using [Figure 5: No overrides Yes when priority values are the same \(on page 132\)](#) and the policy engine process, there are parent and grandparent groups, and there are multiple permissions links defined in the group hierarchy. The following permissions are applied for each example session.

#### Session with user X and target A

There are 2 permissions links to be considered for these two entities. The link between U2 and T2 and the link between U1 and T1. Both links have priority 0 permissions set. U2 ⇔ T2 has Chat set to priority 0 No and U1 ⇔ T1 has Chat set to priority 0 Yes. Therefore, user X cannot start a Chat session or a Monitor session with target A. The priority 0 No for Chat in U2 to T2 overrides the priority 0 Yes for Chat in U1 to T1.



**Note:** The link between U4 and T4 is not considered as user X is NOT a member of group U4.

#### Session with user X and target B

Only the links between U2 and T2 and U1 and T1 are considered. User X is not a member of U4 and target B is not a member of T4. Therefore, user X cannot start a Chat session or a Monitor session with target B.

### Session with user Y and target A

There are 3 permissions links to be considered. U1 to T1, U2 to T2, and U4 to T4. Therefore, user Y can start a Monitor session with target A. The priority 1 value set in the link between U4 to T4 override the priority 0 values set in the link between U1 and T1. A Chat session cannot be started because the priority 1 value No, set for Chat in the U4 to T4 link, overrides the priority 1 No in the U2 to T2 link and the priority 0 Yes in the U1 to T1 link.

### Session with user Y and target B

There are 2 permission links considered for these two entities. U2 to T2, and U1 to T1. Therefore, user Y cannot start a Chat session or a Monitor session with target B. The priority 0 No value for Chat in the link between U2 to T2 overrides the priority 0 Yes value for Chat in the link between U1 to T1.



**Note:** The link between U4 and T4 is not considered as target B is not a member of group T4.



**Note:** The same explanation applies if the priority for Yes and No is both set to 1 or 5. No overrides Yes when the priority values are the same.

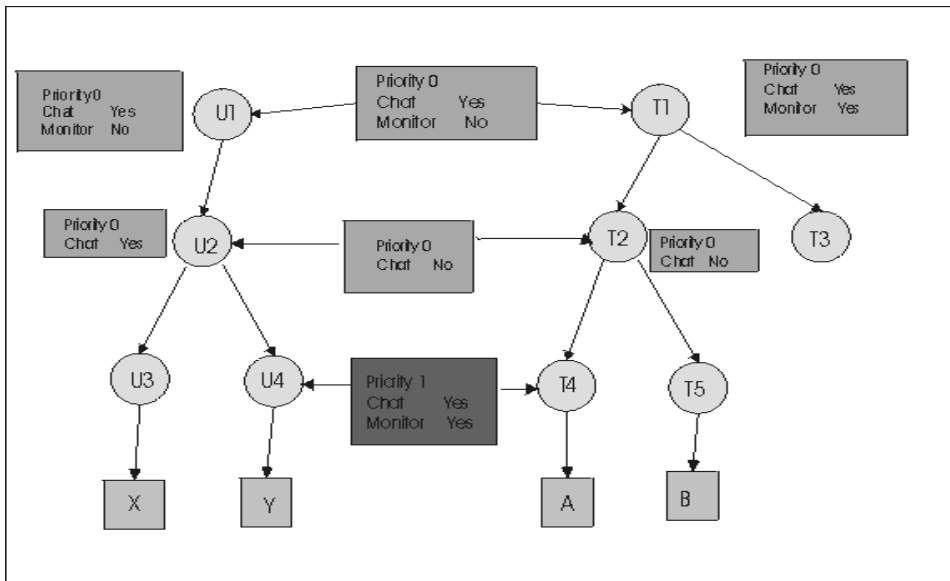
## Example 5: Higher priority Yes overrides lower priority No

Edit an existing link in **Manage Permissions** to change the value of the priority 1 link that is defined between U4 and T4. Change the value of Chat from No to Yes.

Edit the Permissions link

1. Click **Target groups > All target group**.
2. Select T4.
3. Click **Manage Permissions**.
4. The Manage Permissions screen is displayed.
5. Click the **Existing Profile** button.
6. Select the link between U4 and T4.
7. Click the selector button.
8. Keep the priority 1 option selected for Chat. Select the value Yes.
9. Click **Submit**.

Figure 6. Higher priority Yes overrides lower priority No



Determine permissions for example 5

User X is a member of group U3, U2, and U1.

User Y is a member of group U4, U2, and U1.


Target A is a member of group T4, T2, and T1.

Target B is a member of group T5, T2, and T1.

Using [Figure 6: Higher priority Yes overrides lower priority No \(on page 134\)](#) and the policy engine process, there are parent and grandparent groups, and there are multiple permissions links defined in the group hierarchy. The following permissions are applied for each example session

**Session with user X and target A**

There are 2 permissions links to be considered for these two entities. The link between U2 and T2 and the link between U1 and T1. Both links have priority 0 permissions set. U2 to T2 has Chat set to No and U1 to T1 has Chat set to Yes. Therefore user X cannot start a Chat session or a Monitor session with target A. The priority 0 No for Chat in U2 to T2 overrides the priority 0 Yes for Chat in U1 to T1.

 **Note:** The link between U4 and T4 is not considered as user X is not a member of group U4.

**Session with user X and target B**

Only the links between U2 and T2 and U1 and T1 are considered. User X is not a member of U4 and target B is not a member of T4. Therefore, user X cannot start a Chat session or a Monitor session with target B.

### Session with user Y and target A

There are 3 permissions links to be considered. U1 to T1, U2 to T2, and U4 to T4. Therefore, user Y can start both a Monitor session and a Chat session with target A. The priority 1 values that are set in the link between U4 to T4 override the priority 0 values that are set in the link between U1 and T1.

### Session with user Y and target B

There are 2 permissions links considered for these two entities. The link between U2 to T2 and U1 to T1. Therefore, user Y can start a Chat session with target B but not a Monitor session. The priority 0 No value for Chat in the link between U2 to T2 overrides the priority 0 Yes value for Chat in the link between U1 to T1.



**Note:** The link between U4 and T4 is not considered as target B is not a member of group T4.



**Note:** The same explanation applies if the priority value is set to 5 in the U4 ⇔ T4 link. Priority 5 overrides 1. 1 overrides 0.

## In summary

- Users and targets must be members of user and target groups to be able to establish remote control sessions.
- Permissions links must be set up between the relevant user and target groups.
- All required policies must be enabled in the permissions links.
- If there is only one permissions link defined in the group hierarchy, it is the policies and permissions that are defined in this link that are applied to the remote control session.
- If there are multiple permissions links defined in the group hierarchy the final set of session policies is derived by using the following rules.
  - Priority 5 No overrides all other values.
  - Priority 5 Yes overrides priority 0 No and priority 1 No.
  - Priority 1 No overrides priority 0 Yes and priority 1 Yes.
  - Priority 1 Yes overrides priority 0 No
  - Priority 0 No overrides priority 0 Yes
- If you change policy values by using the **Edit group** feature, the new values are only valid in new permissions link that you create for the group. They are not valid for existing permissions links. Therefore, to you must change the policy values in the links by using **Manage Permissions**.

# Chapter 13. Starting a managed session by using an installed controller

When you start a managed session, you can configure the server to use an installed controller rather than using the Java™ Web Start method. Note that the Java™ Web Start plugin method is deprecated in Remote Control starting from Version 10.0.0 Update 8 (Build Number 0802). This feature makes starting a session faster and it removes any warning message windows that are displayed while the session is starting.

To use this feature, the controller component must be installed on the controller system before you start a remote control session.

Use the **always.use.preinstalled.controller** property in the `trc.properties` file to control this feature. When the property is set to true and you start a managed session, a `.trcjws` file is now created rather than a `.jnlp` file. This feature removes the dependency on using the system JRE when you start a managed session.

1. In the server UI click **Admin > Edit properties file**.
2. Select `trc.properties`.
3. Set **always.use.preinstalled.controller** to *true* and click **Submit**.
4. Click **Admin > Reset Application**

When you start a managed session the controller that is installed is used instead of the Java™ Web Start method.



**Note:** The property has no effect when FIPS or NIST SP800-131A compliance is enabled on the server. The controller that is installed is always used when FIPS or NIST SP800-131A compliance is enabled.



# Chapter 14. Manage permission sets for temporary access to targets

When a controller user requests temporary access to a target, you can respond to the request and define what the controller user is allowed to do during the session. As part of this process you must enable and set values for the policies for the temporary session. You can define a set of policies and permissions that can be saved and used to set the temporary permissions. Thus removing the need for enabling the required policies every time you grant a new request. Use the **Permissions Sets** option in the BigFix® Remote Control Server to create the permissions. For more information about how to respond to a temporary access request, see [Requests for temporary access to targets \(on page 140\)](#).

## Creating a set of permissions

You can create a set of permissions that can be saved and used to define the policies and permissions for a temporary access request session.

To create a set of permissions, complete the following steps in the BigFix® Remote Control Server:

1. Click **Admin > New Permission Set**.

The **Edit Permission Set** screen is displayed.

2. Type in a name for the permissions set in the **Set Name** field.
3. Choose the appropriate method for enabling the policies

- To enable every policy, click **Enabled?**.
- Select the check box next to each policy that you want to enable.

4. Set the priority for each enabled policy.

The default priority value is the value that is displayed first in the list when the **Edit Permission Set** screen is displayed and is set by the **trc.default.request.priority** property in **trc.properties** file. For more information about editing the properties files, see [Editing the properties files \(on page 215\)](#).

**5**

This value is the highest priority. This value overrides any existing policies that might exist between the user and target.

**1**

This value overrides any existing priority 0 policies that might exist between the user and target.

**0**

This value is the lowest priority. Any existing policy in effect between the user and target that is of a higher priority overrides this policy.

5. Set or enter a value for the enabled properties.

For more information about the definitions and values for the policies, see [Server session policies \(on page 95\)](#).

**Set to Yes**

The policy is in effect during the temporary session. depending on the priority that is set for it.

#### **Set to No**

The policy is not in effect during the temporary session. However, if the priority is set to 0 or 1, an existing policy of priority 5 Yes overrides this No value.

6. Click **Submit**.

The permissions set is created. You can select the set whenever you are granting a temporary access request so that you can enable and set values for specific policies without having to manually select each one.

## Viewing sets of permissions

After you create sets of policies and permissions, you can view the list of sets by using the **View Permissions Sets** option.

To view the list of permissions sets, click **Admin > All Permission Sets**.

The **View Permissions Sets** screen is displayed. All defined permissions sets are listed.

## Modifying a defined set of permissions

You can edit a set of permissions to change the following information

- The name of the set.



**Note:** Duplicate names are not allowed.

- Enable or disable policies.
- Set or change priority levels.
- Set or change the policy value.

To edit a set of permissions, complete the following steps:

1. Click **Admin > All Permission Sets**.
2. Select the permissions set.
3. Select **Edit Permission Set** from the **Actions** list on the left.
4. Make the changes to the policies.
5. Click **Submit**.

The changes are saved to the selected set of permissions.

## Deleting permission sets

You can remove one or more defined sets of permissions if they are no longer required by using the **Delete Permission Set** action.

To remove sets of permissions, complete the following steps:

1. Click **Admin > All Permission Sets**.
2. Select the permissions sets.
3. Select **Delete Permission Set** from the **Actions** list on the left.
4. On the **Confirm Deletion** screen, click **Submit**.

The selected permission sets are deleted.

# Chapter 15. Requests for temporary access to targets

Users can start a remote control session only with the targets that they have permission to access. The access is defined through their group membership and the relationships that are set up between the groups. However, a user can request temporary access to one or more targets that they do not normally have access to. When a request for temporary access is received it is known as an outstanding access request, with a status of pending. These requests are listed in the outstanding requests list in the BigFix® Remote Control Server. When you grant the request it becomes a live request, with a status of granted and is moved to the live requests list. If you refuse the request, its status changes to rejected and it is removed from the outstanding list. However, all outstanding, live, or denied requests are also displayed in the **All access requests** list. The requests remain there until they expire or are removed by the cleanup task that runs periodically to delete expired or no longer required requests. Email functions must be enabled in order for the notification process to take place. For more information, see [Setting up email \(on page 48\)](#).

## Handle a request for temporary access to targets

When a user creates a request for temporary access to target systems, an email is sent to the administrator or a group of administrators to inform them of the request.

Display the **Outstanding requests** list to view this new request and determine its outcome by using one of the following actions

- Grant
- Deny
- Delete

When a request is submitted, the recipient of the email is determined by property values in the `trc.properties` file. You can create a user group and assign to it, the specific users with admin authority who can receive the email. The property `trc.ticket.admin` must be set to the user group name that you create. If this property is not assigned a value, it is the admin user whose email address is set in the `email.admin` property that receives the email. For more information about editing the properties files, see [Editing the properties files \(on page 215\)](#).

## Give users temporary access to target systems

You can allow users to temporarily access targets by granting a request for access. When you grant a request you can define what the user is allowed to do during the session. You can set the policies and permissions that are effective during the temporary access, provide the user with any additional information that you think might be relevant, and set a date and time period that the access is valid for. Use the **show effective policies** option to check whether there are existing policies set for the user and target that must be considered when you set the policies for the temporary access to the target.

Allowing temporary access can be carried out in three ways

1. Grant an outstanding access request.
2. Grant a denied request.
3. Grant an anonymous request.

## **Granting an outstanding access request**

When you receive an email that informs you that a request for temporary access is submitted, you can see the request by looking in the **Outstanding Access Requests** list.

To grant temporary access, complete the following steps:

1. Click **Reports > Outstanding Access Requests**.
2. Select the request.
3. Select **View/Edit Request** from the **Actions** list on the left.  
The **Manage Access to Target** pane is displayed. The **Requested access requirements** section displays the things that the user requested.
4. Click the arrow button next to the target name at **Request Targets** to view effective policies and check whether there are any existing policies set for the user and target.  
Any existing policies that are set for the user and target, must be considered when you set the policies and permissions for the temporary access.
5. Click **Cancel** to return to the **Manage Access to Target** screen.
6. Use the **Specify access allowed** pane to set the policies and time period for the access.

### **Setting the permissions effective during the session**

You can enable and set the policies and permissions that are effective during the temporary session by using an already defined permission set or by enabling individual policies. Choose the appropriate method for setting the policies.

- a. **Permissions Set** - Use an already defined set of permissions.
  - i. Select a defined set of permissions from the list
  - ii. Click the arrow button next to **Permissions**, to show the policies, and permissions that are set. You can also change any of the values.

For more information about permissions sets, see [Creating a set of permissions that can be applied to a group \(on page 178\)](#).

- b. **Permissions** - Manually enable each policy.
  - i. Click the arrow button next to **Permissions**.
  - ii. Choose the appropriate method for enabling the policies.
    - To enable every policy, click **Enable all**. You must select this option if there are existing policies set.
    - To enable some policies, select the check box next to each policy that you want to enable. It is important to enable all policies that you want,

particularly if there are existing permissions set between the user and the target. Any existing policy that is not enabled is not in effect in the temporary session.

- c. Set the priority for each enabled policy. The default priority value is the value that is displayed first in the list and is set by the **trc.default.request.priority** property in **trc.properties** file. For more information about editing the properties files, see [trc.properties \(on page 216\)](#).

**5**

This value is the highest priority. This value overrides any existing priority 0 and priority 1 policy that might exist between the user and target.

**1**

This value overrides any existing priority 0 policy that might exist between the user and target.

**0**

This value is the lowest priority. Any existing permission that is in effect between the user and target that is of a higher priority, overrides this policy. Therefore, you must set the policy to a higher priority value if there are existing permissions.

- d. Set or enter a value for the enabled properties. For more information about definitions and values for the policies, see [Server session policies \(on page 95\)](#).

#### **Set to Yes**

The policy is in effect during the temporary session if there are no existing permissions set up between the user and target. If there are existing permissions, the priority value determines whether the policy is in effect.

#### **Set to No**

The policy is not in effect during the temporary session if there are no existing permissions set up between the user and target. If there are existing permissions, the priority value determines whether the policy is in effect. If the priority is set to 0 or 1, an existing policy of priority 5 Yes overrides the No value and the policy is in effect for the temporary session.

#### **Admin Notes®**

Type in here any relevant additional information. For example, to inform the user of the time that the session is valid for if it is different from the requested time.

For example : Session is valid today between 12:00:00 and 14:30:00.

#### **Starting on**

- a. Select from the calendar or type the date, in the format **yyyy-mm-dd**, on which you want the access to commence.
- b. Type in a time in the format **hh:mm:ss** that you want the access to commence.

#### **Ending on**

- a. Select from the calendar or type the date, in the format **yyyy-mm-dd**, on which you want the access to end.
- b. Type in a time in the format **hh:mm:ss**, that you want the access to end.

7. Click **Grant**.

An email is sent to the requesting user to inform them that the request for temporary access is granted. The request is saved to the **Live access requests** list.

### **Granting an already denied access request**

If you deny a request for temporary access, you can modify the request and change the status of the request to granted. When you change the status of the request, you can also define what access is allowed and when the access is allowed.

To grant an already denied request for temporary access, complete the following steps:

1. Click **Reports > All Access Requests**.
2. Select the request.
3. Select **View/Edit request** from the **Actions** list on the left.
4. Go to step 6 ([on page 141](#)), to complete the details for the request.

An email is sent to the requesting user to inform them that the request for temporary access is granted. The request is saved to the **Live access requests** list.

### **Granting an anonymous request**

An anonymous request is a request for temporary access that is made by a user who is not registered in the BigFix® Remote Control Server. The user must provide details of the targets that they are requesting access to. You must search for these targets to determine whether the temporary access can be allowed.

To accept an anonymous request for temporary access, complete the following steps:

1. Click **Reports > Outstanding Access Requests**.
2. Select the request.
3. Select **View/Edit request** from the **Actions** list on the left.
4. The **Manage Access to Targets** screen is displayed. No targets are selected.
5. Specify the access that is allowed.
  - Use the justification from the user to determine the targets that are being requested.
  - Choose the appropriate method to select targets.

### Select Targets

- a. Click **Select Targets**.
- b. Select one or more targets from the **Search targets** list.
- c. Click **Submit**. The target name is displayed.

### Select Target Groups

- a. Click **Select Target Groups**.
- b. Select one or more target groups from the **Search** list.
- c. Click **Submit**.

All targets that are members of the selected groups are displayed.

6. Go to step 6 ([on page 141](#)), to complete the details for the request.

An email is sent to the user to inform them that their request is granted. The email contains a link to the Remote Control application so that they can access the targets.

## Revoking requests for temporary access to target systems

After a request is granted, you can update the request to refuse the access by using the **Revoke** option.

To revoke a request for temporary access to a target, complete the following steps:

1. Click **Reports > Live Access Requests**.
2. Select the request.
3. Select **View/Edit request** from the **Actions** list on the left.

The **Manage Access to Target** screen is displayed but as the status is granted, the policies and permissions that were set for the temporary access are not displayed.

4. To change any of the policies for the request, click the **Manage Permissions** link to view the policies that are set. To change the policies, complete steps 5 ([on page 118](#)), to 9 ([on page 119](#)).

If you do not need to change the policies, click **Revoke**. If you click **Cancel** on the **Manage Permissions** screen, any changes that are made to the policies are not saved.

An email is sent to the requesting user to inform them that the request for temporary access is no longer allowed. The request is removed from **Live access requests** list.

## Denying requests for temporary access to target systems

When a request for temporary access to targets is received, you can refuse the request by using the **Deny** option.

To deny a request for temporary access to a target, complete the following steps:

1. Click **Reports > Outstanding Access Requests**.
2. Select the request.



3. Select **View/Edit request** from the **Actions** list on the left.
4. In the **Admin Notes** field, type a reason for denying the request.
5. Click **Deny**.

An email is sent to the requesting user to inform them that the request for temporary access is rejected. The request is removed from the **Outstanding Access Requests** list.

## Delete requests for temporary access to target systems

You can remove requests for access that are no longer required by using the **Delete** option. You can delete requests in multiple ways.

- Select requests from a list of requests.
- When you are viewing or editing a request.

### Deleting access requests from a request list

To remove requests from a list of requests, complete the following steps:

1. Click **Reports** then one of the following items.
  - **Outstanding Access Requests.**
  - **Live Access Requests.**
  - **All Access Requests.**
2. Select the requests.
3. Select **Delete Request** from the **Actions** list on the left.
4. On the **Confirm Deletion** pane, click **Submit**.

The selected requests are removed from the Remote Control database.

### Deleting access requests while editing a request

To remove a request when you are viewing or editing it, complete the following steps:

1. Click **Reports** . Click one of the following items.
  - **Outstanding Access Requests.**
  - **Live Access Requests.**
  - **All Access Requests.**
2. Select the requests.
3. Select **View/Edit Request** from the **Actions** list on the left.
4. Click **Delete** on the **Manage Access to Target** pane.

The request is removed from the Remote Control database.

## View requests for temporary access to target systems

When requests for temporary access to targets are submitted, you can view the lists of the requests for reporting purposes. There are multiple ways to view the requests.

- View outstanding access requests.
- View live access requests.
- View all access requests.

### Viewing outstanding access requests

When requests for temporary access to targets are first received, they are known as outstanding access requests. The status of these requests is set to pending.

To view the **Outstanding Access Requests** list click **Reports > Outstanding Access Requests**.

The list of all outstanding access requests is displayed.

### Viewing live access requests.

When requests for temporary access to targets are granted, they are known as live access requests. The status of these requests is set to granted.

To view the **Live Access Requests** list click **Reports > Live Access Requests**.

The list of all live access requests is displayed.

### Viewing all access requests.

Unless a request for access is deleted, it remains in the Remote Control database until the defined time period for it expires. Up to that point it can be set to three different states. To show all defined requests for access and their states you can use the **All access requests** option. The state of the request is listed as a number and corresponds to the following values

**0**

The request is pending and must be addressed. It is also displayed in the outstanding requests list.

**1**

The request is granted. It is also displayed in the live access requests list.

**2**

The request is rejected.

To view the **All Access Requests** list, click **Reports > All Access Requests**.

The list of all access requests is displayed.

# Chapter 16. Generate custom reports

Two types of reports can be generated in the Remote Control server. Common reports are reports that are provided with the application. The reports are aimed at generating general information that you might need on a more regular basis. You can run the reports from the menus in the BigFix® Remote Control Server UI. Custom reports are reports that you create or modify to generate information specific to your own environment.



**Note:** A report manager is used for controlling the output of the reports. The output from the reports is cached. Therefore, the application does not need to go back and reload the data from the database, the next time that the report is run. The cached results are displayed more quickly. There are three properties in the `trc.properties` file that you can use to set the interval for reloading of the data from the database.

- `report.timeout.frequency`
- `report.manager.frequency`
- `report.manager.period`

For more information about the properties, see [trc.properties \(on page 216\)](#).

The **Refresh** link on the upper right of the screen can be used to reload the output of a report to show any changes in the data.

## Create a Custom Report

Custom reports are created by a Super User or Administrator and are useful for generating reports that specifically meet the needs of their environment. To generate a custom report, a customized SQL query is run against the database and its output is displayed on screen.

Custom reports can be created in multiple ways:

- By sorting, filtering, or removing columns from a generated report, to meet your own requirements.
- By directly editing the SQL that is used to generate the report. You must understand how to use SQL to complete this method.
- By creating a new report by using the Edit SQL feature to build a query by adding required tables and columns. This method can be done in multiple ways:
  - Select **Reports > New** to create a new report.
  - Use an existing report as the basis for the new report.

You must understand SQL for this method. For more information about the database tables, see [Database table and column descriptions \(on page 366\)](#).

- By adding database tables and columns to existing reports.

## Creating a report by sorting and filtering

You can create a custom report by sorting and filtering the columns of an already defined report. Generate the report that is used as the basis for your new report and then use the sort, or filter option on the generated report.

To create the custom report, complete the following steps:

1. Generate the report from the menus by completing the following steps:
  - a. Click the menu that contains the report.  
For example, the **Targets** menu or **All Custom Reports**.
  - b. Click the report.  
For example, **All Targets**.
2. You can customize the report by performing any of the following actions:
  - **Sort, Move or delete a column**
    - a. Click the heading of the column that you want to work on. An icon with four arrows is displayed at the top of the column.
    - b. Hover the mouse over the icon to display the actions.
      - Sort up (Ascending) - click the up arrow.
      - Sort down (Descending) - click the down arrow.
      - Move the column to the left - click the left arrow.
      - Move the column to the right - click the right arrow.
      - Delete the column - click the cross in the center.



**Note:** If the key column of a report is deleted, some of the actions in the menu on the left are not available.

- c. The report is redisplayed in the order you selected.
  - **Filter a column**
    - If you click any cell in the report, the column is limited to the value that you select.  
  
For example: If you select IBM® in the **Manufacturer** column when **All Targets** is displayed, only the targets that are manufactured by IBM® are redisplayed.
  - Repeat step 2 ([on page 148](#)) until you have the report to your requirements
3. To save the new report, complete the following steps:
  - a. Click **Reports > Save As Custom Report**.
  - b. Change the name in the **Query name** field to one relevant for the new report.
  - c. Change or delete the description in the **Description** field.
  - d. Enter a menu name.

This name is displayed in the **Custom Reports** menu.

e. Select any groups that can have access to this report.



**Note:** The created report is displayed only in the **Custom Reports** menu of the Admin user or Super User who created the report. If groups are selected, the report is also displayed in the **Custom Reports** menu of any users who are members of the selected groups.

f. Click **Submit**.

The report is displayed and its name is displayed in the **Custom Reports** menu.

## Creating a report by editing the SQL statement

If you know SQL, you can create a custom report by editing the SQL query that is used to generate an existing report. To edit the SQL, complete the following steps:

1. To generate your base report, perform step 1 ([on page 148](#)) . Generate the base Report
2. Click **Reports > Save custom query**.
3. In the **SQL data** field, make the changes to the SQL.
4. There are 2 options available now.
  - To check the output of the report, go to step 5 ([on page 149](#)).
  - To save the report go to step 7 ([on page 149](#)).
5. Click **Run Report**.
6. If the generated report is what you require, go to step 7 ([on page 149](#)), otherwise, complete the following actions.
  - Click **Reports > Save As Custom Report**.
  - Repeat from step 3 ([on page 149](#)) until the report meets your requirements.
7. Select **Reports > Save custom query**.
8. Change the name in the **Query name** field to one relevant for the new report.
9. Change or delete the description in the **Description** field.
10. Enter a menu name. This name is displayed as a menu item in the **Custom Reports** menu.
11. Select any groups that can have access to this report.



**Note:** The created report is displayed only in the **Custom Reports** menu of the Admin user or Super User who created the report. If groups are selected, the report is also displayed in the **Custom Reports** menu of any users who are members of the selected groups.

12. Click **Submit**.

Your custom report is created.

## Create a report by using the Edit SQL feature

Using the Edit SQL feature, you can create a query, by adding the required tables, columns, and any specific search conditions to generate your report. For more information about the Remote Control database table names and columns, see [Database table and column descriptions \(on page 366\)](#).

You can use the Edit SQL feature in two ways:

- Select **Reports > New**.
- Edit the SQL of an existing report.

In the set of windows that are used in **Edit Report**, click **Submit** only when you finish creating and adding things to your report. Otherwise, click **Back** to return to the main **Edit Report** window to continue modifying your report.

### Selecting the **New** option in the **Reports** menu to create a new report

1. Click **Reports > New**.
2. On the screen that is displayed, on the upper right, click **Edit SQL**.
3. On the **Edit Report** window, select **Add Table** to start building the query for the new report.
4. On the **Add Tables** window, select the table and click **Add**.  
For example, *COMMON.USER\_GROUP*.
5. Repeat from step 3 ([on page 150](#)) to add more tables if you require.
6. Click **Back** to return to the **Edit Report** window.
7. Click **Add Column** to select the columns to be displayed in the report.  
The **Modify Report Columns** window is displayed. The **Add Column** option is applicable only if more than one table is selected for the report. If you select one table only, the list is blank and the next step is not required.
8. From the list, select a column and click **Add**.
9. Repeat from step 8 ([on page 150](#)) until all columns are added.
10. Click **Back** to return to the **Edit Report** window.
11. To delete a column, complete the following steps:
  - a. Select **Delete Column**.
  - b. On the **Delete Report Columns** window, select the column and click **Delete**. Repeat this step to delete more columns. In this example, click **Delete** until the first column in the list is **GROUP\_KEY**.
  - c. Click **Back** to return to the **Edit Report** window.
12. To re arrange the report columns complete the following actions:
  - a. Select **Arrange Columns** on the **Edit Report** window.
  - b. On the **Order Columns** screen, select the column from the list and click **<** or **>** to move the columns to the left or the right.  
In this example, select **USER\_GROUP.NAME** then click the left arrow button until the column is first in the list. Repeat this step to re arrange more columns.
  - c. Click **Back** to return to the **Edit Report** window.

13. To specify a condition in your query, complete the following steps:

- Click **Modify conditions** on the **Edit Report** window.
- On the **Modify Report Limits** window, choose the appropriate method to select a limit.
  - Click **Quick Limits** to select an already defined limit from the list.
    - Click **Add** to add this condition to your query.
    - Click **Back** to return to the **Edit Report** window.
  - Click **Add**, to create an **AND** or **OR** condition for one of the columns in your query.

```
For example AND USER_GROUP.NAME LIKE DefaultGroup
```

- The **Modify Reports** expanded screen is displayed.
- Select **AND** or **OR** from the list.
- Select the column from the list.
- Select the operator from the list.
- Enter the value for the condition in the field, in the format and type that is specified on screen.
- Use the **Append column to query** option to select whether to display the condition column in the report. Select **Yes** or **No**.
- Click **Add** to return to the **Edit Report** window. A message is displayed.

```
Limit added: "AND USER_GROUP.NAME LIKE DefaultGroup
```

14. To see the full SQL for the query, complete the following steps:

- a. Click **Edit SQL** on the **Edit Report** window.  
The **Edit SQL** screen is displayed.
- b. Click **Update** to make changes.
- c. Click **Back** to return to the **Edit Report** window.

15. To name your new report, complete the following steps:

- a. Click **Edit Name** on the **Edit Report** window.
- b. On the **Edit Name** window, type in a name for your report and click **Update**.  
The message 'Report was renamed ' is displayed on the screen.
- c. Click **Back** to return to the **Edit Report** window.

## 16. Submit

When you click **Submit**, the query is run and the report that it generates is displayed with the name that you defined, in **Edit Name**.

- To save the new report, complete the following steps:
  - Click **Reports > Save custom query**.
  - Change the **Query name** if required.
  - Enter a description for your report.

- Enter a menu name. This name is displayed in the **Custom Reports** menu.
- Select the groups that can have access to the report.



**Note:** The created report is displayed only in the **Custom Reports** menu of the Admin user or Super User who created the report. If groups are selected, the report is also displayed in the **Custom Reports** menu of any users who are members of the selected groups.

- Click **Submit**.

The new report is created.

## **Creating a new report by using an existing report**

You can create a custom report by using the Edit SQL feature on an existing report.

Generate the base report by selecting the required report from the menu.

For example, to use the **All Targets** report as the base report, complete the following steps:

- a. Select **Targets > All targets**.
- b. Click **Edit SQL**, on the upper right of the screen.
- c. Follow from step 3 ([on page 150](#))

## **Creating a report by adding tables and columns**

You can create a custom report by adding database tables and columns to existing reports. For more information, see [Adding a database table to a query \(on page 161\)](#). After you add the required tables and columns, you can save the report.

To save the report, complete the following steps:

Click **Reports > Save As Custom Report**.

- a. Change the **Query name** if required.
- b. Enter a description for your report.
- c. Enter a menu name.  
This name is displayed in the **Custom Reports** menu.
- d. Select the groups that can have access to this report.





**Note:** The created report is displayed only in the **Custom Reports** menu of the Admin user or Super User who created the report. If groups are selected, the report is also displayed in the **Custom Reports** menu of any users who are members of the selected groups.

e. Click **Submit**.

## Running a custom report

You can run custom reports by using one of the following methods.

- Run them from the **Custom reports** menu.
- Generate a list of custom reports and select one to run.

Choose the appropriate method for running a custom report

1. Running a report from the **Custom reports** menu.
  - a. Click **Reports > Custom Reports**.
  - b. Click the **Custom Report** name.
2. Running a custom report from the **Custom Reports** list.
  - a. Click **Reports** then select **All Reports, My Custom Reports, or All Custom Reports**.



**Note:** **All Reports** is the **only** option available to a **Super User**.

- b. If you selected **All Reports**, select **User Custom Reports**. If you selected **My Custom Reports, or All Custom Reports**, select the report from the list.
- c. Select **Run** from the **Reports** menu, or from the **Actions** list on the left.

The custom report is generated and its results are displayed on the screen.

## Viewing custom reports

Custom reports can be viewed in the following ways.

- By selecting the **All Custom reports, or My Custom Reports** menu items.



**Note:** This method is not available to Super Users.

- By running the **User Custom Reports** report from the **All Reports** list.

To view the custom reports, complete step 1 or step 2.

1. Viewing custom reports by selecting **All Custom Reports**, or **My Custom Reports**.
  - a. Click **Reports**.
  - b. Click **All Custom Reports** to display the list of all custom reports Click **My Custom Reports** to display the list of custom reports that were created by the currently logged on administrator.
2. Viewing custom reports by running the **User Custom Reports**, report.
  - a. Click **Reports > All Reports**.
  - b. Select **User Custom Reports**.
  - c. Select **Run**, from the **Reports** menu or the **Actions** list on the left.

The **User Custom reports** list is displayed. The list contains all custom reports that were created by the currently logged on Super User or Administrator.

## Manage custom reports

There are a number of actions that you can perform when you select a custom report from the list.

### Edit Custom Report and Access

Change details about the custom report and also change the group access to this report by selecting or deselecting groups in the list.

### Remove my access

Remove custom reports from your **Custom Reports** menu.

### Delete Custom Report

Deletes the selected custom reports.

## Editing a custom report by using the **Edit Custom Report and Access** feature

Use the **Edit Custom report and Access** feature to select a custom report and edit its details. You can change the name, description, and menu name, although its main use would be to add or remove group access to the report or to edit the reports SQL.

To use **Edit Custom Report and Access**, complete the following steps:

1. Select **Reports**.
2. To generate a list of Custom reports **Click All Reports, My Custom Reports** or **All Custom Reports**.



**Note:** A Super User can generate the **All Reports** list only.

3. If you select **All Reports**, go to step [4 \(on page 154\)](#). If you select **My Custom Reports**, or **All Custom Reports** go to step [6 \(on page 154\)](#)
4. Select **User Custom Reports**.
5. Select **Run** from the **Reports** menu or the **Actions** list on the left.
6. Select the required report from the list.
7. Select **Edit Custom Report & Access** from the **Actions** list on the left.

8. Change the **Query name**, **Description**, or **Menu name** if required.
9. In the **SQL data** field, make any required changes to the SQL.



**Note:** You must understand SQL for this method.

10. Select the groups that can have access to the report.



**Note:** The created report is displayed only in the **Custom Reports** menu of the Admin user or Super User who created the report. If groups are selected, the report is also displayed in the **Custom Reports** menu of any users who are members of the selected groups.

11. Choose one of the following options.
  - To save the report and finish, click **Submit**.
  - To check the output of the report, go to step [12 \(on page 155\)](#).
12. Click **Run Report**.
13. If the generated report is what you require click **Submit**, otherwise, complete the following steps.
  - From the **Reports** menu, select **Save custom query**.
  - Repeat from step [8 \(on page 155\)](#) until the report meets your requirements.

## Removing your access to a report

Use the **Remove My Access** feature to remove a custom report from your **Custom Reports** menu.

1. Select **Reports**.
2. To generate a list of custom reports, click **All Reports**, **My Custom Reports**, or **All Custom Reports**.



**Note:** A Super User can generate the **All Reports** list only.

3. If you select **All Reports**, select **User Custom Reports**, then select **Run** from the **Reports** menu or the **Actions** list on the left. Select the required reports from the list.
4. If you select **My Custom Reports**, or **All Custom Reports**, select the required reports from the list.
5. Select **Remove My Access** from the **Actions** list on the left

The currently logged on Super User or Administrator can no longer run the selected custom reports from their **Custom Reports** menu.

You can check by clicking the **Reports** menu.

If the selected custom report is the only custom report that the Super User or Administrator had, the **Custom Reports** menu is not displayed in the **Reports** menu.

If the **Custom Reports** menu item is still available in the **Reports** menu, click **Custom Reports**. The selected custom reports are not displayed in the menu or any sub menus.



**Note:** An Administrator has access to all custom reports. Therefore, they can still run the selected custom reports by running them from the **All Custom Reports**, report.

## Deleting custom reports

Use the **Delete Custom Report** feature to delete custom reports.

1. Select **Reports**.
2. To generate a list of custom reports, click **All Reports**, **My Custom Reports**, or **All Custom Reports**.



**Note:** A Super User can generate the **All Reports** list only.

3. If you select **All Reports**, go to step [4 \(on page 156\)](#). If you select **My Custom Reports**, or **All Custom Reports**, go to step [6 \(on page 156\)](#).
4. Select **User Custom Reports**.
5. From the **Reports** menu or the **Actions** list on the left, select **Run**.
6. Select the reports from the list.
7. Select **Delete Custom Report** from the **Actions** list on the left.

The list of reports is refreshed and the selected custom reports is no longer in the list.

# Chapter 17. Manage the home page for a user or group

When you log on to the BigFix® Remote Control Server, the first page that is displayed is the default home page. You can set your own home page, set the home page for a user, or set the home page for a group of users. If you have a list of targets that you access regularly, you can create a favorites list and set it as your default home page. If you want a group of users to see a list of specific targets when they log on, you can create a custom report to display these targets and set it as their default home page. The page that is displayed when a user logs on to the BigFix® Remote Control Server is determined by the following conditions.

1. Does the user have a default home page set?

**Yes**

This home page is the page that is displayed when the user logs on.

**No**

Check the users groups for a home page.

2. Do any of the groups that the user belongs to have default a home page set?

**Yes**

- If only one group has a default home page set, this home page is displayed when the user logs on.
- If more than one group has a default home page set, the home page that was most recently set for the groups is displayed.

**No**

The `trc.properties` file is checked.

3. If no default home page is set by the user or for any groups that the user belongs to, the value of the `default.homepage.method` property in the `trc.properties` file is used.



**Note:** The value of `default.homepage.method` is set to report by default, which displays the report that is defined in the `default.query` property. This report is the **All targets** report by default. If `default.homepage.method` is set to search, the search targets page is displayed when the user logs on. For more information, see [trc.properties \(on page 216\)](#).

The default home page that is set by the user, overrides any home page that is set for the groups that the user belongs to. For example, user1 sets a default home page to the favorites list of targets. User1 is a member of user group `testusers`. A custom query of all targets that are manufactured by companyX is created and is set to the default home page for user group `testusers`. However, when user1 logs on it is the favorites list that is displayed as the home page.

## Create and set a home page

You can set standard reports or custom report to the default page.

## Setting a default home page as a user

To set a default home page, complete the following steps:

- Choose the appropriate method for generating a relevant report.
  - Run a standard report from any of the BigFix® Remote Control Server menus
  - Run a custom report that you have access to from the **Custom reports** menu.

For information about how to create and save a custom report, see [Create a Custom Report \(on page 147\)](#).

- Click **Options > Set Current Report as Homepage**

For example, to make the favorites report your home page:

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

Your home page is set and the following message is displayed. *Your home page has been set to report XXXXXXXX, where XXXXXXXX is the name of the report that you set. For example, Your home page has been set to report Favorites.*

When you log on to the server, the **Favourites** report is the first page that is displayed.

## Setting a home page for a group

A default home page for groups can be set by using custom reports. You can set the default home page for a group in the following ways:

- Edit the access for a saved custom report.



**Note:** Only administrators have authority to edit the access for a custom report.

- When you save a custom report.

To set a default home page for a group, complete the following steps.

1. Choose the appropriate method for setting the home page
  - a. Edit the access for a saved custom report.
    - i. Select **Reports > My Custom Reports**, or **Reports > All Custom Reports**.
    - ii. Select the report.
    - iii. Select **Edit Custom Report & Access**. Go to step 2 ([on page 158](#)).
  - b. When you save a custom report.
    - i. Generate the custom report. For more information about the various ways that a custom report can be generated, see [Create a Custom Report \(on page 147\)](#).
    - ii. When you generate your report click **Reports > Save As Custom Report**.
2. On the **Edit Custom Report and Group Access Rights** pane type in a name and menu name for the report.

3. Select **Make Default Homepage** for each group that is to have this new report as their default home page.
4. Click **Submit**.

The default home page is set for the selected groups. Whenever a user who is a member of the selected groups logs on to the BigFix® Remote Control Server, the saved report is displayed as their home page.

However, if the user also has a default home page set, they see their default home page instead.

## Viewing the default home page list

After default home pages are set, you can view the default home page list by completing the following steps:

1. Select **Reports > Default homepages**.
2. Select one of the following options:

### For user groups

The list of defined user groups is displayed. The name of the report that is set as the default home page is shown in the **Name** field.

### For Users

The list of users who have a default home page set is listed.

## Editing the default home page for a group

You can change the default home page that is set for a group by using the **Edit Group Homepage** option. The option is available when you view the **Group home pages** report.

To edit the default home page, complete the following steps:

1. Select **Reports > Default homepages > For user groups**.
2. Select one of the groups in the list.
3. From the **User groups** menu or the **Actions** list on the left, select **Edit Group Homepage**.  
The **Edit group default homepage** page is displayed showing the list of custom reports that are defined.
4. Choose the appropriate method for selecting the home page.
  - Select **None**. The users in the group no longer have a custom report set as their home page.
  - Select one of the listed custom reports. This report is saved as the new home page for the group members.
5. Click **Submit**.

When members of the selected group log on to the server, the new default home page is displayed.

## Reset the default home page

When a default home page is set for a user or a group, you can reset the default home page by using the following options.

- **Reset User Homepage**
- **Reset Group Homepage**

## Resetting the default home page for a user

If a user has a default home page set, the page is displayed when the user logs on. To change the home page use **Reset User Homepage** to reset their home page. The next time that the user logs on, the home page that is set for any groups that they belong to is displayed. If the groups do not have a home page set, the default home page, as defined in `trc.properties`, is displayed.

To reset a users default home page, complete the following steps:

1. Select **Reports > Default homepages > For users** .
2. Select the users.
3. From the **Users** menu or the Action list on the left, select **Reset User Homepage**.

A message is displayed when the home page is reset.

The next time that the user logs on, the home page that is set for any groups that they belong to is displayed. If the groups do not have a home page set, the default home page, as defined in `trc.properties`, is displayed.

## Resetting the default home page for a group

To reset a groups default home page, complete the following steps:

1. Click **Reports > Default homepages > For user groups**.
2. Select one of the groups in the list.
3. From the **User groups** menu or the Action list on the left, select **Edit Group Homepage**.  
The **Edit group default homepage** page is displayed showing the list of custom reports that are defined.
4. Choose the appropriate method for selecting the home page
  - Select **None**. The users in the group no longer have a custom report set as their home page. The home page is set to the default home page as defined in the `trc.properties` file.
  - Select one of the listed custom reports. This report is saved as the new home page for the group members.
5. Click **Submit**.

The next time any of the members of the selected group logs on, the new default home page is displayed.



# Chapter 18. Adding tables and columns to queries

Use the options menu in the BigFix® Remote Control Server to perform actions on reports. This section details the options that are available to super user and administrator users only. For more information about more options that are available to all users, see the *BigFix® Remote Control Controller User's Guide*. Add extra data to your reports by adding database tables and columns to the query that is run to generate the report data. A knowledge of the database tables is required for using this option. For more information about the database tables and columns, see [Database table and column descriptions \(on page 366\)](#).



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

## Adding a database table to a query

When a report is displayed, you can add more data to it by adding one or more database tables to the query that is used to generate the data. After you add a table, you can add one or more columns from the new table to the report.

To add a database table, complete the following steps:

1. Click **Options > Add Table to Report**
2. Select the database table from the list.

A message is displayed showing that the table was successfully added. To add the required database columns to the report, see [Adding a database column to a query \(on page 161\)](#).

## Adding a database column to a query

After you add a database table to your report, you can add columns from the table to the report by selecting the **Add Column to Report** option. The report is displayed with the new columns added.

To add a column, complete the following steps:

1. Click **Options > Add Column to Report**
2. Select the database table then the column from the list.

A message is displayed showing that the column was successfully added and the report is displayed with the new columns added.

# Chapter 19. Configuration and troubleshooting options in the Admin menu

The **Admin** menu in the BigFix® Remote Control Server provides you with configuration and troubleshooting information. The following options are available in the menu:

- **Edit properties file**
- **LDAP Configuration Utility**
- **View Application Log**
- **Send Application Log**
- **Import Data**
- **View Current Server Status**
- **All Remote Control Gateways**
- **New Remote Control Gateway**
- **Reset Application**
- **Configure session dialog**
- **New Permission Set**
- **All Permissions Sets**
- **Create Secure Registration Token**
- **List Secure Registration Tokens**
- **Target Membership Rules**

## Editing the properties file

Use the **Edit Properties Files** option to edit the various property files that are present in the system to configure Remote Control to your own requirements.

The following properties files are available in Remote Control

- `trc.properties`
- `log4j2.properties`
- `ldap.properties`
- `common.properties`
- `appversion.properties`
- `controller.properties`
- `ondemand.properties`

For details of the variables and relevant values that are required for these files, see [Editing the properties files \(on page 215\)](#).

## Configure LDAP properties by using the LDAP wizard

The LDAP properties file is initially installed with default values that can be changed to your requirements. You can use the LDAP configuration utility to test the connection to your LDAP server and correctly configure your user and group search parameters. The utility can be used to change and test LDAP property values to determine the correct configuration for importing the required user and group information from your LDAP server to the Remote Control database.



**Note:** The utility configures the connection, user, and group search properties only. For more information about enabling LDAP and more LDAP configuration parameters, see the *BigFix® Remote Control Installation Guide*.

## Configure LDAP by using the LDAP configuration utility

The LDAP configuration utility contains 4 sections that you can use to configure and test certain LDAP properties to determine the correct values for your requirements.

- Connection
- Group search
- User search
- Other settings

You must complete section 1 in the utility before you can access and use the remaining sections.

To access and run the utility select **Admin > LDAP Configuration Utility**.

The LDAP configuration utility is displayed.

## Testing your LDAP connection

The first step is to test that you can successfully connect to your LDAP server. This section of the utility must be completed and verified before you can continue. To test your LDAP connection, complete the following steps:

1. Enter the connection information.

### **Connection URL**

Defines the URL used to connect to your LDAP server.

### **Connection Name**

This must be set to the user ID that is defined for authenticating a read-only LDAP connection with the LDAP server. The user name must contain all the necessary rights to read all the required information from the directory tree.

### **Connection Password**

This must be set to the password defined for authenticating a read-only LDAP connection with the LDAP server. You can enter a plain text or an encrypted password.

If you enter a plain text password, you can encrypt it by clicking **Encrypt Password**.



**Note:** When you click **Encrypt Password**, **Connection Password Encrypted** is automatically selected.

If you enter an encrypted password, you must also select **Connection Password Encrypted**.

### **Connection Password Encrypted**

Determines whether the password is treated as encrypted or not. If you select **Connection Password Encrypted** the password is treated as encrypted if you do not select it, the password is treated as plain text.



**Note:**

- a. This option is automatically selected when you click **Encrypt Password**.
- b. If you enter an encrypted password in the **Connection Password** field and deselect **Connection Password Encrypted**, the password is not decrypted. The password remains encrypted for security reasons.

### **Alternate URL**

Defines a secondary LDAP server name. If the primary LDAP server is down, you can use the alternative LDAP server for authentication.

### **Security Authentication**

Select the security authentication. Specifies the security level to use. If you are using SSL, select **Simple**. If you are using SASL, select **DIGEST-MD5**.

2. Click **Test Connection**.

If a successful connection is made to the LDAP server, `Connection OK` is displayed. If a connection is not possible, `Connection Error` is displayed. Click the question mark for more details of what is causing the error.

When you have a successful connection to your LDAP server, you can then configure and test group and user search parameters.

## **Configure LDAP using Secure LDAP**

You can configure the Remote Control Server to connect to a LDAP server using an SSL (encrypted) connection. To do this complete the following steps:

1. In the LDAP configuration wizard, in the **Connection URL** field, select the LDAPS (Secure LDAP) protocol.  
Example: **Connection URL** = `ldaps://MyLdapServer`
2. Trust the certificate sent by the LDAP server. To do this, import the certificate into the **Signer Certificates** section of the Remote Control Server keystore. The default path of the keystore file is `[server_installation]/wlp/usr/servers/trcserver/resources/security/key.jks`. Otherwise, check the path of the keystore file specified in the configuration file `[server_installation]/wlp/usr/servers/trcserver/ssl.xml`. To import the certificate, perform the following steps:
  - a. Launch the `ikkeyman` tool under `[server_installation]/java/jre/bin/`.
  - b. Select the Key Database File and open it.
  - c. Select the Remote Control server keystore file and click **OK**.
  - d. Select **Signer Certificates**.
  - e. Click **Add** and select the certificate to import.
  - f. Restart the Remote Control server service.
3. To test the connection, in the LDAP configuration wizard, click **Test Connection**.

If the configuration is correct, the connection test will be successful. If the [LDAP synchronization](#) is on, when the next time the synchronization task is run, the LDAP users will be imported and visible in the page [Users - All Users](#).

## Configuring LDAP group search parameters

Use the **Group Search** section to search for groups in the LDAP directory tree. The search is started at the directory that is defined in the **GroupBase** field, and uses the search query that is specified in the **Group Search** field.

1. Enter the group search information. You can click the question mark next to each field for more information.

### Group Base

Specify the LDAP directory that you want to start the group search from. If this property is left blank, the search is started from the top-level element in the directory, for example `OU=location,DC=domain,DC=com`. You can refine your search by starting the search from within a specific organizational unit (OU). For example, to start the search from an OU called Test, set the property value as `OU=Test,OU=location,DC=domain,DC=com`. The search looks for groups within Test OU that match the **GroupSearch** criteria. If **GroupSubtree** is selected, any OUs that belong to the Test OU are also searched.



**Note:** You can use the **Browse** icon to the right of the field to go through your directory structure and select a specific starting location.

### Group Search

Specify the LDAP filter expression to be used for the group search, for example, `(objectClass=group)`. The expression must filter the results so that just the groups that you want are imported to the Remote Control database. The default value is `(objectClass=group)`, which means, look for users in any object that is a group within the specified **GroupBase**. This value, imports all Active Directory groups to Remote Control.



**Note:** When you use `(objectClass=group)`, some environments can have thousands of groups so it is important to create a filter that imports only the groups that you want. The search can be further refined by using more complex queries. For example, the following values `GroupBase=(OU=location,DC=domain,DC=com)` `GroupSearch=(&(objectClass=group)(name=Dep*))` return any groups within the location OU whose name starts with *Dep*. For example, groups with names `department1` or `deputy` might be returned.

### Group Subtree

Select this option if you want to recursively search the subtree of the element that is specified in the **GroupBase** attribute for groups. If you do not select this option, only the top level is searched. Default value is not selected.

### Group Name

The LDAP attribute name that is used for a group search. This property is set to *name* by default.

### Group Description

The LDAP attribute name that is used to get the description for this group. This value is set to *description* by default.

### Group Membership Attribute

The LDAP attribute name that is used to find the members of the groups that are returned as a result of the specified search. The default value is *member*.

2. Click **Test Groups Search**. A message box is displayed with the total number of groups that are found as a result of the search. Click **OK**.

The resulting groups are displayed in the text box on the right. This list of groups are imported from LDAP when LDAP synchronization is enabled. You can click the icon to the left of each group name to see a list of the LDAP attributes and values that are defined for the group.

When you have the required group search results, use the **User search** section of the utility to configure and test values for your User Search LDAP properties. For more information, see [Configuring LDAP user search parameters \(on page 166\)](#). Save your current configuration by following the steps in [Saving your LDAP configuration \(on page 171\)](#).

## Configuring LDAP user search parameters

Use the User Search section to search for users in the LDAP database. The search starts at the directory that is defined in the **User Base** field, and uses the search query that is specified in the **User Search** field.



**Note:** Depending on the type of LDAP server that you install, click **Set Defaults** to load the LDAP utility with the default parameter values for your server type.

## 1. Enter the user search information.

### User Base

Specify the LDAP directory that you want to start the user search from. If left blank, the search is started from the top-level element in the directory. For example, `OU=location,DC=domain,DC=com`. You can refine your search by going deeper into the OU structure and select to start the search from within a specific organizational unit. For example, to start from an OU called Test, set the User Base value to `OU=Test,OU=location,DC=domain,DC=com`. The search starts at the Test OU and looks for users that match the **User Search** criteria. If **User Subtree** is selected, any OU that belongs to Test OU is also searched.



#### Note:

- Use the **Browse** icon to the right of the field to navigate through your directory structure and select a specific starting location.
- To import users not belonging to any OU, you need to remove the OU from the User Base.



**Warning:** This action will import the whole domain tree.

### User Search

Specify the LDAP filter expression to be used for the user search. For example `(objectClass=user)`. The defined expression must filter the results such that only the users that you want are imported to Remote Control. The default value is `(userPrincipalName={0}@MyCompany.com)`. {0} is substituted with the user ID that is used to log on to Remote Control, and *MyCompany.com* is the host name of your LDAP server. That is, look for users whose **userPrincipalName** matches any users that are found within the specified **UserBase**.



**Note:** Some environments have thousands of users. Therefore, it is important to create a filter that imports only the users that you want. To limit the users to only those users who are members of groups that are imported into Remote Control through the **GroupSearch** filter, you must select **User Must be in a Group**. If you do not select this property, the users that do not belong to any of the imported LDAP groups are automatically assigned to the **DefaultGroup** user group. The search can be further refined by using more complex queries. For example, set the following values. `GroupBase=(OU=location,DC=domain,DC=com)` `UserSearch= (&(objectClass=user) (|(memberOf=CN=Department1,OU=GROUPS, OU=location,DC=domain,DC=com) (memberOf=CN=Department3,OU=GROUPS, OU=location,DC=domain,DC=com))(name={0}))` Define three groups, `Department1`, `Department2`, and `Department3`. The query authenticates and imports any users that have an **objectClass** value equal to `user` and that are members of the groups `Department1 OR Department3`. Users from `Department2` cannot log on to Remote



Control because they are not imported. The (&(name={0})) is added to the end to specify that the name attribute is used for logging in. This value must match whatever attribute was specified as **userid**.

### User Subtree

Select this option if you want to recursively search the subtree of the element that is specified in the **UserBase** attribute for users. If you do not select it, only the top level is searched. The default state is not selected.

### User Must be in a Group

Select this option to limit the users that are imported to only those users who are members of groups that are imported into Remote Control through the **GroupSearch** filter. The default state is not selected.



**Note:** To import users who do not belong to any LDAP group, you must deselect "User Must be in a Group" check box.



**Warning:** This action imports all users identified by the domain and OU specified in the User Base. You can give permissions to those users only by giving permission to the **DefaultGroup** (which is the local Remote Control group), where all users are automatically added regardless from their group membership.

### LDAP attributes

Type which user-specific LDAP attribute names must be used for importing the user details into the corresponding Remote Control user properties.

#### UserId

The user ID is the LDAP attribute that contains the user ID that is chosen to be mapped to the **userid** field in Remote Control.

#### sAMAccountName

sAMAaccount must be set to use the user ID only portion of the logon (without the UPN Suffix).

#### userPrincipalName

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

Set **UserId** to the **userPrincipalName** value to ensure that the user ID that is entered is not reported as containing invalid characters. For example, an apostrophe might be reported as an invalid character.

#### User Password



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

#### **User Email**

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



**Note: User Email** must not have a null value. If your Active Directory Tree does not contain email information, a different attribute must be used. For example, it can be set to `userPrincipalName`.

#### **Employeeid**

The name of the LDAP attribute in the user's directory entry that contains the user's employee ID.

#### **Title**

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

#### **Forename**

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

#### **Initials**

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

#### **Surname**

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

#### **Department**

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

#### **Company**

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

#### **Location**

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

#### **Floor**

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

**Address\_1**

The name of the LDAP attribute in the user's directory entry that contains the user's address\_1 details.

**Address\_2**

The name of the LDAP attribute in the user's directory entry that contains the user's address\_2 details.

**Town**

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

**Country**

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

**State**

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

**Telephone**

The name of the LDAP attribute in the user's directory entry that contains the user's telephone number.

**Mobile**

The name of the LDAP attribute in the user's directory entry that contains the user's mobile number.

2. Click **Test User Search**

A message box is displayed with the total number of users that are found as a result of the search.

3. Click **OK**

The resulting users are shown in the text box. If LDAP synchronization is enabled, this list of users would be imported from LDAP. You can click the icon to the left of each user name to see a list of the LDAP attributes and values that are defined for the user. Click the icon to the right of the user name to display the Remote Control user field values. The user field values are imported into the Remote Control database.

When you have the required user search results, you can save your current configuration by following the steps in [Saving your LDAP configuration \(on page 171\)](#).

## Setting the page size of LDAP search retrievals

Use the **Other settings** section of the LDAP configuration utility to configure more LDAP properties.

## Page Size

Set this value to the page size of LDAP search retrievals. Do not set this property to anything greater than the maximum page size for the LDAP server. Default value is 1000.

## Saving your LDAP configuration

When you have your required results from the Group and User search parameters that you entered, you can save the configuration by clicking **Save**. Your values are saved to the LDAP properties file and are loaded into the utility the next time that you run it.

## Viewing the application log

The application log lists all server activity. The most recent activities are appended to the end of the file. You can use this file to look for errors if a problem occurs.

To view the application log, click **Admin > View Application Log**.

The application log is displayed, click **CTRL + END** to go to the end of the file.

## Saving the application log for exporting

If a problem occurs, you can save the application log to a file by using the **Send Application Log** option. This file can then be sent to support for debugging.

To save the application log, complete the following steps:

1. Click **Admin > Send Application Log**.
2. Click **Save** to save to a specific location.

The file is saved as `trc.log`.



**Note:** Click **open** to open the `trc.log` file in text mode.

## Import data into the database

You can use the **Data Import** option to import data into the Remote Control database. For more information about this function, see [Import data from csv files into the Remote Control database \(on page 360\)](#).

## Viewing the server status

To view the current server status, click **Admin > View Current Server Status**.

The **View Current Server Status** screen is displayed.

## Viewing the Remote Control gateways

When you create Remote Control gateways, you can view the list of defined gateways. For more information about installing gateway support and configuring gateway connections, see [Access targets on different networks \(on page 194\)](#).

To view all defined gateways, click **Admin > All Remote Control Gateways**.

The list of defined gateways is displayed.

## Editing an Remote Control gateway

To edit the details of an Remote Control gateway, complete the following steps:

1. Click **Admin > All Remote Control Gateways**
2. Select the gateway.
3. From the **Admin** menu or the **Actions** list on the left, select **Edit Remote Control Gateway**.
4. Change the details.
5. Click **Submit**.

## Deleting an Remote Control gateway

To delete Remote Control gateways, complete the following steps:

1. Click **Admin > All Remote Control Gateways**.
2. Select one or more gateways.
3. From the **Admin** menu or the **Actions** list on the left, select **Delete Remote Control Gateway**.
4. On the **Confirm Deletion** screen, click **Submit**.

The gateway details are removed from the Remote Control database.

## Creating an Remote Control gateway

If you configure your network for gateway support and have controllers that connect to targets by using a gateway to make the connection, you must provide the server with details of the gateway system.

To add an Remote Control gateway to the server, complete the following steps:

1. Click **Admin > New Remote Control Gateway**.
2. Supply the following information for your gateway.
  - Host name
  - Description
  - IP address
  - Port
3. Click **Add another IP address** to enter the IP address and port if the system you are using as the gateway has multiple IP addresses.

#### 4. Click **Submit**.

After you create a gateway, you must configure it by using the gateway configuration file. For more information, see [Configure the gateway support \(on page 194\)](#).

## Resetting the Application

When you update the properties files, use **Reset Application** to force the application to load the new values from the database.

To reset the application, click **Admin > Reset Application**.

The current screen is displayed with the following message: `Reinitialised all application objects`



**Note:** If at any time a system hang occurs, you must stop and restart the Remote Control server service.

## Configuring the user acceptance window

When user acceptance is enabled for remote control sessions, an acceptance window is displayed on the target system when the session is requested. The target user can use this window to accept or refuse the session. This window is displayed with standard text that is included with the product. You can also configure this text by using the **Configure session dialog** feature to change the content of the user acceptance window to your own requirements. You can display a specific icon, set a default locale, and create a specific customization for selected locales to change the window title, and display customized text if required. For each of the locales that are listed in the **Configure Target session acceptance dialog** utility there is a set of translated standard text messages. However, if you create a customized locale, the text that is displayed is determined by which type of text is defined, as shown in the following table.

**Table 3. Determine the text that is displayed in the user acceptance window**

Target locale - customized text is defined	Default locale - customized text is defined	Target locale - standard text is defined	Resulting Text is:
√	√	√	Target locale - customized text
	√	√	Default locale - customized text
		√	Target locale - standard text
			Standard US-English



**Note:** This process is applied to each of the customizable text options separately, that is the **Title**, **Paragraph 1** and **Paragraph 2**. It is possible to display both custom and standard text. For example, select a locale to



customize, type in customized text for **Paragraph 1** and **Paragraph 2** and leave the window title field blank. The acceptance window, for a target that is configured for this locale, displays the standard window title and the customized **Paragraph 1** and **Paragraph 2** text.

To configure the session dialog, complete the following steps:

1. Select **Admin > Configure session dialog**.
2. On the **Configure Target session acceptance dialog** window, enter the required information.

### General

#### **Select an existing icon**

Select an icon to be displayed in the acceptance window. The selected icon is previewed on the right. You can upload your own icon files by using the **File Import** feature. For more information, see [Uploading user acceptance window icons \(on page 178\)](#).

#### **Hide mode selection**

Select this option to hide the session mode buttons on the user acceptance window. If you do not select this option, the session mode buttons are displayed on the user acceptance window. Not selected is the default value.

#### **Default locale**

Select the required default locale. The default locale indicates which language is displayed when there are no translations available for the current locale of the target system. For example, a target is configured for France, if a customized French translation is not available and English is selected as the default locale, English text is displayed. If you do not want to set a default locale, select **No default locale**.

#### **Customisations**

Shows the number of customized locales that are created and saved.

### Locale Customisation

You can create multiple customizations. Select a locale, enter the required values and click **Save**.

#### **Locale**

Select the locale that you want to set customized options for.

#### **Load customisations**

Use the **Load customizations** options to populate the fields with already saved text or to clear the fields. Select the required option.

#### **Load built-in text**

Select this option to populate the fields with the standard text. You can also edit the text.



**Note:** If you populate the fields with standard text and click **Save**, the text becomes the customized text for the selected locale.

#### **Load default customisations**

Select this option to populate the fields with the customized text that is saved for the default locale. You can also edit the text.

#### **Clear customisable fields**

Select this option to clear the fields.

#### **Title**

Enter the customized text that is to be displayed in the acceptance window title.

#### **Paragraph 1**

Enter the customized text that is to be displayed in the first paragraph of the acceptance window.

This paragraph usually contains any legal text that is required.

#### **Paragraph 2**

Enter the customized text that is to be displayed in the second paragraph of the acceptance window.

This paragraph usually contains any additional help text that is required.

3. Click **Save**. Click **Close** to exit from the **Configure Target session acceptance dialog** window.



#### **Note:**

- If during the customization process you select a different locale, you have the following options:

##### **Save**

Click to save the options for the current locale.

##### **Don't Save**

Click to clear the text fields and keep the newly selected locale available.

##### **Cancel**

Click to return to the **Configure Target session acceptance dialog** window with the previous locale still selected.

- If you leave the **Title**, **Paragraph 1**, or **Paragraph 2** fields blank, no customized text is saved for that option.

After you create and save customized options, if a remote control session with user acceptance enabled is requested, the user acceptance window is displayed on the target. The window displays the customized or standard text that is configured and saved for the target computers locale.

## Configure the user acceptance window for a peer to peer session

When you use the **Configure session dialog** feature in the BigFix® Remote Control Server UI and save customized locales, these values are saved to the database. When a remote control session is requested, the values are passed to the target computer to be saved in the properties. You can configure the properties locally on the target if the target takes part in peer to peer sessions only.



**Note:** If you set values locally for the properties and the target takes part in remote control sessions started from the server, the local values are overwritten with values passed from the server.

### CustomConfirmTitle

Use this property to define a customized window title for the user acceptance window. When there is no translation available for the locale that the target is configured for, the default string, that is saved in **CustomConfirmTitle**, is displayed for the window title. If you want a customized window title for specific locales, you can create multiple **CustomConfirmTitle.X** properties, where *X* is the locale. For example, *CustomConfirmTitle.fr*.

### ConfirmExtraText

Use this property to define a customized **Paragraph 1** for the user acceptance window. When there is no translation available for the locale that the target is configured for, the default string, that is saved in **ConfirmExtraText**, is displayed for **Paragraph 1**. If you want a customized **Paragraph1** for specific locales you can create multiple **ConfirmExtraText.X** properties, where *X* is the locale. For example, *ConfirmExtraText.es*.

### CustomConfirmOptions

Use this property to define a customized **Paragraph 2** for the user acceptance window. When there is no translation available for the locale that the target is configured for, the default string, that is saved in **CustomConfirmOptions**, is displayed for **Paragraph 2**. If you want a customized **Paragraph 2** for specific locales, you can create multiple **CustomConfirmOptions.X** properties, where *X* is the locale. For example, *CustomConfirmOptions.zh*.

### AllowSessionModeOverride

Use this property to determine whether the session mode buttons that are valid for the session are displayed on the acceptance window.

Set to Yes.

The session mode buttons that are valid for the remote control session are not displayed on the user acceptance window.



Set to *No*.

The session mode buttons that are valid for the remote control session are displayed on the user acceptance window.

## Configuring the user acceptance window on a windows target

Configure the user acceptance window properties locally on the target if the target takes part in peer to peer sessions only. For a Windows target, you can edit the target registry to set the properties.

To configure the target properties on a Windows operating system, complete the following steps:

1. Run regedit.exe
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`  
On a 32-bit system, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Remote Control\Target`.
3. Choose the appropriate method for configuring the properties.
  - Set a custom default string
    - a. Right-click the relevant property and select **Modify**.



**Note:** For more information about the properties, see [Configure the user acceptance window for a peer to peer session \(on page 176\)](#).

- b. Type in the string and click **OK**.
- Create a locale-specific property
  - a. Right-click the right pane and select **New > String Value**.
  - b. Type in the name for the property along with the locale and press **ENTER**. For example,
 

```
CustomConfirmTitle.fr.
```
  - c. Right-click the new property and select **Modify**.
  - d. Type in the string and click **OK**.
4. Restart the Remote Control target service.

To add a custom icon to the acceptance window you can rename your file to `CustomConfirmIcon.bmp` and save the file to the directory defined in the **WorkingDir** target property.



**Note:** The file must be 32 by 32 pixels in size and in BMP format.

## Configuring the user acceptance window in Linux

You can configure the user acceptance window properties locally on the target if the target takes part in peer to peer sessions only. For a Linux target, you can edit the target configuration file to set the properties.

To configure the target properties in Linux, complete the following steps:

1. Edit the `/etc/trc_target.properties` file.
2. Choose the appropriate method for configuring the properties.
  - Set a custom default string

Type in the default string for the relevant property.

- Create a locale-specific property

Add an entry for the property along with the locale and the custom string. For example,  
**CustomConfirmTitle.fr** = [custom string].

3. Save the file.
4. Restart the target service.

To add a custom icon to the acceptance window, you can rename your file to `CustomConfirmIcon.bmp` and save the file to the directory defined in the **WorkingDir** target property.



**Note:** The file must be 32 by 32 pixels in size and in BMP format.

## Uploading user acceptance window icons

Use the **Import File** function in the BigFix® Remote Control Server UI to upload icon files that you want to display in the user acceptance window. For more information about what can be configured in the user acceptance window, see [Configuring the user acceptance window \(on page 173\)](#).

To upload an icon file, complete the following steps:

1. Click **Admin > Import Data**.
2. Select **Import File**.
3. In the **Upload icon for Session Acceptance Dialog** section, click **Browse** and go to your icon file.



**Note:** Icons must be in BMP format and 32 by 32 pixels in size.

4. Click **Submit**.

The uploaded icon files are displayed in the **Configure session dialog** window.

## Creating a set of permissions that can be applied to a group

Use the create permission set option to create a set of policies that can be used to set temporary permissions when a user requests temporary access to a target. You can also choose the permission set when you create a user or target group. For more information about creating the permissions, see [Creating a set of permissions \(on page 137\)](#).

## Viewing the permissions sets

After you create sets of policies and permissions you can view the list of these sets by using the **All Permissions Sets** action.

To view the list click **Admin > All Permission Sets**.

The **View Permissions Sets** screen is displayed listing all defined permissions sets.

## Creating a secure registration token

You can create a secure authentication token for secure target registration.

When the **enforce.secure.registration** property is set to true on the server, the target must have a secure registration token so that it can register with the server. For more information about secure registration tokens and how they are used, see [Secure target registration \(on page 40\)](#).

To add a secure registration token to the server, complete the following steps:

1. Click **Admin > Create Secure Registration Token**.
2. Supply the following information for the token.

The default time period starts from the current date and time until 23:59 on the next day.

- **Description for token.** Enter a description for the token.
- **Starting on.** Click the calendar pull down and select a date that the token is valid from. Enter a start time or keep the default time.
- **Ending on.** Click the calendar pull down and select a date that the token is valid to. Enter an end time or keep the default time.

3. Click **Submit**.



**Note:** Before you leave the page, you must copy the registration token. Keep the token secure and confidential.

## Viewing the list of secure registration tokens

After you create secure registration tokens, you can view the list of tokens by using the **List Secure Registration Tokens** option.

To view the list click **Admin > List Secure Registration Tokens**.

The description and validity period of the tokens is displayed along with the user who created the tokens. The token data is not displayed.

For more information about secure registration tokens and how they are used, see [Secure target registration \(on page 40\)](#).

## Deleting secure registration tokens

To cancel a secure registration token, or remove expired tokens, you can use the **Delete Secure Registration Tokens** option.

To delete tokens, complete the following steps:

1. Click **Admin > List Secure Registration Tokens**.
2. Select one or more tokens.
3. Select **Delete Secure Registration Tokens** from the **Actions** list on the left.
4. Click **Submit** on the **Confirm Deletion** screen.

The secure registration token details are removed from the Remote Control database.

## Use rules to define target membership

Targets can be manually assigned to target groups by using the **Manage Group Membership** function. However, you can also create rules that automatically assign targets to target groups. The rules are used to match on the target's computer name, IP address or both and assign the target to the target group that is associated with the rule. If the target satisfies more than one rule it is assigned to the groups associated with these rules. Rules can be defined by using the **Target Membership Rules** function. You can create, view, edit, change the order of, and delete rules. Use properties in the `trc.properties` file to determine when the rules are applied. Use the rules to assign a target to multiple groups by checking the target computer name and IP address against all defined rules. The target is assigned to the groups associated with all matching rules. You can also limit the check by setting a rule to stop processing any further checking. In this case, the target is assigned only to the groups associated with this matching rule and any previously processed rules that matched the target details.

### Define when membership rules are applied

If you create rules to determine a target's group membership, configure the properties in the `trc.properties` file before you allow the targets to register with the server. Do this to ensure that the group membership is correctly assigned. You can configure the properties to assign targets to groups at registration time only, or to completely manage the target membership based on the defined rules. The following properties can be configured to determine when the target membership rules are applied.

#### **rc.tmr.at.registration**

Determines whether the target membership rules are applied to any new targets when they first contact the Remote Controlserver. Default value is Yes.

#### **Yes**

Whenever a target first contacts the server its computer name and IP address is checked against any defined rules. If matches are found, the target is assigned to the target groups associated with the rules.

#### **No**

Whenever a new target first contacts the server its computer name and IP address are not checked against any defined rules. You can manually assign a target to a group after it registers with the server.

#### **rc.tmr.at.every.callhome**

Determines whether the target membership rules are applied every time that a target contacts the Remote Control server. Default value is No.

##### **Yes**

Each time a target contacts the server its computer name and IP address are checked against any defined rules. If matches are found, the target is assigned to the target groups associated with the rules. The target's group membership is recalculated each time that it contacts the server to incorporate any changes that were made to the target rules since the last time it contacted the server.

##### **No**

Each time a target contacts the server its computer name and IP address are not checked against any defined rules.

#### **rc.tmr.at.triggered.callhomes**

Determines whether the target membership rules are applied any time that a target contacts the Remote Control server due to a change in its computer name or IP address or if the target comes online. Default value is Yes.

##### **Yes**

Each time a target contacts the server due to a change in its configuration, or when it comes online, its computer name and IP address are checked against any defined rules. If matches are found, the target is assigned to the target groups associated with the rules.

##### **No**

When a target contacts the server due to a change in its configuration, or when it comes online, its computer name and IP address are not checked against any defined rules.

#### **rc.tmr.at.rules.change**

Determines whether the target group membership is immediately recalculated for any targets that are affected by an addition, deletion, or change to a rule. When this property is enabled, any targets whose group membership was assigned by using rules have their group membership recalculated to incorporate the rule change. Default value is Yes.

##### **Yes**

Each time that you add, or delete a rule, or change a rule, the target group membership, for all targets whose group membership was assigned by using rules, is recalculated. The group membership of any target whose computer name or IP address matches the changed rule, is changed to reflect the change in the rule.

For example:

A *rule1* assigns targets with a computer name that starts with *test%* to the target group *testtargets*. Target *test1* contacts the server and is assigned to target group *testtargets*. Edit *rule1* and change the computer name condition to a name that starts with *admin %*. The group membership for target *test1* is recalculated. It is no longer a member of *testtargets* as it does not satisfy the new condition. Its computer name does not begin with *admin*.

## No

The addition, deletion, or change to a rule does not affect the target group membership of any targets whose group membership was assigned by using rules.



**Note:** The next time one of these targets contacts the server, their group membership is recalculated if **rc.tmr.at.every.callhome = Yes**, or **rc.tmr.at.triggered.callhomes =Yes** and the following conditions are satisfied.

- Their computer name or IP address satisfies the new rule
- They are effected by the rule that was deleted
- They do not satisfy the updated rule



**Note:** The group membership of targets that are manually assigned to target groups is not modified by target rules.

```
For example :
If an administrator assigns target1 to target group T1 by using
the Manage Group Membership function, it remains a member of
T1 until it is manually removed from the target group or until
the group is deleted.
```

## Creating rules

You can create rules that assign targets to target groups if their computer name or IP address matches conditions set in the rules. For example, you can assign targets to one or more target groups when they first register with the BigFix® Remote Control Server or every time they contact the server. For more information about properties that affect the group assignment, see [Define when membership rules are applied \(on page 180\)](#).

To create a rule, complete the following steps:

1. Click **Admin > Target Membership Rules**.
2. Select **Create new rule**.
3. On the **New Rule** screen, enter the information that is required to create the rule.

### Computer name

Enter all or part of the computer name to be checked against the target computer name. You can use wildcard characters. Use ? to denote one character and use % to denote multiple characters.

#### For example:

If you enter *test*, any targets whose computer name is `test` satisfy this rule.

If you enter *admin%*, any targets whose computer name starts with `admin` satisfy this rule.

If you enter *admin??*, any target whose computer name starts with `admin` and then another 2 characters satisfy this rule, for example, `admin22`, `adminGB`.

### IP start

Enter the IP address that is at the start of the range of IP addresses that match with this rule.



**Note:** IPv6 is also supported in the IP ranges.

### IP end

Enter the IP address that is at the end of the range of IP addresses that match with this rule.

### Stop processing

Enable this option if you want the group membership assignment to stop when the target details match this rule. If you define multiple rules, the computer name and IP address of the target is checked against every rule. However, if you enable stop processing for a rule, and a target matches the rule, the server does not check the targets details against any other rules. The target is assigned to the target groups that are associated with this matching rule and any previously processed matching rules.

### Comments

Can be used to enter a description for the rule or for some other information. Optional field.

### Priority

You can give the rule a priority level that determines when it is checked against the target. The priority level starts at 1 and increments by one as each new rule is created. Priority 1 is the highest priority. This rule is the first to be checked against the target.

The first rule that is created is automatically assigned a priority 1 value. When you create the next rule, you have the option of selecting priority 1 or 2 for this new rule. Selecting 1 makes the new rule the first rule to be checked. Each time that you create a new rule, you can select a priority level. The rules are then rearranged according to their priority level, from 1 to  $n$ , where  $n$  is the number of rules that are created.



**Note:** If you have rules that must be checked, you can make them a higher priority to ensure that they are checked against the target. Rules with a lower priority, might not be reached if you have a rule with **Stop processing** enabled near the top of the rules list.

4. Select the required groups that you want the target to be assigned to if it matches the conditions for the rule.
5. Click **Submit**.

## Viewing rules

After you create rules for assigning targets to target groups you can view the list of defined rules by completing the following steps:

1. Click **Admin > Target Membership Rules**
2. Select **Show rules**.

The list of defined rules is displayed. You can select the rules to edit the rules definition or delete the rules.

## Checking rules

You can enter a target's IP address or computer name and use the **Simulate against rules** function to check whether the target matches with any of the defined rules. The rules are displayed and any rules that match are highlighted. You can see from the matched rule what target groups the target would be assigned to if it contacted the server.

To check the target's details against already defined rules, complete the following steps:

1. Click **Admin > Target Membership Rules**
2. Select **Simulate against rules**.
3. Type in the target details that you want to search on.

### IP address

Type in the IP address that you want to check against the rules.

### Computername

Type in the computer name that you want to check against the rules.

4. Click **Test**

The List of rules is displayed. Any rules that match the IP address or computer name are highlighted and the word **matched** is displayed next to it. You can also see from the matched entry which target groups the target would be assigned to. If no match is found, a message is displayed.

## Editing rules

After you create rules for assigning targets to target groups, you can edit a rule to change the conditions that determine the target's group membership by completing the following steps:



1. Click **Admin > Target Membership Rules**
2. Select **Show rules**.
3. Select the rule.
4. Select **Edit rule**.
5. Change the information and select **Submit**.

The rule is changed. The new condition is used the next time a target's information is checked against the rule.

## Deleting rules

After you create rules for assigning targets to target groups, you can delete the rules if they are no longer required. There are multiple types of deletion that you can select.

### **Leave target membership and target groups unchanged**

You can select this option to delete the rule and nothing else. The group membership for any targets that matched this rule remains the same.

### **Reset target membership and preserve target groups**

You can select this option to delete the rule and reset the target group membership. The targets that matched this rule are no longer members of the target groups that are associated with this rule.

### **Reset membership and delete target groups**

You can select this option to delete the rule, reset the target group membership, and delete the target group. The targets that matched this rule are no longer members of the target groups that are associated with this rule. The target groups are also deleted from the Remote Control database.

Delete rules by completing the following steps:

1. Click **Admin > Target Membership Rules**.
2. Select **Show rules**.
3. Select the rules.
4. Select **Delete rules**.
5. On the **Target Membership Rules** screen, select the type of deletion.
6. Click **Submit**.

The target membership rule is deleted from the Remote Control database.

## Chapter 20. Ensure targets are registered correctly

When targets contact the server, they send configuration details that are checked against the target details in the Remote Control database. A check is done to see whether the target already contacted the server. If no match is found, a new hardware key is generated and a new target entry is created in the database. In most cases, the matching process is successful if the details supplied by the target are unique. However, in cases where targets do not have unique identifying data, or the target configuration changes, it can be more difficult to ensure the correct registration of the target. You can configure properties in the `trc.properties` file for multiple matching options so that a new entry is not created for existing targets, or multiple targets are not matched to the same entry.

### **match.computername.only**

Match on computer name only.

### **match.guid.only**

Match on GUID only.

### **Perfect or Best Match with change notifications**

There is no specific property to set for perfect match, this option is used if the

**match.computername.only** and **match.guid.only** properties are set to false. Best match can be enabled by using the **match.allow.data.changes** property. This configuration is the default configuration.

## Find a perfect or best match for a target

The perfect match option is enabled by default in Remote Control. This option is used to find a perfect match for a target, where 4 criteria are used to find a match. The criteria are Virtual Product Data (VPD), UUID, MAC\_ADDRESS, and COMPUTERTNAME. A perfect match is defined as finding a target in the database where all 4 criteria are matched successfully. However, if any of these values change for a target, 2 further properties can be used to find a match.

- **match.change.notification** - Can be used if any of the criteria values change for the target.
- **match allow.data.changes** - Can be used if only one of the criteria values change for the target. This option is defined as a best match.

### **match.change.notification**

**True**

If no match is found, a new hardware key is generated and a new target entry is created in the database.

**1 match.**

If a match is found, the details of the matched database entry are updated.

**> 1 match found.**

If more than one match is found, the first match is used. This scenario is unlikely to be found.

**False**

The old target details are not sent to the server and the new changed details are used to try to find a match. However, if only one of the 4 criteria has changed and the **match.allow.data.changes** property is set to true, a best match is looked for.

**match.allow.data.changes**

This property is used to try to find a best match for a target in the database.

**True**

This value is the default value. When set to true, a best match is successful if all but 1 of the 4 criteria match an already registered target.

**0 matches.**

If no match is found, a new hardware key is generated and a new target entry is created in the database.

**1 match.**

If a match is found, the details of the matched database entry are updated.

**> 1 match found.**

If more than one match are found, create a new hardware key.

**False**

If the perfect match process is enabled and no match is found for all 4 of the target criteria, the best match option is not considered. Depending on the value of **match.change.notifications**, if no match is found then a new target entry is created in the database.

## Match on computer name

Configure this matching option to use the target's computer name to find a match in the database. Use this method only if you have control over the naming of the targets and your environment uses targets that always have unique computer names. To use this method, enable the following property in the `trc.properties` file.

**match.computername.only**

## True

When a target contacts the server, its computer name is used to try to find a match in the database. One of the following results can be achieved.

### 0 matches.

If no match is found, a new hardware key is generated and a new target entry is created in the database.



**Note:** However, if the target is already registered and no match is found because its computer name changed, the **match.change.notifications** property can also be used. If **match.change.notifications** is set to true, the target can send the old computer name and the new computer name to try to find a match.

### 1 match.

If a match is found, the details of the matched database entry are updated.

### > 1 match found.

If more than one match is found, the other criteria that are used in the perfect match process are checked against the database. They are checked to see whether a perfect match or best match can be found. This scenario might occur if the database was previously used in an older version of Remote Control. It can also occur if the database was previously used with a different matching algorithm and there were different computers with the same computer name registered.

## False

This value is the default value. When a target contacts the server, its computer name is not used to try to find a match in the database.

## Match on GUID

Configure this matching option to use the target's Globally Unique Identifier (GUID) to find a match in the database. The GUID is created by the target software.



**Note:** When you use this method, you must not clone any computers in your environment after the target software is installed without first deleting the **TGT\_INFO.PROPERTIES** file. The file is in the target's data folder. Failure to delete the file before cloning causes many targets to match with one database entry.

### **match.guid.only**

## True

When a target contacts the server, its GUID is used to try to find a match in the database. If a match is found, the details of the matched database entry are updated. If no match is found, a new hardware key is generated and a new target entry is created in the database.

**0 matches.**

If no match is found, a new hardware key is generated and a new target entry is created in the database.

**1 match.**

If a match is found, the details of the matched database entry are updated.

**> 1 match found.**

If more than one match is found, the other 3 criteria used in the perfect match option are then checked against the database to see whether a perfect match or best match can be found. If none can be found, the entry for the first match that was found is updated.

**False**

When a target contacts the server, its GUID is not used to try to find a match in the database.

# Chapter 21. Record the session on the target

When the **Force session recording** policy is set to Yes, a remote control session is automatically recorded and uploaded to the server at the end of the session. This recording is done on the controller by default. During a collaboration session, a recording that is performed by a controller might not contain the full remote control session if session handover takes place. To ensure that a full session recording can be maintained, server policies can be configured to record the session in the target instead of the controller. The recording can also be saved to the target system after it is successfully uploaded to the server. For more information about the handover feature, see the *BigFix® Remote Control Controller User's Guide*.

## **Record the session in the target system**

Determines whether the recording of the session is done on the target system instead of the controller, when the **Force session recording** policy is set to Yes.

## **Keep session recording in the target system**

Determines whether a copy of the session recording, that was done on the target and successfully uploaded to the Remote Control server, is also saved to the target system.

For more information about the policies, see [Server session policies \(on page 95\)](#).



**Note:** When the target cannot contact the server to upload the recording, it keeps it in a queue. It later tries to contact the server. If it is successful, it sends a list of the session IDs that correspond to the recordings, to the server. The server checks each ID against the session history and if it does not find a session history for a particular ID it reports this issue to the target. If **Keep recording in target** is set to NO, the target deletes the recording. If the property is set to Yes, the target removes the recording from the queue but keeps the recording on its own disk. The following scenarios could cause the server not to find the IDs.

- The BigFix® Remote Control Server was restored from a previous backup, or the server was reinstalled with a clean database and no record of the Session ID exists in the database.
- The target was configured to connect to a different server. For example, it was pointing to Server1 and now it is redirected to Server2 but this server has no matching Session ID for the recording.

## Chapter 22. Set up for exporting recordings

A remote control session can be recorded and saved to the BigFix® Remote Control Server. This recording can then be exported and saved to a local system later. For example, to be used for education or training purposes. To enable the exporting function, you must complete the follow the setup steps relevant to the operating system you installed the BigFix® Remote Control Server on.

### Setting up a Windows server for exporting recordings

To enable the recording export function on an Remote Control Windows server, complete the following steps

1. Download and run the Java™ Media Framework (JMF) Performance Pack for Windows installer from the following site

```
http://java.sun.com/javase/technologies/desktop/media/jmf/2.1.1/download.html
```

2. Download and install the Xvid codec from [www.xvid.org](http://www.xvid.org).
3. Stop the Remote Control server service.
4. Copy the file `jmf.jar` from the JMF installation directory to the `WEB-INF\lib` directory within the BigFix® Remote Control Server installation directory.
5. If the server version is higher than 10.0.0.0624 and the server is not installed in the default folder (`C:\Program Files (x86)\BigFix`), perform the following steps:
  - a. From the `<Install_dir>\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes` folder, open the `video.properties` file and edit the `video.script.path` to match your install folder.
  - b. From the `<Install_dir>\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\rc` folder, open the `encode.cmd` file, and edit `servhome` to match your install folder.
6. Restart the Remote Control server service.

#### Important:

- The `jmf.jar` file must be copied again into the `WEB-INF\lib`, directory whenever the BigFix® Remote Control Server is updated, otherwise the exporting function is disabled.
- If the server is not installed in the default folder, the `video.properties` and the `encode.cmd` files need to be changed after the server update.

### Setting up a Linux server for exporting recordings

To enable the recording export function on an Remote Control Linux server, complete the following steps.

1. Download and run the Java Media Framework (JMF) Performance Pack for Linux installer from the following site

```
http://java.sun.com/javase/technologies/desktop/media/jmf/2.1.1/download.html
```

2. Download and install MPlayer with support for the XviD codec.  
Depending on the Linux® distribution, you are using, you might be able to install this by using the regular package repositories if you are using SuSe Linux®. If you are using RedHat Linux®, go to <http://www.mplayerhq.hu>.
3. Edit the `video.properties` file to ensure that the full path to the `encode.sh` file is set up correctly. This file is in the `WEB-INF/rc/encode.sh` directory. You must expand the relative path to an absolute path where the application was deployed by WebSphere Application Server.

```
for example :  
  
/opt/IBM/WebSphere/AppServer61/profiles/installedApplications  
  
/trc.ear/trc.war/WEB-INF/rc/encode.sh.
```

4. Stop the BigFix® Remote Control Server service by using the following command

```
/etc/init.d/trcserver stop
```

5. Copy the file `jmf.jar` from the JMF installation directory to the `WEB-INF/lib` directory within the BigFix® Remote Control Server installation directory
6. Start the BigFix® Remote Control Server service by using the following command

```
/etc/init.d/trcserver start
```



**Note:** It is important to note that the `jmf.jar` file must be copied again into the `WEB-INF/lib` directory, whenever the BigFix® Remote Control Server is updated otherwise the exporting function is disabled.



## Chapter 23. Audit log distribution

The audit log distribution feature runs a task that regularly creates a log file on the server. This file contains session information for all sessions that are established. This feature is enabled and controlled by using the following properties in the `trc.properties` file. For more information about editing this property file, see [trc.properties \(on page 216\)](#).

### **task.logdistribution.enabled**

Set to true or false.

#### **True**

The log is created and written to the server.

#### **False**

The log is not created.

### **task.logdistribution.path**

Defines the location that the log file is written to on the server. This path is created if it does not exist.

### **task.logdistribution.file**

Defines the start of the log file name, which is then appended with a time stamp.

When the feature is enabled, the task is run and the file is created on the server with a name in the following format,

*XXXtimestamp.log*

Where XXX is the value that is set for **task.logdistribution.file**.

*timestamp* is the time in milliseconds.

When the log is created each entry identifies the session, target and user, and a message of what action was carried out.

```
for example : sessionkey=8, target=TIVTEST1, user=Admin
              January 26, 2013 9:15:28 AM GMT
              Session Connection Attempt by Default Administrator
              @192.0.2.0[00:11:25:f7:b2:1e]
```



**Note:** Each time the task runs it includes the log data that was created since the last task execution.

# Chapter 24. Access targets on different networks

If you have targets, controllers, and servers on different networks that cannot directly contact each other, you can install and configure gateway support. After you install, you can configure your network to enable connections to be established. For more information about installing the gateway support, see the *BigFix® Remote Control Installation Guide*.

The Remote Control gateway supports different types of connections

## **Inbound connections**

Configure these connections for the gateway to accept connections from endpoints, controllers, and other gateways.

## **Gateway connections**

Configure a gateway to establish a permanent connection with another gateway.

## **Endpoint connections**

Configure the gateway to locate endpoints from which a request is received.

## **Tunnel Connections**

Used to facilitate TCP connections to the Remote Control server from the target.

The gateway administrator defines the connections that are required for gateways, in the configuration file.

## Configure the gateway support

After you install the gateway component is installed it can be configured by using the gateway configuration file, `trc_gateway.properties`, which is in a Java™ properties file format. This file is in the following directory, depending on the version of Windows operating system that is installed.

### **Windows® systems**

```
\Documents and Settings\All Users\Application Data\BigFix\Remote Control  
\Gateway.
```

```
\ProgramData\BigFix\Remote Control\Gateway.
```

### **Linux® systems**

```
/etc
```

Define the connections that are required in the gateway configuration file. The gateway configuration file has a similar format to a Java™ properties file.

- The gateway supports multiple instances of each connection type
- The configuration directives for each connection have a user-defined prefix.

Depending on the setup of your environment, you can define four types of connections.

- Inbound connections
- Gateway connections
- Endpoint connections
- Tunnel connections

The following optional parameters can be used to further configure your gateway.

#### **FIPSCompliance**

Set the value of this parameter to Yes to use a FIPS certified cryptographic provider for all cryptographic functions. Default value is No.

#### **SP800131ACompliance**

Set the value of this parameter to Yes to enforce NIST SP800-131A compliant algorithms and key strengths for all cryptographic functions. Default value is No.

## Configuring inbound connections

Configure Inbound connections for the gateway to accept connections from endpoints, controllers, and other gateways. You can configure multiple inbound connections and you must define a prefix for each connection parameter so that the gateway finds all required settings for each connection.

```
for example
  Inbound.1.ConnectionType
  finance.network.ConnectionType
  Connection.for.subnet.192.0.2.0.ConnectionType
```



#### **Note:**

1. Do not use #, or ! as a prefix. These characters are reserved for comments in properties files.
2. If you want to include spaces in the prefix, you must escape them with \

```
for example : my connection.ConnectionType
  should be defined as my\connection.ConnectionType
```

Inbound connections are configured by using the following parameters:

#### **ConnectionType**

Defines the type of connection. Must be set to `Inbound`. For example:

**`inbound.1.ConnectionType=Inbound`**

#### **PortToListen**

Defines the TCP port that gateways and endpoints must use to connect to this gateway. The port for listening for inbound connections. This parameter is a required parameter.

**BindTo**

This parameter is optional and can be configured to accept incoming connections on specific network interfaces. Defines the IP address that is used to create connections with. For example: **inbound.1.BindTo=192.0.2.1** Default is 0.0.0.0. This parameter is an optional parameter.

**AllowGateways**

Determines whether other gateways can connect to this connection. This parameter is optional.

**True**

Gateways are permitted to connect to this connection. This value is the default value.

**False**

Gateways are not permitted to connect to this connection.

**AllowEndpoints**

Determines whether other endpoints can connect to this connection. This parameter is optional.

**True**

Endpoints are permitted to connect to this connection. This value is the default value.

**False**

Endpoints are not permitted to connect to this connection.

**RetryDelay**

Defines the time in seconds between attempts to establish the control connection. This parameter is optional. Default is 45 seconds.

**Passphrase**

If required, the gateway can be configured to request a secret passphrase from the remote gateway to be used for authentication. This parameter is optional. For security purposes, the passphrase is automatically encrypted when you start the gateway.

## Configuring gateway connections

Gateway connections are used to configure a gateway to establish a permanent control connection with another gateway. You can configure multiple gateway connections and must define a prefix for each connection parameter so that the gateway can find all required settings for each connection. If a gateway connection is down or cannot be reached, it tries to get connected as it must have a permanent connection.

```
for example
Gateway.1.ConnectionType
G2.ConnectionType
```

See the Notes in [Configuring inbound connections \(on page 195\)](#) for rules for defining prefixes.

Gateway connections are configured by using the following parameters:

**ConnectionType**

Defines the type of connection. Must be set to `Gateway`. For example:

**gateway.1.ConnectionType=Gateway.**

**DestinationAddress**

Defines the IP address of the remote gateway that the connection is being made to. The gateway with this address must also be configured to accept inbound connections. This parameter is required.

**DestinationPort**

Defines the TCP port that the other gateway is listening on. This parameter is required.

**BindTo**

This parameter is optional. Use this parameter to configure the gateway to establish the outgoing gateway connection from a specific network interface. For example, if a firewall on the network is configured to allow only 1 of the gateway's interfaces through. Defines the IP address of the network interface through which the connections are made. For example: **gateway.1.BindTo=192.168.74.1**

Default is 0.0.0.0.

**SourcePort**

Defines the port that the outgoing gateway connections are using. This parameter is optional. Default is 0.

**RetryDelay**

Defines the time in seconds between attempts to establish the control connection. This parameter is optional. Default is 45 seconds.

**KeepAlive**

Defines the time in seconds between keepalive requests. This parameter is optional. Default is 900.

**Timeout**

The time, in seconds, to wait before a connection attempt is considered to be timed out. Default is 90.

**Passphrase**

Defines a secret passphrase if the remote gateway requires it for authentication. For security purposes, the passphrase is automatically encrypted when you start the gateway.

## Configuring endpoint connections

Endpoint connections configure the gateway to locate other endpoints from which a request is received. These connections are only needed on the gateways where the targets that you want to connect to are. You must define a prefix for each connection parameter so that the gateway can find all required settings for each connection.



**Note:** To stop an unnecessary increase in network traffic, you must not configure an endpoint connection on intermediate gateways that merely connect two separate gateways.

Endpoint connections are configured by using the following parameters:

**ConnectionType**

Defines the type of connection. Must be set to `Endpoint`. For example:

**endpoint.1.ConnectionType=Endpoint**

**SubnetAddress**

Defines the IP address of a subnet that can be connected to, either directly or indirectly. You must define an endpoint connection for each required subnet. This way, the gateway automatically filters out attempts to endpoints that it cannot reach. This parameter is optional.



**Note:** The default is 0.0.0.0/0.0.0.0, which specifies that the gateway attempts to connect to any endpoint.

**SubnetMask**

Defines the subnet mask of a subnet that can be connected to, either directly or indirectly. If you do not specify a value, the gateway tries to connect to any target. Therefore, by specifying specific values you can define which addresses to look at so that it is optimized. This parameter is optional. Default is 0.0.0.0.

**BindTo**

Defines the IP address of the network interface through which the connection is made. If required, the gateway can be configured to connect to the endpoints from a specific port and interface only. This configuration might be required if the endpoints have a desktop firewall that allows only the gateways to connect to them. For example: **endpoint.1.BindTo=192.168.74.1** This parameter is optional. Default value is 0.0.0.0.

**SourcePort**

Defines the port that outgoing connections are made from. This parameter is optional. Default is 0.

**Timeout**

The time, in seconds, after which an endpoint connection is considered to be timed out. This parameter is optional. Default value is 45 seconds.

## Configuring tunnel connections

Tunnel connections provide a way for targets to connect to the server when there is no other way to connect to each other. You can define multiple tunnel connections. The gateway supports two types of connection, one for each end of a tunnel. The gateway supports tunnels to multiple destinations. For example, if you have a single site with multiple instances of Remote Control to support multiple customers. You must define a prefix for each connection parameter so that the gateway can find all required settings for each connection.

Tunnel Connections are configured by using the following parameters:

**ConnectionType**

Defines the type of connection. For example: `tunnel.1.ConnectionType=InboundTunnel`

### **InboundTunnel**

An inbound tunnel connection is used to configure a gateway to listen for incoming connections from endpoints that want to connect to the server.

### **OutboundTunnel**

An outbound tunnel connection, is used to connect the tunnel to the destination, for example the Remote Control server.

**The connection types use the following parameters.**

#### **Inbound connections.**

##### **TunnelID**

The TunnelID is used to associate an inbound connection with the correct outbound connections. The default value is TRCSERVER. For example:

`tunnel.1.TunnelID = TRCSERVER`. This parameter is optional.

##### **PortToListen**

Defines the TCP port that the target must use to connect to the tunnel connection. This parameter is required.

##### **BindTo**

Defines the IP address that is used to create the connection. This parameter is optional.

##### **RetryDelay**

Defines the time in seconds to wait before the gateway listens for new connections. This parameter is optional.

#### **Outbound connections.**

##### **TunnelID**

The TunnelID is used to associate an inbound connection with the correct outbound connections. The default value is TRCSERVER. For example:

`tunnel.1.TunnelID = TRCSERVER`. This parameter is optional.

##### **BindTo**

Defines the IP address that is used to create the connection. This parameter is optional.

##### **Destination Address.**

Defines the IP address of the BigFix® Remote Control Server that the tunnel connection is being made to. This parameter is required.

##### **DestinationPort**

Defines the TCP port that the BigFix® Remote Control Server is listening on.  
This parameter is required.

#### Timeout

Defines the time in seconds to wait before a connection attempt is considered to be timed out. This parameter is optional.

## Configuring the targets to use tunnel connections

For targets that need to contact an BigFix® Remote Control Server on a different network you can modify the **ProxyURL** target property so that a connection to the server can be made by using a tunnel connection.

### Configuring a Windows target to use tunnel connections

To modify the **ProxyURL** property on a Windows target, 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 the **ProxyURL** entry and click **Modify**.
4. Type `trcgw://gatewayaddress:port` in the **Value data** field and click **OK**.  
Where *gatewayaddress* is the host name or IP address and *port* is the port of the gateway that the target must connect to so that it can use the tunnel connection.
5. Restart the target service.

### Configuring a Linux target to use tunnel connections

To modify the **ProxyURL** property on a Linux target, complete the following steps:

1. Edit the `trc_target.properties` file and modify the **ProxyURL** entry by setting it to  
`trcgw://gatewayaddress:port.`  
Where *gatewayaddress* is the IP address or host name of the gateway that the target connects to so that it can use the tunnel connection. *Port* is the port that the target must connect to so that it can use the tunnel connection.
2. Save the file.
3. Restart the target service.

## Configure gateways in IPv6 networks

### Configure inbound connections

When an inbound connection is defined in the gateway configuration file, it can listen by default for incoming connections from any IPv4 address and would be configured as follows

```
prefix.ConnectionType=Inbound
```



```
prefix.PortToListen=8881
```

```
prefix2.ConnectionType=InboundTunnel
```

```
prefix2.PortToListen=8882
```

Previously to create an inbound connection for IPv6, the connection was bound to the IPv6 ANY address, which is 0:0:0:0:0:0 or in compressed notation: ::.

```
prefix.ConnectionType = Inbound
```

```
prefix.PortToListen=8881
```

```
prefix.BindTo= \::
```



**Note:** As the colon can be used as a separator in properties files, it must be escaped with a backslash character to indicate that it is part of the value and not the separator.

To configure an inbound connection for incoming connections from IPv6 addresses, you can use *Inbound6* or *InboundTunnel6* instead.

```
prefix.ConnectionType = Inbound6
```

```
prefix.PortToListen = 8881
```

```
prefix2.ConnectionType = InboundTunnel6
```

```
prefix2.PortToListen = 8882
```



**Note:** For the gateway to listen for both IPv4 and IPv6 incoming connections, you must define an **inbound** and an **inbound6** connection type entry in the gateway configuration file.

## Configure endpoint connections

To specify an IP subnet in IPv4, you must specify the subnet address and the subnet mask.

```
prefix.ConnectionType = Endpoint
```

```
prefix.SubnetAddress = 198.51.100.0
```

```
prefix.SubnetMask = 255.255.255.0
```

As IPv6 addresses are much longer than IPv4 addresses, the subnet mask notation is not used for IPv6. Both IPv4 and IPv6 support Classless Inter-Domain Routing (CIDR) notation, which specifies the length of the subnet prefix after the subnet address.

```
prefix.ConnectionType = Endpoint
```

```
prefix.Subnet = 198.51.100.0/24
```

```
prefix2.ConnectionType = Endpoint
```

```
prefix2.Subnet = 2001:db8:d005:ee::/64
```



**Note:** The gateway does not support IPv6 subnets with the SubnetAddress / SubnetMask notation.

When an endpoint connection is defined in the gateway, by default it tries to locate all endpoints with any IPv4 address.

```
prefix.ConnectionType = Endpoint
```

Previously to configure an endpoint connection for IPv6 the default Subnet had to be overwritten.

```
prefix.ConnectionType = Endpoint
```

```
prefix.Subnet = \::/0
```

To configure an endpoint connection that tries to locate all endpoints with IPv6 addresses, you can now use *Endpoint6* instead.

```
prefix.ConnectionType = Endpoint6
```

## Gateway setup example

The following example illustrates a gateway and tunnel connection setup. There are three networks present, a secure network, a DMZ network and an unsecure network. Firewalls are installed to control traffic between the secure network and the DMZ and between the DMZ and the unsecure network. The security policy in force does not allow network connections to be initiated from the unsecure network to the DMZ or from the DMZ to the secure network. Network connections from the secure to the DMZ and from the DMZ to the unsecure network are allowed for particular ports. The BigFix® Remote Control Server component is installed on a server that is attached to the secure network and controller computers are also present on the secure network. Applications are run on servers that are attached to the unsecure network and these servers are unattended. The Remote Control target is installed on these systems to provide remote access for maintenance and support. No connections can be initiated from the unsecure network to the DMZ or from the DMZ to the secure network, therefore a chain of proxy servers cannot be used. The proxy server on the unsecure network is unable to connect to the proxy server on the DMZ to forward incoming HTTP requests. The solution for this scenario is to install a gateway in each of the networks.

Remote Control components present

**Table 4. Remote Control components present on network**

<b>Network name</b>	<b>Server</b>	<b>Con- troller</b>	<b>Tar- get</b>
Secure network	Yes	Yes	No
DMZ	No	No	No
Unsecure net- work	No	No	Yes

Networks**Table 5. Networks**

<b>Network name</b>	<b>Subnet address</b>	<b>Netmask</b>
Secure network	10.1.0.0	255.255.255.0
DMZ	10.2.0.0	255.255.255.0
Unsecure net- work	10.3.0.0	255.255.255.0

Machines**Table 6. Machines**

<b>Hostname</b>	<b>IP ad- dress</b>	<b>Roles</b>
SERVER	10.1.0.2	Remote control server on port 80
GATE- WAYA	10.1.0.254	Remote control gateway on port 8881
GATE- WAYB	10.2.0.254	Remote control gateway on port 8881
GATE- WAYC	10.3.0.254	Remote control gateway on port 8881
TARGET	10.1.0.3	Remote control target on port 888

Firewall

**Table 7. Firewall**

Source	DestinationPort	Port	Description
10.1.0.254/255.255.255.255	10.2.0.254/255.255.255.255	8881	Allow GATEWAYA to connect to GATEWAYB
10.2.0.254/255.255.255.255	10.3.0.254/255.255.255.255	8881	Allow GATEWAYB to connect to GATEWAYC

Gateway setup

- Gateway support is installed on computer GATEWAYA in the secure network. An Remote Control gateway that is named GATEWAYA is also installed because there are controllers present on the secure network. The controllers need to connect to the targets on the unsecure network.

To install the gateway support, see the *BigFix® Remote Control Installation Guide*.

To create the gateway, complete the following steps on the BigFix® Remote Control Server:

1. Click **Admin > New Remote Control Gateway**.
  2. On the **Add Remote Control Gateway** screen, enter the required details
    - **Host name** - GATEWAYA
    - **Description** - (optional)
    - **IP address** - 10.1.0.254
    - **Port** - 8881
  3. Click **Submit**.
- Gateway support is installed on computer GATEWAYB in the DMZ network.

To install the gateway support see BigFix® Remote Control Installation Guide.

- Gateway support is installed on computer GATEWAYC in the unsecure network.

To install the gateway support, see the *BigFix® Remote Control Installation Guide*.

- GATEWAYA is configured with a gateway control connection to GATEWAYB.
- GATEWAYB is configured with a gateway control connection to GATEWAYC.
- Gateway A is configured with an outbound tunnel connection to the Remote Control server.
- Gateway C is configured with an inbound tunnel connection on port 8880.
- The targets in the unsecure network are configured to connect through the inbound tunnel connection on GATEWAYC.

Gateway configurationGATEWAYA configuration file

Inbound.1.ConnectionType= Inbound

Inbound.1.PortToListen = 8881

Gateway.A.ConnectionType=Gateway

Gateway.A.DestinationAddress = 10.2.0.254 - GATEWAYA connects to GATEWAYB

Gateway.A.DestinationPort = 8881

Gateway.A.RetryDelay = 15

Gateway.A.KeepAlive = 900

OutboundTunnel.1.ConnectionType=OutboundTunnel

OutboundTunnel.1.DestinationAddress = 10.1.0.2 - connection to the Remote Control server

OutboundTunnel.1.DestinationPort = 80

#### GATEWAYB configuration file

Inbound.1.ConnectionType= Inbound

Inbound.1.PortToListen = 8881

Gateway.B.ConnectionType=Gateway

Gateway.B.DestinationAddress = 10.3.0.254 - GATEWAYB connects to GATEWAYC

Gateway.B.DestinationPort = 80

Gateway.B.RetryDelay = 15

Gateway.B.KeepAlive = 900

#### GATEWAYC configuration file

Inbound.1.ConnectionType= Inbound

Inbound.1.PortToListen = 8881

InboundTunnel.1.ConnectionType=InboundTunnel

InboundTunnel.1.PortToListen = 8880. The port that the target must use to connect to the tunnel connection

Endpoint.1.ConnectionType=Endpoint

Endpoint.1.SubnetAddress= 10.3.0.0 - the network address of the unsecure network that the target is connected to.

Endpoint.1.SubnetMask= 255.255.255.0

When a target requires an HTTP or HTTPS connection with the BigFix® Remote Control Server, it first connects to port 8880 on GATEWAYC. GATEWAYC accepts this connection and immediately creates a tunnel to GATEWAYA,

through GATEWAYB. GATEWAYA then connects to the BigFix® Remote Control Server and acknowledges the connection to GATEWAYC through GATEWAYB. When the tunnel is established, gateways C and A start to read any data from their respective connections. They forward it to each other through the tunnel and write any traffic that is received from the tunnel to this connection. The result is that the target and the server can communicate and are unaware that the traffic is being tunneled. When either party shuts down their end of the connection, the tunnel is torn down and the other connection is also shut down.

## Track connection requests

An area of memory that is known as the **Request Pool** is used to track requests. The connection requests are kept in the pool until the pool is full and the oldest requests are recycled. This is done to prevent requests from looping around in the gateway network undetected.

The following parameters can be used to configure the request pool:



**Note:** Configuration of the request pool is optional.

### **RequestPool.Size**

The amount of memory, in KB, to reserve for the request pool. The default is 2048 or 2 megabytes.

### **RequestPool.MinimumTTL**

The minimum time, in minutes, before a request can be recycled. The default is 5 minutes.



**Note:** Each request requires 32 bytes of memory. The gateway can handle more than 200 requests per second with the default settings.

## Logging gateway activity

When the gateway support is installed, a log file is created in the following directories:

### **Windows® systems**

```
Documents and Settings\All Users\ Application Data\BigFix\Remote Control
\Gateway
```

Or

```
\ProgramData\BigFix\Remote Control\Gateway.
```

### **Linux® systems**

```
/var/opt/bigfix/trc/gateway
```

The name of the log file is `TRCGATEWAY-hostname-suffix.log`. `hostname` denotes the computer name or host name of the system where the gateway is installed. `suffix` is determined by the LogRotation and LogRollover settings.

For example, `TRCGATEWAY-mygateway-1-THU-18H.log`

To configure logging complete the following steps:

1. Configure the following properties within the `trc_gateway.properties` file.

#### **LogLevel**

Set the required logging level.

The log level determines the types of entries and how much information is added to the log file.

Default value is 2.

#### **LogRotation**

Controls the period after which an older log file is overwritten. Log rotation can be disabled.

Default value is Weekly.

#### **LogRollOver**

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.

2. Save the file.

For more information about the properties, see [Properties for configuring logging activity \(on page 425\)](#)

## Configuration file example

When the configuration file is created, it provides examples of the required configuration parameters that you can use to create a configuration file to satisfy your network requirements. The following file is an example of the file when it is installed.

```
# Please refer to the Administrator's Guide for instructions regarding this
```

```
# Configuration file for Remote Control Gateway
```

```
# configuration file.
```

```
# Logging levels
```

```
#
```

```
# 0 no logging
```

```
#1 error
```

```
# 2 informational (default)
```

```
# 4 debug information (only by request from HCL)
```

```
# LogLevel = 2
```

# Log rotation and rollover

LogRotation = Weekly

LogRollover = Daily

# LogRotation Rotate between log files (Daily, Weekly, Monthly, Disabled)

# LogRollover Switch log files (Hourly, Daily)

#

# Defaults

# LogRotation Weekly

# LogRollover Daily

# Use a FIPS certified cryptographic provider for all cryptographic functions

FIPSCompliance = No

# Request Pool

# The gateway stores session requests that it is processing in the request

# pool. The request pool uses a fixed amount of memory.

# Size of the request pool (kilobytes)

# Each request needs 32 bytes

# RequestPool.Size = 2048

# Time before a request from the pool can be re-used, in minutes

# RequestPool.MinimumTTL = 5

# Defaults

#

# RequestPool.Size 2048

# RequestPool.MinimumTTL 5

# Inbound Connections

# Connections to accept incoming connections from endpoints and gateways



```
# Inbound.1.ConnectionType = Inbound
# Inbound.1.PortToListen = 8881
# Inbound.PortToListen TCP port that gateways and endpoints should
# use to connect to this gateway (required)
# Inbound.BindTo Accept incoming connections on the
# specified IP address only (optional)
# Inbound.RetryDelay Time, in seconds, between attempts to
# listen for incoming connections (optional)
# Inbound.Passphrase Secret passphrase that remote gateways are
# required to authenticate with (optional)
# Inbound.1.AllowGateways Allow gateways to connect to this connection
# (yes/no or true/false) (optional)
# Inbound.1.AllowEndpoints Allow endpoints to connect to this connection
# Defaults
# (yes/no or true/false) (optional)
#
# Inbound.BindTo 0.0.0.0
# Inbound.RetryDelay 45
# Inbound.AllowGateways yes
# Inbound.AllowEndpoints yes

# Examples
# Inbound.2.ConnectionType = Inbound
# Inbound.2.PortToListen = 8881
# Inbound.2.BindTo = 192.168.74.254
# Inbound.2.Passphrase = qagumczw0krbmyajc0kehnrryuTv1zxyevdckcwsrk}bjfi
# Inbound.2.AllowGateways = true
```

```
# Inbound.2.AllowEndpoints = false

# Inbound.3.ConnectionType = Inbound
# Inbound.3.PortToListen = 8881
# Inbound.3.BindTo = 192.168.75.254

# Inbound.4.ConnectionType = Inbound
# Inbound.4.PortToListen = 8881
# Inbound.4.BindTo = 192.168.76.254
# Inbound.4.RetryDelay = 30

# Gateway Connections

# Outgoing control connections to neighbour gateways

# Gateway.1.ConnectionType = Gateway
# Gateway.1.DestinationAddress = 192.168.77.254
# Gateway.1.DestinationPort = 8881

# Gateway.DestinationAddress IP address of the remote gateway
# Gateway.DestinationPort TCP port of the remote gateway
# Gateway.BindTo Force outgoing connections from the
# specified IP address only (optional)
# Gateway.SourcePort Force outgoing connections from the
# specified port only (optional)
# Gateway.RetryDelay Time, in seconds, between attempts to
# connect to the remote gateway (optional)
# Gateway.KeepAlive Time, in seconds, between keepalive
# requests (optional)
# Gateway.Timeout Time, in seconds, before a connection
```

```
# attempt is considered to have timed

# out (optional)

# Gateway.Passphrase Secret passphrase if the remote gateway

# requires authentication

# Defaults

#

# Gateway.BindTo 0.0.0.0

# Gateway.SourcePort 0

# Gateway.RetryDelay 45

# Gateway.KeepAlive 900

# Gateway.Timeout 90

# Examples

# Gateway.2.ConnectionType = Gateway

# Gateway.2.DestinationAddress = 192.168.78.254

# Gateway.2.DestinationPort = 8881

# Gateway.2.BindTo = 192.168.74.254

# Gateway.2.SourcePort = 8882

# Gateway.2.RetryDelay = 90

# Gateway.2.KeepAlive = 180

# Gateway.2.Timeout = 30

# Endpoint connections

# Configures the gateways to try to find an endpoint when a session request

# is received

# Endpoint.1.ConnectionType = Endpoint

# Endpoint.SubnetAddress The network address for the subnet that

# this connection can reach (optional)
```

# Endpoint.SubnetMask The network mask for the subnet that this

# connection can reach (optional)

# Endpoint.BindTo Force outgoing connections from the

# specified IP address only (optional)

# Endpoint.SourcePort Force outgoing connections from the

# specified port only (optional)

# Endpoint.Timeout Time, in seconds, before a connection

# attempt is considered to have timed

# out (optional)

# Defaults

#

# Endpoint.SubnetAddress 0.0.0.0

# Endpoint.SubnetMask 0.0.0.0

# Endpoint.BindTo 0.0.0.0

# Endpoint.SourcePort 0

# Endpoint.Timeout 45

# Examples

# Endpoint.2.ConnectionType = Endpoint

# Endpoint.2.SubnetAddress = 192.168.79.0

# Endpoint.2.SubnetMask = 255.255.255.0

# Endpoint.3.ConnectionType = Endpoint

# Endpoint.3.SubnetAddress = 192.168.80.0

# Endpoint.3.SubnetMask = 255.255.255.0

# Endpoint.4.ConnectionType = Endpoint

# Endpoint.4.BindTo = 192.168.74.254

# Endpoint.4.SourcePort = 8882

```
# Tunnel connections

# Tunnel connections are used to provide connections to the TRC server for the endpoints
# when they cannot reach the server directly or via an http proxy.

# Setting up a tunnel requires two types of connections. On the gateways that can reach
# the server, an outbound tunnel connection needs to be configured. On the gateways that
# the endpoints can reach, an inbound tunnel is required. When an endpoint connects to the
# inbound tunnel port, the gateway will locate one of the corresponding outbound tunnels
# through the gateway control network. The outbound tunnel then connects to the server to
# complete the tunnel. At that point, the gateways will forward all traffic between the
# endpoint and the server through the tunnel.

# Outbound tunnel connection

# OutboundTunnel.1.ConnectionType = OutboundTunnel
# OutboundTunnel.1.DestinationAddress IP address of the server (required)
# OutboundTunnel.1.DestinationPort TCP port of the server (optional)
# OutboundTunnel.1.TunnelID ID to relate inbound and outbound
# tunnels to each other (optional)
# OutboundTunnel.1.BindTo Force outgoing connections from the
# specified IP address (optional)
# OutboundTunnel.1.Timeout Time, in seconds, before a connection
# attempt is considered to have timed
# out (optional).

# Defaults

#
# DestinationPort 80
# TunnelID TRCSERVER
# BindTo 0.0.0.0
```

```
# Timeout 90

#

# Examples

# OutboundTunnel.2.ConnectionType = OutboundTunnel

# OutboundTunnel.2.DestinationAddress = 192.168.81.52

# OutboundTunnel.3.ConnectionType = OutboundTunnel

# OutboundTunnel.3.DestinationAddress = 192.168.81.52

# OutboundTunnel.3.DestinationPort = 443

# Inbound tunnel connection

# InboundTunnel.1.ConnectionType = InboundTunnel

# InboundTunnel.1.PortToListen TCP port that endpoints should use to

# connect to the tunnel (required)

# InboundTunnel.1.TunnelID ID to relate inbound and outbound

# tunnels to each other (optional)

# InboundTunnel.1.BindTo Accept incoming connections on the

# specified IP address only (optional)

# InboundTunnel.1.RetryDelay Time, in seconds, between attempts to

# listen for incoming connections (optional)

# Defaults

#

# TunnelID TRCSERVER

# BindTo 0.0.0.0

# RetryDelay 45
```

## Chapter 25. Editing the properties files

You can use the properties files in Remote Control to customize your environment, configure LDAP, set debug options, and set controller and on-demand target properties. The files can be edited in the BigFix® Remote Control Server UI.

The following properties files are available.

- `trc.properties`
- `log4j2.properties`
- `ldap.properties`
- `common.properties`
- `appversion.properties`
- `controller.properties`
- `ondemand.properties`

For more information about modifying the `log4j2.properties` file, see <http://logging.apache.org/log4j/docs/>

To edit the properties files in the BigFix® Remote Control Server UI, complete the following steps.

1. Click **Admin > Edit properties file**.  
The **Edit Properties File** panel is displayed.
2. Select the relevant file from the list.
3. Make the changes and click **Submit**.
4. For the new property values to take effect click **Admin > Reset Application**.

As there is a short delay while the file is rewritten, you must not make any immediate changes until the application is reset.



**Note:** To manually edit the properties files, locate them on the server and edit them. If you edit the files manually, you must reset the server application by selecting **Admin > Reset Application** for the new values to be displayed when you edit the file in the UI.

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 (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 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
```

## Template of field information

A table-style template has been applied to each of the properties files in the following sections. This template includes the following items:

- Category Description
- Modifiable Field
- Field Description
- Possible Values
- Value Definition

**Category Description:** There are several different categories within the file. Each category focuses on a particular function carried out by the Remote Control program. These categories are the same as those configured in the installation.

Modifiable Field	The field contains one or more parameters used to accomplish a specific task within the category.
Field Description	The field is used to describe precisely what function the field parameter is performing.
Possible Values	This field identifies all of the possible values that can be used within the field parameter.
Value Definition	This field defines how the program will carry out certain functions depending on what value is associated with the field parameter.

## trc.properties

Definitions of the properties in the `trc.properties` file that is packaged with the BigFix® Remote Control Server.

DO NOT EDIT THE FOLLOWING LINE

```
rc.enabled=
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
rc.heartbeat_timeout=
```



Modifiable Field	<b>rc.heartbeat_timeout</b>
Field Description	While an endpoint is active, it periodically reports back to the server. This value is the number of minutes between each report back to the server or heartbeat.
Possible Values	User Defined
Value Definition	

```
rc.create.assets.from.callhome=
```

Modifiable Field	<b>rc.create.assets.from.callhome</b>
Field Description	If target information sent from the target to the server is not already in the database, create these targets in the database
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Target information is added to the database.</p> <p><b>False</b></p> <p>Target information is not added to the database.</p>

```
rc.create.assets.from.brokers=
```

Modifiable Field	<b>rc.create.assets.from.brokers</b>
Field Description	Use to allow an unregistered target to register with the server at the start of a remote control session that uses a broker. The target information is sent to the server when the target user enters the connection code.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Unregistered targets are added to the database.</p> <p><b>False</b></p> <p>Unregistered targets are not added to the database.</p>

DO NOT EDIT THE FOLLOWING LINES

```
rc.validation.relative.url=
rc.audit.relative.url=
rc.upload.url=
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
rc.show.controller.splash=
```

Modifiable Field	<b>rc.show.controller.splash</b>
Field Description	Use this property to determine whether the controller splash screen is displayed before the remote control session starts.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The controller splash screen is displayed before the remote control session starts. True is the default value.</p> <p><b>False</b></p> <p>The controller splash screen is not displayed during the initiation of a remote control session.</p>

```
rc.recording.directory=
```

Modifiable Field	<b>rc.recording.directory</b>
Field Description	Directory that is used for storing session recordings on the Server.
Possible Values	User-defined. For example, <code>rc_recordings</code> . Can be specific or relative.
Value Definition	

```
unknown.recording.action=
```

Modifiable Field	<b>unknown.recording.action</b>
Field Description	Determines what action is returned to the target if a target requests to upload a recording for a session that is not known to the server.
Possible Values	0, 1, 2
Value Definition	<p><b>0</b></p> <p>The target can upload the recording.</p> <p><b>1</b></p> <p>The target must keep the recording locally in its file system.</p> <p><b>2</b></p>

The target must delete the recording.

```
rc.dialog.session.accept.directory=
```

Modifiable Field	<b>rc.dialog.session.accept.directory</b>
Field Description	Directory that is used for storing bitmap files that are uploaded when you configure the session acceptance window.
Possible Values	User-defined. For example, <code>/sad_config</code> . Can be specific or relative.
Value Definition	

DO NOT EDIT THE FOLLOWING LINE:

```
schema=
```

### Category Description: Email Settings

```
email.enabled=
```

Modifiable Field	<b>email.enabled</b>
Field Description	Enable the email function.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Email is enabled.</p> <p><b>False</b></p> <p>Email is not enabled.</p>

```
smtp.server=
```

Modifiable Field	<b>smtp.server</b>
Field Description	The address of the SMTP server you are using for email.
Possible Values	User-defined. For example, <code>myserver.email.com</code>
Value Definition	

```
smtp.authentication=
```

Modifiable Field	<b>smtp.authentication</b>
------------------	----------------------------

Field Description	The SMTP server must authenticate the SMTP user ID and password.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>SMTP server must authenticate the user ID and password.</p> <p><b>False</b></p> <p>SMTP server does not authenticate the user ID and password.</p>

```
smtp.userid=
```

Modifiable Field	<b>smtp.userid</b>
Field Description	The user ID for the SMTP server.
Possible Values	User-defined string
Value Definition	

```
smtp.password=
```

Modifiable Field	<b>smtp.password</b>
Field Description	The password for the SMTP server.
Possible Values	User-defined
Value Definition	You can enter the password as plain text. However, for security purposes the password can be encrypted. To encrypt the password, enter the plain text and click <b>Encrypt</b> .

```
error.admin.contact=
```

Modifiable Field	<b>error.admin.contact</b>
Field Description	Details or relevant message for contacting an administrator to report a problem.
Possible Values	User-defined message. For example, <code>Contact helpdesk on 123456-123-123</code>
Value Definition	

```
file.email.name =
```

Modifiable Field	<b>file.email.name</b>
Field Description	Default file name that is used when a report is mailed out. For example, Selecting <b>Email Report</b> from the <b>Options</b> menu. The report is exported into a CSV file with this file name and attached to the email.
Possible Values	User-defined. For example, <code>report.csv</code> .
Value Definition	Must not be blank and must contain only characters that are valid for a file name.

```
file.email.mime.type =
```

Modifiable Field	<b>file.email.mime.type</b>
Field Description	Represents the mime type for the file that is attached to an email when a report is mailed out.
Possible Values	User-defined. For example, <code>application/vnd.ms.excel</code> .
Value Definition	User-defined. Default is <code>application/vnd.ms.excel</code> . Must be a mime-type that is compatible only with plain-text or comma-separated value (CSV) files.

```
file.email.encoding =
```

Modifiable Field	<b>file.email.encoding</b>
Field Description	Represents the encoding for the file that is attached to an email when a report is mailed out.
Possible Values	UTF-8, UTF-16BE, UTF16LE
Value Definition	Default value is UTF16LE (Windows™ standard for Excel).


```
file.email.type =
```

Modifiable Field	<b>file.email.type</b>
Field Description	Represents the type for the file that is attached to an email when a report is mailed out.
Possible Values	TSV, CSV
Value Definition	User-defined. TSV (Tab Separated Value), CSV (comma-separated value).

**Category Description: Email Templates**`url=`

Modifiable Field	<b>url</b>
Field Description	The main URL that is used to access the BigFix® Remote Control Server UI.
Possible Values	User-defined - for example <code>http://192.0.2.0/trc</code>
Value Definition	User-defined. URL and context root of application.

`secure.url=`

Modifiable Field	<b>secure.url</b>
Field Description	Determines the base URL that is used to redirect requests when secure communications are required.
Possible Values	User-defined - for example <code>https://X.X.X.X/trc</code> where X.X.X.X is the IP address of your BigFix® Remote Control Server.   <b>Note:</b> The <b>url</b> property must also be configured. Do not replace HTTP with HTTPS in the <b>url</b> property because the ports for each might be different.
Value Definition	User-defined. URL and context root of application when you use secure connections.


`enforce.secure.web.access=`

Modifiable Field	<b>enforce.secure.web.access</b>
Field Description	An HTTP request that is not a target request. The upload, or validation request is redirected to the same URL but uses the value that is set in the <b>secure.url</b> parameter as a base.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The http request is redirected to the secure url. This value is the default value.</p> <p><b>False</b></p> <p>The http request is not redirected to the secure url.</p>




**Note:** When you change the value of this property, you must restart the BigFix® Remote Control Server service for the new value to take effect.

`enforce.secure.endpoint.callhome=`

Modifiable Field	<b>enforce.secure.endpoint.callhome</b>
Field Description	Determines the url that is used by targets when they send information to the BigFix® Remote Control Server.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>If an HTTP request is received from a target, the request is redirected to the secure url. The secure url is also returned in the response form the server. Forces targets to use the secure url when they contact the BigFix® Remote Control Server. When you enable this property and you configure a broker in your environment, you must set the <b>ServerURL</b> parameter in the broker properties file to HTTPS. Otherwise, the broker does not redirect to the secure url and the target cannot send information to the server. This value is the default value.</p> <p><b>False</b></p> <p>Targets are not forced to use the secure url when they contact the BigFix® Remote Control Server. False is the default value.</p> <p> <b>Note:</b> When you change the value of this property, you must restart the BigFix® Remote Control Server service for the new value to take effect.</p>

`enforce.secure.endpoint.upload=`

Modifiable Field	<b>enforce.secure.endpoint.upload</b>
Field Description	Determines whether the controller or target must use the secure url to upload the recordings and audit information to the server.

Possible Values	True / False
Value Definition	<p><b>True</b></p> <p>If an HTTP upload or a validation request is received, the server redirects the request to an equivalent URL. The URL is built with the value that is defined in <b>secure.url</b> as a base. The server also uses the value of <b>secure.url</b> as a base to provide the upload and validation URLs to the controller and target when the session starts. When you enable this property and you configure a broker in your environment, you must set the <b>ServerURL</b> parameter in the broker properties file to HTTPS. Otherwise, the broker does not redirect to the secure url and the target cannot send information to the server. This value is the default value.</p> <p><b>False</b></p> <p>If an HTTP upload or a validation request is received, the server does not redirect to the secure url.</p> <p> <b>Note:</b> When you change the value of this property, you must restart the BigFix® Remote Control Server service in order for the new value to take effect.</p>

```
enforce.secure.weblogon=
```

Modifiable Field	<b>enforce.secure.weblogon</b>
Field Description	Forces the default logon from the server UI to use HTTPS. This property requires <b>secure.url</b> to be set with the full host name.
Possible Values	True / False
Value Definition	<p><b>True</b></p> <p>Log on requests from the BigFix® Remote Control Server UI use HTTPS. HTTPS is not shown in the url, but the logon page with USERID/PASSWORD is posted by using HTTPS. The URL that is defined in the <b>secure.url</b> parameter is used. If <b>secure.url</b> is set incorrectly, the logon does not succeed. Enabling this parameter does not prevent a logon request that uses</p>



	<p>HTTP through another tool or page. This value is the default value.</p> <p><b>False</b></p> <p>Log on by using HTTP or HTTPS. Whichever protocol that is used in the URL that is entered in the browser is used.</p>
--	---

```
enforce.secure.alllogon=
```



Modifiable Field	<b>enforce.secure.alllogon</b>
Field Description	Force any logon action to use HTTPS, deny any non-HTTPS logon. When you enable this property, you must set <b>secure.url</b> with the full host name.
Possible Values	True / False
Value Definition	<p><b>True</b></p> <p>Any logon attempt that uses HTTP is rejected and redirected to the logon page. This value is the default value.</p> <p><b>False</b></p> <p>Log on by using HTTP or HTTPS. Whichever protocol that is used in the URL that is entered in the browser is used.</p>

```
account.lockout=
```


Modifiable Field	<b>account.lockout</b>
Field Description	Lock a user account after a consecutive number failed logon attempts. Set to 0 to disable this function.
Possible Values	user defined
Value Definition	User-defined. Integer.

```
account.lockout.timeout=
```

Modifiable Field	<b>account.lockout.timeout</b>
Field Description	If a user account is locked out due to consecutive failed logon attempts, re-enable the account after this time. The period can be MIN, HOUR, DAY, MONTH.


	 <b>Note:</b> This property is only valid when <b>account.lockout</b> is enabled.
Possible Values	User-defined
Value Definition	<p>User-defined. MIN, HOUR, DAY, MONTH. For example, set to <i>5MIN</i> means that the account is locked for 5 minutes. Set to <i>2DAY</i> means that the account is locked for 2 days.</p>  <b>Note:</b> If left blank, the account is locked until manually set.

```
account.lockout.allowlogonfrom=
```

Modifiable Field	<b>account.lockout.allowlogonfrom</b>
Field Description	<p>Use this property to allow users to log on from this host even if their account is locked out due to consecutive failed logon attempts. If your account is locked, you can log on to the BigFix® Remote Control Server from the computers whose IP address is listed. For example, <i>192.0.2.1;192.0.2.2;</i></p>  <b>Note:</b> It is important to end each host name with a semi-colon.
Possible Values	User-defined -
Value Definition	User-defined. A list of IP addresses separated by a semi-colon. End the list with a semi-colon.

```
account.lockout.reset.on.emailpassword=
```

Modifiable Field	<b>account.lockout.reset.on.emailpassword</b>
Field Description	Determines whether a locked account is reset when the user selects the forgotten password check box on the logon screen.
Possible Values	True / False
Value Definition	<p><b>True</b></p> <p>The locked account is reset when the password reset email is received from the administrator.</p>

	<p><b>False</b></p> <p>The locked account is not reset when the forgotten password request is received.</p> <p> <b>Note:</b> As this property uses the forgotten password feature, email must be enabled in the system.</p>
--	--

```
always.use.preinstalled.controller=
```

Modifiable Field	<b>always.use.preinstalled.controller</b>
Field Description	Determines whether an installed controller is used when you start a managed session, rather than using Java™ Web Start.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The installed controller is used when you start a managed remote control session.</p> <p><b>False</b></p> <p>The installed controller is not used when you start a managed remote control session. This value is the default value.</p>

DO NOT EDIT THIS LINE

```
ip.address=
```

```
email.from=
```

Modifiable Field	<b>email.from</b>
Field Description	The email address to which users respond when they receive email requests; in some cases, this email address might be the same as the administrators email address.
Possible Values	User-defined. For example, <code>trc@example.com</code>
Value Definition	Email address

```
email.admin=
```

Modifiable Field	<b>email.admin</b>
------------------	--------------------

Field Description	The email address of the administrator for reporting problems to.
Possible Values	User-defined. For example, <code>admin@example.com</code>
Value Definition	Email address

**DO NOT EDIT THE FOLLOWING LINES**

```
task.use.other.threads.queue.limit =
http =
audit.relative.url =
upload.relative.url=
addasset.relative.url=
call.home.relative.url=
oms.relative.url=
call.home.command.parameters=
match.on.assettag =
match.on.computername.if.valid.serial.or.uuid.stored =
```

**THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:**

```
queue.processors =
```

Modifiable Field	queue.processors
Field Description	Number of processors (CPUs) in the system that is running the Big-Fix® Remote Control Server Used to determine the number of working threads that can be used by the BigFix® Remote Control Server program.
Possible Values	User-defined
Value Definition	User-defined integer

**DO NOT EDIT THE FOLLOWING LINES**

```
queue.max.length =
serialised.queue.object=
row.sample =
character.width =
max.column.character.width =
min.table.character.width =
```

**YOU CAN EDIT THE FOLLOWING FIELD:**

```
use.scrollable.table
```

Modifiable Field	<b>use.scrollable.table</b>
Field Description	Determine whether you can scroll the results table.
Possible Values	True or False.
Value Definition	<p><b>True</b></p> <p>You can scroll the table.</p> <p><b>False</b></p> <p>You cannot scroll the results table.</p>

#### DO NOT EDIT THE FOLLOWING LINES

```
max.retries=
default.query=
default.pagerows=
query.authorised.queries=
all.users.query=
all.other.users.query=
all.groups.query=
selected.user.query=
selected.users.query=
selected.asset.query=
user.search.query=
asset.search.query=
selected.email.query=
scheduled.task.query=
task.list.query=
all.tasks=
report.list.query=
menu.links.query=
menu.actions.query=
menu.tasks.query=
menu.static.links.query=
menuscheduled.task.log.query=
attachments.query=
query.latest.unprocessed.revision=
query.all.unprocessed.revisions=
query.asset.count=
query.processed.incorrectly=
query.selected.task=
```

```
query.all.xml.revisions=  
query.users.assets=  
query.user.queries=  
query.asset.queries=  
query.unknown.pc.serial=  
query.uploads.in.period.defined=  
query.average.upload.time=  
query.unprocessed.security.assets=  
query.new.assets.in.period.defined=  
query.average.process.time=  
query.processed.in.period.defined=  
query.selected.user.custom.query=  
query.all.custom.query=  
query.selected.users.groups=  
query.unprocessable.pc.assets.count=  
query.menu.static.items=  
search.limit.results =  
max.keys =
```

## Category Description: Action Authority Settings

DO NOT EDIT THE FOLLOWING LINES

```
update.password.auth=  
update.details.auth=  
change.asset.owner.auth=  
add.user.auth=  
all.user.auth=  
all.asset.auth=  
all.custom.reports.auth=  
query.builder.auth=  
search.auth=  
task.auth=  
reprocess.auth=  
group.auth=  
view.group.auth=  
delete.user.auth=  
email.report.authority=  
edit.printer.auth=  
user.skill.auth=  
add.ticket.auth=  
edit.ticket.auth=  
setup.ticket.auth=
```


```

edit.table.auth=
edit.probeset.auth=
edit.po.auth=
rc.auth=
asset.revisions =
asset.keep.baseline=

```


THE FOLLOWING LINE CAN BE EDITED FOR YOUR ENVIRONMENT:

```
delete.target.auth=
```


Modifiable Field	<b>delete.target.auth</b>
Field Description	Determines what level of access is required to delete a target when you use the Delete Target action.
Possible Values	U, S, A
Value Definition	<p><b>U</b> User authority.</p> <p><b>S</b> Super User authority.</p> <p><b>A</b> Administrator authority. This value is the default value.</p> <p> <b>Note:</b> If you change the value of this property, you must restart the server service for the new value to take effect.</p>

```
browse.targets.auth=
```

Modifiable Field	<b>browse.targets.auth</b>
Field Description	Determines which levels of user authority see the <b>Browse</b> option that is displayed in the <b>Targets</b> menu.
Possible Values	U, S, A
Value Definition	<p><b>U</b> User authority. All user authorities see the <b>Browse</b> option in the <b>Targets</b> menu. This value is the default value.</p> <p><b>S</b></p>

	<p>Super User authority. Only Super Users and Admin users see the <b>Browse</b> option in the <b>Targets</b> menu.</p> <p><b>A</b></p> <p>Administrator authority. Only Admin users see the <b>Browse</b> option in the <b>Targets</b> menu.</p> <p> <b>Note:</b> If you change the value of this property, you must restart the server service for the new value to take effect.</p>
--	--

`view.all.targets.auth=`


Modifiable Field	<b>view.all.targets.auth</b>
Field Description	Determines which levels of user authority see the <b>All targets</b> option that is displayed in the <b>Targets</b> menu.
Possible Values	U, S, A
Value Definition	<p><b>U</b></p> <p>User authority. All user authorities see the <b>All targets</b> option in the <b>Targets</b> menu. This value is the default value.</p> <p><b>S</b></p> <p>Super User authority. Only Super Users and Admin users see the <b>All targets</b> option in the <b>Targets</b> menu.</p> <p><b>A</b></p> <p>Administrator authority. Only Admin users see the <b>All targets</b> option in the <b>Targets</b> menu.</p> <p> <b>Note:</b></p> <ol style="list-style-type: none"> <li>1. If you change the value of this property, you must restart the server service for the new value to take effect.</li> <li>2. If the home page of a user is set to the <b>All targets</b> report, the authority to view the report is determined by the value of <b>view.all.targets.auth</b>. If they do not have authority to view <b>All targets</b>, the <b>Search targets</b> page is displayed.</li> </ol>





3. If you set **view.all.targets.auth** to S or A, you must set **target.search.minimum.nonwildcards** to greater than 1. Otherwise, users with user authority can use the search targets page to display all of the targets.

```
search.session.history.auth=
```

Modifiable Field	<b>search.session.history.auth</b>
Field Description	Determines which levels of user authority sees the <b>Search</b> option that is displayed in the <b>Sessions</b> menu.
Possible Values	U, S, A
Value Definition	<p><b>U</b></p> <p>User authority. All user authorities see the <b>Search</b> option in the <b>Sessions</b> menu. This value is the default value.</p> <p><b>S</b></p> <p>Super User authority. Only Super Users and Admin users see the <b>Search</b> option in the <b>Sessions</b> menu.</p> <p><b>A</b></p> <p>Administrator authority. Only Admin users see the <b>Search</b> option in the <b>Sessions</b> menu.</p> <p> <b>Note:</b> If you change the value of this property, you must restart the server service for the new value to take effect.</p>

## Category Description: Schedules

DO NOT EDIT THE FOLLOWING LINES


```
scheduled.upload=
update.client.files=
scheduled.upload.interval=
scheduled.upload.queue.threshold=
scheduled.upload.queue.lookup.threshold=
scheduled.update.demographics=
```

```
scheduled.demographics.check.interval=
get.application.files.relative.url=
changed.software.upload =
changed.hardware.upload =
scheduled.launch.on.startup=
```

YOU CAN EDIT THE FOLLOWING LINES

### Category Description - LDAP synchronization task

```
scheduled.interval=
```

Modifiable Field	<b>scheduled.interval</b>
Field Description	The frequency in numeric value that the server must check for scheduled tasks.
Possible Values	User-Defined
Value Definition	User-Defined. Positive Integer   <b>Note:</b> If you change the value of this property, you must restart the server service for the new value to take effect.

```
scheduled.interval.period=
```

Modifiable Field	<b>scheduled.interval.period</b>
Field Description	The unit of time in which the server must check for scheduled tasks.
Possible Values	minutes or hours or days
Value Definition	Minutes or Hours or Days

```
scheduled.task.period=
```

Modifiable Field	<b>scheduled.task.period</b>
Field Description	The interval units to be used when scheduling tasks.
Possible Values	minutes or hours or days
Value Definition	Minutes or Hours or Days

DO NOT EDIT THE FOLLOWING LINES

```

scheduler.use.queue=
task.process.xml.max.queue.length=
task.process.files.max.queue.length=
task.process.filescan.max.queue.length=
task.process.software.security.length=

```

#### YOU CAN EDIT THE FOLLOWING LINES

**DBCleaner** is a looping utility that is used to clean up older log files that are based on age of entries (in days). Frequency is in days. To disable cleaning, set the value to **-1**.

```
dbcleaner.launch.on.startup=
```

Modifiable Field	<b>dbcleaner.launch.on.startup</b>
Field Description	Start <b>dbCleaner</b> when the server application starts.
Possible Values	1 or 0
Value Definition	1 to start <b>dbCleaner</b> . 0, do not start <b>dbCleaner</b> .

```
dbcleaner.frequency=
```

Modifiable Field	<b>dbcleaner.frequency</b>
Field Description	Frequency the <b>DBCleaner</b> runs at in days
Possible Values	Set to <b>-1</b> to disable cleaning
Value Definition	User-Defined - number of days

```
dbleaner.interval.period=
```

Modifiable Field	<b>dbleaner.interval.period</b>
Field Description	Period the database logs are cleaned
Possible Values	User-Defined. For example, <i>mins</i> , or <i>hours</i> , or <i>days</i> , or <i>months</i>
Value Definition	User-Defined - number of days

```
server.log.max.age=
```

Modifiable Field	<b>server.log.max.age</b>
Field Description	Maximum age of entries in the server log file before they are deleted.
Possible Values	User-Defined

Value Definition	User-Defined - number of days
------------------	-------------------------------

```
target.offline.max.age=
```

Modifiable Field	<b>target.offline.max.age</b>
Field Description	Number of days that an offline target (that is no longer calling home) is kept in the database.
Possible Values	User-Defined  When the value is set to 0, no offline target cleanup is performed.
Value Definition	User-Defined - number of days

DO NOT EDIT THE FOLLOWING LINE

```
tx.log.max.age=
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
task.log.max.age=
```

Modifiable Field	<b>task.log.max.age</b>
Field Description	Maximum age of entries in the task log table before they are deleted.
Possible Values	User-Defined
Value Definition	User-Defined - number of days

```
transfers.history.max.age=
```

Modifiable Field	<b>transfers.history.max.age</b>
Field Description	Maximum age of entries in the transfer table before they are deleted.
Possible Values	User-Defined
Value Definition	User-Defined - number of days

```
user.access.max.age=
```

Modifiable Field	<b>user.access.max.age</b>
Field Description	Maximum age of entries in the access table before they are deleted.
Possible Values	User-Defined

Value Definition	User-Defined - number of days
------------------	-------------------------------

DO NOT EDIT THE FOLLOWING LINES:

```
logon.disclaimer=
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

### Category Description: Password Settings

```
password.encrypt=
```

Modifiable Field	<b>password.encrypt</b>
Field Description	Determines whether passwords are encrypted in the database.
Possible Values	Yes or No
Value Definition	<p><b>Yes</b></p> <p>Passwords are encrypted in the database.</p> <p><b>No</b></p> <p>Passwords are not encrypted in the database.</p>

```
password.reuse=
```

Modifiable Field	<b>password.reuse</b>
Field Description	Determines whether users can reuse passwords.
Possible Values	Yes or No
Value Definition	<p><b>Yes</b></p> <p>Users can reuse passwords.</p> <p><b>No</b></p> <p>Users cannot reuse passwords.</p>

```
expire.new.password=
```

Modifiable Field	<b>expire.new.password</b>
Field Description	Determines whether users are required to set their own password after they receive the computer-generated password.
Possible Values	True or False
Value Definition	<b>True</b>

	<p>Users must set their own password after they receive the computer-generated password.</p> <p><b>False</b></p> <p>Users do not have to set their own password after they receive the computer-generated password.</p>
--	---

```
password.timeout=
```

Modifiable Field	<b>password.timeout</b>
Field Description	Determines whether passwords expire.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords expire.</p> <p><b>False</b></p> <p>Passwords do not expire.</p>

```
password.timeout.period=
```

Modifiable Field	<b>password.timeout.period</b>
Field Description	Defines after how many days passwords expire.
Possible Values	User-defined. The default value is 90.
Value Definition	User-defined integer

```
password.period=
```

Modifiable Field	<b>password.period</b>
Field Description	Maximum number of days before a password can be reused.
Possible Values	User-defined
Value Definition	User-defined integer

```
password.check=
```

Modifiable Field	<b>password.check</b>
Field Description	Determines whether to enable password rule checking.
Possible Values	True or False

Value Definition	<p><b>True</b></p> <p>Passwords must follow certain rules. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not follow rules.</p>
------------------	---

```
password.must.have.non.numeric=
```

Modifiable Field	<b>password.must.have.non.numeric</b>
Field Description	Determines whether passwords must contain non-numeric characters.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must contain non-numeric characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not need to contain non-numeric characters.</p>

```
password.must.have.numeric=
```

Modifiable Field	<b>password.must.have.numeric</b>
Field Description	Determines whether passwords must contain numeric characters.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must contain numeric characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not have to contain numeric characters.</p>

```
password.must.have.non.alphanumeric=
```

Modifiable Field	<b>password.must.have.non.alphanumeric</b>
Field Description	Determines whether passwords must contain non-alphanumeric characters.

Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must contain non-alphanumeric characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not have to contain non-alphanumeric characters.</p>

```
password.min.length=
```

Modifiable Field	<b>password.min.length</b>
Field Description	Minimum length of a password.
Possible Values	User-defined. Default value is eight.
Value Definition	User-defined integer

```
password.max.length=
```

Modifiable Field	<b>password.max.length</b>
Field Description	Maximum length of a password.
Possible Values	User-defined. Default value is fifteen.
Value Definition	User-defined integer

```
password.requires.mixedcase=
```

Modifiable Field	<b>password.requires.mixedcase</b>
Field Description	The password must contain both lowercase and uppercase characters.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Passwords must contain both lowercase and uppercase characters. This value is the default value.</p> <p><b>False</b></p> <p>Passwords do not need to contain both lowercase and uppercase characters.</p>



```
password.max.sequence=
```

Modifiable Field	<b>password.max.sequence</b>
Field Description	Maximum length of a sequence of characters. For example, 1234.
Possible Values	User-defined. Default value is three.
Value Definition	User-defined integer

```
password.max.matching.sequential.chars=
```

Modifiable Field	<b>password.max.matching.sequential.chars</b>
Field Description	Maximum number of repeating characters. For example, 111 aaa.
Possible Values	User-defined. Default value is two.
Value Definition	User-defined integer

```
password.max.previous.chars=
```

Modifiable Field	<b>password.max.previous.chars</b>
Field Description	Maximum number of sequential password characters that can be reused in a new password.
Possible Values	User-defined. Default value is three.
Value Definition	User-defined integer

```
password.iterationcount =
```

Modifiable field	<b>password.iterationcount</b>
Field Description	Use to define the number of times that a password is hashed before it is stored in the database.
Possible Values	User defined.
Value Definition	Default is 5000. The property has no maximum value. The higher the iteration count, the longer it takes for someone to try to break the password. However, the larger the iteration count, the slower it is to log on to the server or to change your password. A higher iteration count slows the system down. Therefore you must set it to a value that is acceptable to your environment and maintains acceptable performance.

DO NOT EDIT THE FOLLOWING LINE

```
table.column.internationalisation =
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
csv.export.use.byte.order.mark=
```

Modifiable Field	<b>csv.export.use.byte.order.mark</b>
Field Description	Determines whether a Unicode UTF-8 Byte Order Mark (BOM) is included at the start of the file when you export a CSV file.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Include a Unicode UTF-8 Byte Order Mark (BOM).</p> <p><b>False</b></p> <p>Do not include a Unicode UTF-8 Byte Order Mark (BOM).</p>

```
tsv.export.use.byte.order.mark=
```

Modifiable Field	<b>tsv.export.use.byte.order.mark</b>
Field Description	Determines whether a Unicode UTF-8 Byte Order Mark (BOM) is included at the start of the file when you export a TSV file.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Include a Unicode UTF-8 Byte Order Mark (BOM).</p> <p><b>False</b></p> <p>Do not include a Unicode UTF-8 Byte Order Mark (BOM).</p>

```
edit.properties.show.file.comments =
```

Modifiable Field	<b>edit.properties.show.file.comments</b>
Field Description	Determines whether you see the comments in the properties file when you edit the properties in the server UI.
Possible Values	1 / 0
Value Definition	<b>1</b>

	<p>The comments are displayed when you edit the properties.</p> <p><b>0</b></p> <p>The comments are not displayed when you edit the properties.</p>
--	---

```
edit.properties.show.translated.comments=
```

Modifiable Field	<b>edit.properties.show.translated.comments</b>
Field Description	Determines whether you see the available globalized comments in the properties file when you edit the properties in the server UI.
Possible Values	1 / 0
Value Definition	<p><b>1</b></p> <p>The comments are displayed when you edit the properties.</p> <p><b>0</b></p> <p>The comments are not displayed when you edit the properties.</p>

```
date.time.format=
```

Modifiable Field	<b>date.time.format</b>
Field Description	Defines the way dates and times are input into any date/time fields
Possible Values	User-defined
Value Definition	User-defined. For example, <code>EEEE, dd MMMM yyyy, HH:mm:ss</code>

```
date.only.format =
```

Modifiable Field	<b>date.only.format</b>
Field Description	Defines the way dates are input into any date only fields
Possible Values	User-defined
Value Definition	User-defined. For example, <code>EEEE, dd MMMM yyyy</code>

```
time.only.format =
```

Modifiable Field	<b>time.only.format</b>
------------------	-------------------------

Field Description	Defines the way dates are input into any date only fields
Possible Values	User-defined
Value Definition	User-defined. For example, HH:mm:ss

```
invalid.macs =
```

Modifiable Field	<b>invalid.macs</b>
Field Description	List of target Mac addresses that are unacceptable to send to the server in the target information.
Possible Values	User Defined for example - 000000000001
Value Definition	

```
invalid.assettags =
```

Modifiable Field	<b>invalid.assettags</b>
Field Description	List of target <b>assettags</b> that are unacceptable to send to the server in the target information.
Possible Values	User Defined for example, unknown
Value Definition	

```
invalid.net.addresses =
```

Modifiable Field	<b>invalid.net.addresses</b>
Field Description	List of target network addresses that are unacceptable to send to the server in the target information.
Possible Values	User Defined for example -0.0.0.0,127.0.0.0/8
Value Definition	

```
report.timeout.frequency =
```

Modifiable Field	<b>report.timeout.frequency</b>
Field Description	When a report is generated its output is cached, so that it can be re-loaded without the application going back to the database for the data. The property <b>report.timeout.frequency</b> defines the time value that the report output is cached for.
Possible Values	User Defined

Value Definition	
------------------	--

```
report.manager.frequency =
```

Modifiable Field	<b>report.manager.frequency</b>
Field Description	This property defines the time value for how often the Report manager loops and re loads the report data from the database
Possible Values	User Defined
Value Definition	

```
report.manager.period =
```

Modifiable Field	report.manager.period
Field Description	Defines the time period that is used for <b>report.timeout.frequency</b> and <b>report.manager.frequency</b> .
Possible Values	User Defined. For example seconds, minutes, hours. Default is minutes
Value Definition	

```
allow.target.group.override =
```

Modifiable Field	<b>allow.target.group.override</b>
Field Description	Determines the group that a target is made a member of during a silent target installation when the <b>GROUP_LABEL</b> parameter is used.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The target is assigned to the target group that the <b>GROUP_LABEL</b> parameter defines.</p> <p><b>False</b></p> <p>The target is assigned to the default target group that is defined for the <b>default.group.name</b> property.</p> <p>The <b>GROUP_LABEL</b> parameter is ignored.</p>

```
allow.override.at.triggered.callhomes =
```

Modifiable Field	<b>allow.override.at.triggered.callhomes</b>
------------------	--

Field Description	Determines the group that a target is made a member during triggered target callhomes when the <b>GROUP_LABEL</b> parameter is used.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The target is assigned to the target group that the <b>GROUP_LABEL</b> parameter defines.</p> <p><b>False</b></p> <p>The <b>GROUP_LABEL</b> parameter is ignored.</p>

```
default.group.name =
```

Modifiable Field	<b>default.group.name</b>
Field Description	Defines the name that is given to the default group of users
Field Description	Defines the name that is given to the default group of targets
Possible Values	User Defined. For example, DefaultGroup
Value Definition	

### Category Description: Default Non-Binary policies values

```
default.rc_def_inactivity =
```

Modifiable Field	<b>default.rc_def_inactivity</b>
Field Description	Number of seconds to wait before the remote control session connection ends automatically after no session activity.
Possible Values	User Defined - seconds
Value Definition	<ul style="list-style-type: none"> <li>• 0 - disables the timer and the session does not time out.</li> <li>• Less than 60 - session times out after 60 seconds.</li> <li>• Greater than 60 - session times out when the value is reached.</li> </ul>

```
default.rc_def_grace_time =
```

Modifiable Field	<b>default.rc_def_grace_time</b>
------------------	----------------------------------

Field Description	Sets the number of seconds to wait for the target user to respond before a session starts or times out, used with <b>Enable user acceptance for incoming connections</b> .
Possible Values	User-defined - 0 - 60 seconds
Value Definition	If set to 0, the session starts without displaying the user acceptance window on the target. Default is 5

```
default.rc_def_timeout_op =
```

Modifiable Field	<b>default.rc_def_timeout_op</b>
Field Description	Determines what action is taken if the user acceptance window timeout lapses. That is, the target user does not click accept or refuse within the number of seconds defined for <b>Acceptance Grace time</b>
Possible Values	ABORT or PROCEED
Value Definition	<p><b>Abort</b></p> <p>Session is not started. Default is Abort.</p> <p><b>Proceed</b></p> <p>Session is started.</p>

#### DO NOT EDIT THE FOLLOWING LINES

```
default.rc_def_local_audit
default.rc_def_pre_script =
default.rc_def_post_script=
```

#### YOU CAN EDIT THE FOLLOWING LINES

```
default.rc_def_script_op =
```

Modifiable Field	<b>default.rc_def_script_op</b>
Field Description	Determines what action is taken if the prescript execution fails. A positive value or 0 is considered as a successful run of the pre-session script. A negative value, script that is not found, or not finished running within 3 minutes is considered a failure.
Possible Values	ABORT or PROCEED
Value Definition	<b>Abort</b>

	<p>If the prescript run is a fail, the session does not start.</p> <p><b>Proceed</b></p> <p>If the prescript run is a fail, the session continues.</p>
--	--

```
default.rc_def_insession_ft =
```

Modifiable Field	<b>default.rc_def_insession_ft</b>
Field Description	Controls the transfer of files during an <b>Active</b> session. Its value determines the availability of the <b>Send file</b> or <b>Pull file</b> options in the <b>File Transfer menu</b> within the controller window.
Possible Values	NONE, BOTH, SEND, PULL
Value Definition	<p><b>Set to NONE</b></p> <p>The <b>Send file</b> and <b>Pull file</b> options are not available for selection. No file transfers can be initiated.</p> <p><b>Set to BOTH</b></p> <p>The <b>Send file</b> and <b>Pull file</b> options are available for selection. Files can be transferred to the target and transferred from the target. BOTH is the default value.</p> <p><b>Set to PULL</b></p> <p>Only the <b>Pull file</b> option is available for selection. Files can be transferred only from the target.</p> <p><b>Set to SEND</b></p> <p>Only the <b>Send file</b> option is available for selection. Files can be transferred only to the target.</p>



#### DO NOT EDIT THE FOLLOWING LINES

```
default.rc_def_ft_actions =
default.rc_def_allowed_times
new.password.template
access.request.request.template
access.request.request.anon.template
access.request.reject.template
access.request.reject.anon.template
access.request.grant.template
access.request.grant.anon.template
```



## YOU CAN EDIT THE FOLLOWING LINES

```
trc.feature.remote.install =
```

Modifiable Field	<b>trc.feature.remote.install</b>
Field Description	<p>Determines the availability of the remote installation function.</p> <p> <b>Note:</b> The remote installation feature is deprecated in Remote Control V9.1.3. Therefore, during a server upgrade, if you select to keep existing properties, the value of this property is still set to <b>False</b> by default.</p>
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The Remote Install function is available in the <b>Admin</b> menu.</p> <p><b>False</b></p> <p>The Remote Install function is not available in the <b>Admin</b> menu. This value is the default value.</p> <p> <b>Note:</b> If you change the value of this property, you must restart the server service.</p>

```
trc.feature.denied.program.execution.list =
```

Modifiable Field	<b>trc.feature.denied.program.execution.list</b>
Field Description	Determines the availability of the Denied Program Execution policy when you create groups or permissions links.
Possible Values	True / False
Value Definition	<p><b>True</b></p> <p>The <b>Denied program execution list</b> policy is displayed on the <b>Edit group</b> screen and the <b>Manage Permissions</b> screen.</p> <p><b>False</b></p> <p>The <b>Denied program execution list</b> policy is not displayed on the <b>Edit group</b> screen and the <b>Manage Permissions</b> screen.</p>



**Note:** This feature works only on the following operating systems

- Windows™ XP (32-bit editions only)
- Windows™ Server 2003 (32-bit editions only)



**Note:** If you set this property back to true, after it is set to false, you must restart the server service.

```
trc.ticket.allow.access =
```

Modifiable Field	<b>trc.ticket.allow.access</b>
Field Description	Determines the availability of the <b>Request Access</b> function.
Possible Values	1 or 0
Value Definition	<p><b>1</b></p> <p>The <b>Request Access</b> option is displayed on the start session screen. This option allows the controller user to temporarily access a target that they do not have permission to access.</p> <p><b>0</b></p> <p>The <b>Request Access</b> option is not displayed on the start session screen and the <b>Request Access</b> menu item is disabled.</p>

```
trc.ticket.allow.allaccess =
```

Modifiable Field	<b>trc.ticket.allow.allaccess</b>
Field Description	Determines the availability of the <b>Request Access</b> function when a user who is not registered in Remote Control tries to access by using the anonymous URL. For more information about the anonymous URL and how to request access to targets when you are not a registered user in the BigFix® Remote Control Server, see the <i>BigFix® Remote Control Controller User's Guide</i> .
Possible Values	1 or 0
Value Definition	<b>1</b>

The Request Access to target screen is displayed when the user types in the anonymous URL.


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

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

**0**

The logon screen is displayed when the user types in the anonymous URL.

```
trc.ticket.admin =
```

Modifiable Field	<b>trc.ticket.admin</b>
Field Description	Defines the user group of administrators who receive an email when an access request is submitted.
Possible Values	User defined. For example, <i>Adminemail</i> .   <b>Note:</b> <ol style="list-style-type: none"> <li>1. The group name must be a valid user group that is already defined in the server.</li> <li>2. If this field is left blank, the email address that is set for the property <b>email.admin</b> receives an email when an access request is submitted.</li> </ol>
Value Definition	The group name must be already defined in the database.

```
trc.ticket.groupprefix =
```

Modifiable Field	<b>trc.ticket.groupprefix</b>
Field Description	Defines the prefix that is assigned to the name of the temporary user and target groups that are created when an access request is granted.
Possible Values	User-defined. For example, t\$t
Value Definition	The temporary groups names are in the format  P_R_G  Where

	<ul style="list-style-type: none"> <li>• P = trc.ticket.groupprefix property</li> <li>• R = the request key value for the access request</li> <li>• G = the group type U for user group, T for target group.</li> </ul> <p>for example : t\$t_5_U</p>
--	---

```
trc.ticket.priority =
```

Modifiable Field	<b>trc.ticket.priority</b>
Field Description	Defines the default priority level for access request permissions.
Possible Values	0, 1, or 5
Value Definition	<p>The priority value that is used when you set permissions for an access request. The value overrides any other permission values.</p> <p>For example: 5 is the highest priority. 5 overrides 1 and 1 overrides 0.</p>

```
trc.default.request.priority =
```

Modifiable Field	<b>trc.default.request.priority</b>
Field Description	Defines the priority value that is displayed first in the priority list when you set the permissions for an access request.
Possible Values	0, 1, 5
Value Definition	<p><b>0</b></p> <p>0 is displayed first in the list.</p> <p><b>1</b></p> <p>1 is displayed first in the list.</p> <p><b>5</b></p> <p>5 is displayed first in the list.</p>

DO NOT EDIT THE FOLLOWING LINES

```
trc.ticket.temp.usergrpupdesc
trc.ticket.temp.targetgrpupdesc
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
task.logdistribution.enabled =
```

Modifiable Field	<b>task.logdistribution.enabled</b>
Field Description	Determines whether the logs that contain session information are written to the BigFix® Remote Control Server.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The logs are written to the server to the location defined by <code>task.logdistribution.path</code>.</p> <p><b>False</b></p> <p>The logs are not written to the server.</p>

```
task.logdistribution.path =
```

Modifiable Field	<b>task.logdistribution.path</b>
Field Description	Determines the location that the log file that contains session information is written to on the server.
Possible Values	User defined. For example, <code>c:\logtask\logs</code>
Value Definition	

DO NOT EDIT THE FOLLOWING LINE

```
task.logdistribution.file
```

YOU CAN EDIT THE FOLLOWING LINES

```
registry.title.X =
```

Modifiable Field	<b>registry.title.X</b>
Field Description	Defines the name of the menu item that is displayed in the registry keys menu. Use the menu to view the value for the specific registry key that is defined by <code>registry.key.X</code>
Possible Values	User defined. For example, Services.
Value Definition	<code>X = 0 - 9.</code>

```
registry.key.X =
```

Modifiable Field	<b>registry.key.X</b>
Field Description	Defines the path to a specific registry key that you can use to view its value on the target.
Possible Values	User defined. For example, <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services</code>
Value Definition	X = 0 - 9.

```
nat.ip.support =
```

Modifiable Field	<b>nat.ip.support</b>
Field Description	Used to define the list of IP addresses that are used by the server when a connection is made to a target when NAT addresses are present.
Possible Values	0, 1, 2, 3, 4
Value Definition	<p><b>0</b></p> <p>IP=heartbeatlist.</p> <p>Server uses the heartbeat list of IP addresses to make a connection with the target.</p> <p><b>1</b></p> <p><i>IP= heartbeatlist; source</i></p> <p>Server uses the <b>heartbeatlist</b> list of IP addresses then the source IP address to make a connection with the target.</p> <p><b>2</b></p> <p><i>IP = source;heartbeatlist</i></p> <p>Server uses the source IP address then the <b>heartbeatlist</b> of IP addresses to make a connection with the target.</p> <p><b>3</b></p> <p><i>IP = heartbeat;source</i></p> <p>Server checks the IP addresses that are listed in the <b>nat.exclude.list</b> property to see whether the source IP is there. If it is not, the server uses the <b>heartbeatlist</b> of</p>

	<p>IP addresses and then source IP address to make a connection with the target.</p> <p><b>4</b></p> <p><i>IP = source;heartbeat</i></p> <p>Server checks the IP addresses listed in the <b>nat.exclude.list</b> property to see whether the source IP is there. If it is not, the server uses the source IP and then the <b>heartbeatlist</b> of IP addresses to make a connection with the target.</p>
--	--

```
nat.exclude.list =
```

Modifiable Field	<b>nat.exclude.list</b>
Field Description	Defines a list of NAT addresses that are ignored by the server.
Possible Values	User defined.
Value Definition	

```
match.allow.data.changes =
```

Modifiable Field	<b>match.allow.data.changes</b>
Field Description	Is used to find a match for a target in the database if a perfect match cannot be found. For more information about how targets are registered, see <a href="#">Ensure targets are registered correctly (on page 186)</a> .
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>This value is the default value. When set to true, a best match is considered if all but 1 of the 4 perfect match criteria match an already registered target.</p> <p><b>False</b></p> <p>If the perfect match process is enabled and no match is found for all 4 of the target criteria, the best match option is not considered. Depending on the value of <b>match.change.notifications</b>, if no match is found then a new target entry is created in the database.</p>

```
match.computername.only =
```

Modifiable Field	<b>match.computername.only</b>
Field Description	Determines whether a targets computer name is used to see whether it is already registered with the BigFix® Remote Control Server. When a target contacts the server, its computer name is compared to the computer names of the targets that are already registered with the server. If a match is found, the details of the matched target are updated. If no match is found, a new target entry is created. For more information about how targets are registered, see <a href="#">Ensure targets are registered correctly (on page 186)</a> .
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>When a target contacts the server, the targets computer name is checked against the computer names of already registered targets. If a match is found, the details of the matched target are updated with the details of the target that is contacting the server. If no match is found, a new target entry is created.</p> <p><b>False</b></p> <p>When a target contacts the server, the targets computer name is not used to see whether the target is already registered with the server.</p>

```
match.guid.only =
```

Modifiable Field	<b>match.guid.only</b>
Field Description	Determines whether a targets <i>guid</i> is used to see whether it is already registered with the BigFix® Remote Control Server. When a target contacts the server, its <i>guid</i> is compared to the <i>guid</i> values of the targets that are already registered with the server. If a match is found, the details of the matched target are updated. If no match is found, a new target entry is created. For more information about how targets are registered, see <a href="#">Ensure targets are registered correctly (on page 186)</a> .
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>When a target contacts the server, the targets <i>guid</i> is checked against the <i>guid</i> values of already registered targets. If a match is found, the details of the matched</p>



	<p>target are updated with the details of the target that is contacting the server. If no match is found, a new target entry is created.</p> <p><b>False</b></p> <p>When a target contacts the server, the targets <i>guid</i> is not used to see whether the target is already registered with the server.</p>
--	---

`match.change.notification =`

Modifiable Field	<b>match.change.notification</b>
Field Description	Use this property to force a target to save its configuration details locally. If any of the target details change, it can send the old details and its current details to the server. The details can be used to try to find a match in the database. For more information about how targets are registered, see <a href="#">Ensure targets are registered correctly (on page 186)</a> .
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>This value is the default value. The target saves its details locally to a file called <code>tgt_info.properties</code>. When the target contacts the server, it sends its old details and its new details. The old details are used to try to find a perfect match for the target in the database.</p> <p><b>False</b></p> <p>The old target details are not sent to the server and the new changed details are used to try to find a match. However if only one of the 4 criteria changes and the <b>match.allow.data.changes</b> property is set to true, then a best match is looked for.</p>

`rc.tmr.at.registration =`

Modifiable Field	<b>rc.tmr.at.registration</b>
Field Description	Determines whether a target is assigned to target groups by using rules the first time it registers with the BigFix® Remote Control Server
Possible Values	True or False

Value Definition	<p><b>True</b></p> <p>When a target contacts the server for the first time, its computer name and IP address is compared to the computer names and IP addresses that are defined in the target membership rules. If a match is found, the target is assigned to the target groups that are defined in the matching rules.</p> <p><b>False</b></p> <p>When a target contacts the server for the first time, the targets computer name and IP address are not checked against any defined rules.</p>
------------------	--

```
rc.tmr.at.every.callhome =
```

Modifiable Field	<b>rc.tmr.at.every.callhome</b>
Field Description	Determines whether a target is assigned to target groups by using rules every time it contacts the BigFix® Remote Control Server
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Every time that a target contacts the server its computer name and IP address are compared to the computer names and IP addresses that are defined in the target membership rules. If a match is found, the target is assigned to the target groups that are defined in the matching rules. Therefore, the targets group membership is recalculated every time that it contacts the server.</p> <p><b>False</b></p> <p>Every time that a target contacts the server its computer name and IP address are not checked against any defined rules.</p>

```
rc.tmr.at.triggered.callhomes =
```

Modifiable Field	<b>rc.tmr.at.triggered.callhomes</b>
Field Description	Determines whether a target is assigned to target groups by using rules any time it contacts the BigFix® Remote Control Server because of a change to its configuration or when it comes online.

Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>When a target contacts the server because of a configuration change or when it comes online, its computer name and IP address are compared to the computer names and IP addresses that are defined in the target membership rules. If a match is found, the target is assigned to the target groups that are defined in the matching rules.</p> <p><b>False</b></p> <p>Any time a target contacts the server because of a configuration change or when it comes online, its computer name and IP address is not checked against any defined rules.</p>

```
rc.tmr.at.rules.change =
```

Modifiable Field	<b>rc.tmr.at.rules.change</b>
Field Description	When a rule is added, edited, or deleted. Determines whether the target group membership is altered for targets that were assigned to target groups by using rules.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Applies to targets whose group membership was assigned by using rules. Their group membership is recalculated whenever a rule is added, edited, or deleted.</p> <p><b>False</b></p> <p>Applies to targets whose group membership was assigned by using rules. Their group membership is not recalculated whenever a rule is added, edited, or deleted.</p>

DO NOT EDIT THE FOLLOWING LINES


```
hb.timeout.lookup.mode
hb.timeout.att.defn
```

THE FOLLOWING LINE CAN BE EDITED FOR YOUR ENVIRONMENT:

```
oracle.increment.keys.off =
```

Modifiable Field	<b>oracle.increment.keys.off</b>
Field Description	Used as a workaround for a driver bug in the Oracle JDBC versions 5 & 6 drivers that are included with Oracle 11g
Possible Values	1 or 0
Value Definition	<p><b>1</b></p> <p>Set to 1 if you are using the Oracle JDBC versions 5 &amp; 6 drivers.</p> <p><b>0</b></p> <p>Set to 0 if you are using JDBC 4 drivers (Oracle 10i) or if future versions of the JDBC driver address the get autogenerated keys bug.</p>

```
default.homepage.method=
```


Modifiable Field	<b>default.homepage.method</b>
Field Description	Used to determine whether the default home page is a report, or the search targets page. This property is useful if you have numerous targets in the Remote Control database. The default home page that is set by the server is the <b>All targets</b> report. The report can take some time to load if you have numerous targets. Then you must scroll through the report to find the relevant target. If you set the search page as the home page, you can search for specific targets as soon as you log on.
Possible Values	report or search
Value Definition	<p><b>report</b></p> <p>The default home page is set to the report that is defined by the query in the <b>default.query</b> property. By default it is the <b>All targets</b> report.</p> <p><b>search</b></p> <p>The default home page is set to the <b>search targets</b> page.</p> <p> <b>Note:</b> This property is overridden if a home page is already defined. For example,</p>



- The user defines their own home page.
- A home page is defined for the user groups that the user belongs to.

For more information about setting a home page, see [Manage the home page for a user or group \(on page 157\)](#).

```
workaround.rdp.console.w2k3 =
```

Modifiable Field	<b>workaround.rdp.console.w2k3</b>
Field Description	Used as a workaround for a Windows™ 2003 limitation. A remote control session cannot capture the display if a remote desktop session has taken place or is taking place on the target.
Possible Values	0, 1 or 2
Value Definition	<p>When a Remote Desktop user uses the <b>/admin</b> or <b>/console</b> option to start a Remote Desktop session with a Windows™ Server 2003 system and an Remote Control user starts a remote control session before, during or after the Remote Desktop session, remote control is unable to capture the display. The result is that a gray screen is displayed in the controller. This issue is a limitation in Windows™ Server 2003. Therefore, this property provides a workaround that will reset the Windows™ session either after each Remote Desktop session ends, or before an Remote Control session starts, depending on the value selected.</p> <p><b>0</b></p> <p>The workaround is disabled. This value is the default value.</p> <p><b>1</b></p> <p>Reset the session automatically when a remote control session is started.</p> <p> <b>Note:</b> The Windows™ sessions take a couple of minutes to initialize and a blank desktop is displayed on the controller until the initialization is complete. A message is displayed to inform the controller user that the session is being reset and it might take a few minutes.</p>

**2**

Reset the session automatically when the Remote Desktop user logs out.




**Note:**

1. The value set for this property applies to all targets that are registered with the server. You can set an attribute for a target group to limit the action to selected targets. For more information about the attribute, see [Creating target groups \(on page 71\)](#). If the server property has a different value to the target group attribute, the target group value takes precedence for those targets who are members of the specific target group.
2. If a Remote Desktop session (admin or console) is in progress when the controller attempts to connect to a target, a message is displayed to the controller. The message provides details of the Remote Desktop user and the IP address and computer name that the session is running from.

```
follow.active.session
```

```
=
```

<b>Modifiable Field</b>	<b>follow.active.session</b>
<b>Field Description</b>	<p>If set to Yes, the controller connects to the active session in the target, even if this session is a Remote Desktop session. This feature is available in Remote Control v9.1.2 IF0002 and later versions and is supported on the following Microsoft™ Windows™ operating system versions:</p> <ul style="list-style-type: none"> <li>• Microsoft™ Windows™ Vista</li> <li>• Microsoft™ Windows™ 7</li> <li>• Microsoft™ Windows™ 8</li> <li>• Microsoft™ Windows™ 8.1</li> <li>• Microsoft™ Windows™ 10</li> </ul>

	This feature is not supported on any server edition of Microsoft™ Windows™.
Possible Values	Yes, No
Value Definition	<p><b>Yes</b></p> <p>Support for Remote Desktop sessions is enabled.</p> <p>The BigFix® Remote Control controller connects to the active session in the target, even if the active session is a Remote Desktop session.</p> <p><b>No</b></p> <p>No change in configuration and the controller connects only to the physical console in the target, even if there is an active Remote Desktop session.</p> <p> <b>Note:</b></p> <p>The value set for this property applies to all targets that are registered with the server. You can set an attribute for a target group to limit the action to selected targets. For more information about the attribute, see <a href="#">Creating target groups (on page 71)</a>. If the server property has a different value to the target group attribute, the target group value takes precedence for those targets who are members of the specific target group.</p>

`target.search.minimum.nonwildcards =`

Modifiable Field	<b>target.search.minimum.nonwildcards</b>
Field Description	Sets the minimum number of non-wildcard characters that are allowed to be entered when you search for a target.
Possible Values	User-defined integer, default is 0.
Value Definition	Determines the minimum non-wildcard characters that must be entered in the search targets field on the search targets page. For example set to 2 means that at least 2 non-wildcard characters must be entered. For example, <code>se</code> or <code>te</code> . If you enter less than the minimum characters, the following error is displayed on the screen - The search

string must contain at least  $X$  non-wildcard characters.  $X$  is the value set in the property.



**Note:** If you set **view.all.targets.auth** to `S` or `A`, you must set **target.search.minimum.nonwildcards** to greater than 1. The reason is to prevent users who have user authority from using the search targets page to display all targets.

```
target.search.maximum.wildcards =
```

Modifiable Field	<b>target.search.maximum.wildcards</b>
Field Description	Sets the maximum number of wildcard characters that are allowed to be entered when you search for a target. The wildcard characters that are allowed are *, %, * and _.
Possible Values	User-defined integer, default is 0.
Value Definition	The value set determines the maximum number of wildcard characters that you can enter in the search targets field, on the search targets page. For example, set to 1 means that only 1 wildcard character can be entered. For example, <code>se*</code> or <code>te*</code> . If you enter more than the maximum characters the following error is displayed on the screen - The number of wildcards in the search string cannot exceed $X$ . $X$ is the value set in the property.

**To reduce the volume of unnecessary heartbeats, the following properties can be configured.**

```
heartbeat.retry =
```

Modifiable Field	<b>heartbeat.retry</b>
Field Description	If a target cannot contact the BigFix® Remote Control Server, use this property to define the number of minutes that the target waits before it tries to contact the server again.
Possible Values	User-defined, minutes
Value Definition	Default is 10.

```
heartbeat.delay=
```



Modifiable Field	<b>heartbeat.delay</b>
Field Description	The maximum delay in minutes that a target waits between sending heartbeats to the BigFix® Remote Control Server.
Possible Values	User-defined: minutes
Value Definition	Default is 20 minutes. Prevent multiple heartbeats in quick succession by delaying the actual heartbeat when a heartbeat is triggered.

```
heartbeat.on.wake =
```

Modifiable Field	<b>heartbeat.on.wake</b>
Field Description	Trigger a heartbeat when the target system wakes from standby or hibernation.
Possible Values	1 or 0
Value Definition	<p><b>1</b></p> <p>Trigger a heartbeat when the target system wakes from standby or hibernation.</p> <p><b>0</b></p> <p>Do not trigger a heartbeat when the target system wakes from standby or hibernation. This value is the default value.</p>


```
heartbeat.on.userchange =
```

Modifiable Field	<b>heartbeat.on.userchange</b>
Field Description	Trigger a heartbeat when a user logs on or off
Possible Values	1 or 0
Value Definition	<p><b>1</b></p> <p>Trigger a heartbeat when a user logs on or off. This value is the default value.</p> <p><b>0</b></p> <p>Do not trigger a heartbeat when a user logs on or off.</p>

```
heartbeat.on.change =
```

Modifiable Field	<b>heartbeat.on.change</b>
Field Description	Trigger a heartbeat when any of the values included in a heartbeat change.
Possible Values	1 or 0
Value Definition	<p><b>1</b></p> <p>Trigger a heartbeat when any of the values included in a heartbeat change. This value is the default value.</p> <p><b>0</b></p> <p>Do not trigger a heartbeat when any of the values included in a heartbeat change. This value is the default value.</p>

```
heartbeat.on.stop =
```

Modifiable Field	<b>heartbeat.on.stop</b>
Field Description	Trigger a heartbeat when the target is stopped or the system is shutting down
Possible Values	1 or 0
Value Definition	<p><b>1</b></p> <p>Trigger a heartbeat when the target is stopped or the system is shutting down.</p> <p><b>0</b></p> <p>Do not trigger a heartbeat when the target is stopped or the system is shutting down. This value is the default value.</p> <p> <b>Note: HeartBeatOnStop</b> set to 1 is not recommended unless <b>HeartBeatDelay</b> is set to 0. Otherwise, remote control sessions cannot be started while the heartbeat is being delayed.</p>

```
broker.code.length =
```

Modifiable Field	<b>broker.code.length</b>
------------------	---------------------------

Field Description	Determines the number of characters that are required to be entered for the connection code. Enter the connection code when you start a remote control session through an internet connection broker.
Possible Values	User-defined integer.
Value Definition	Default is 7. There is no limit to the number of characters that can be set. However, you must use your discretion when you set the value.

```
broker.code.timeout =
```

Modifiable Field	<b>broker.code.timeout</b>
Field Description	Determines the number of seconds the connection code timer counts down from before a new code is needed. The timer is displayed on the controller when you start a remote control session by using a broker.
Possible Values	User defined.
Value Definition	Default is 900.

```
broker.trusted.certs.required =
```

Modifiable Field	<b>broker.trusted.certs.required</b>
Field Description	Determines whether strict certificate validation is enabled.
Possible Values	true or false.
Value Definition	<p><b>true</b></p> <p>Strict certificate validation is enabled. This value is the default value.</p> <p><b>false</b></p> <p>Strict certificate validation is disabled.</p>

```
rc.recording.filename.format =
```

Modifiable Field	<b>rc.recording.filename.format</b>
Field Description	Specifies the file name format that is used in the server to store the recordings

Possible Values	User defined. Some formatting variables can be added to the file name to customize it
Value Definition	<p>For example, <code>trcrecording_%S_%D_%T.trc</code></p> <p>Where %S is placeholder for the session ID of the recording</p> <p>%D is placeholder for the date of the recording</p> <p>%T is placeholder for the time stamp of the recording</p> <p>%H is placeholder for the host name of the target</p>

```
rc.enforce.secure.registration =
```

Modifiable Field	<b>rc.enforce.secure.registration</b>
Field Description	Determines whether secure authentication is required when targets call home to the server.
Possible Values	<i>true</i> or <i>false</i>
Value Definition	<p><b>true</b></p> <p>Secure target registration is enabled. Secure tokens are used to authenticate a target when it contacts the server. This default value is <i>true</i>.</p> <p><b>false</b></p> <p>Secure target registration is disabled.</p> <p>For more information about secure tokens and how they are used, see <a href="#">Secure target registration (on page 40)</a>.</p>

## common.properties

```
index.title=
```

Modifiable Field	<b>index.title</b>
Field Description	Title of the Application
Possible Values	User defined. For example, Remote Control
Value Definition	

```
trcjws.use.target.hostname=
```

Modifiable Field	<b>trcjws.use.target.hostname</b>
Field Description	Used to allow the target hostname in addition or instead of the IP address in Managed Mode <code>.trcjws</code> file.
Possible Values	0, 1, 2
Value Definition	<ul style="list-style-type: none"> <li>• 0 (zero) - No hostame addition. (Default)</li> <li>• 1 - Add the hostname to the IP address</li> <li>• 2 - Hostname only</li> </ul>

**DO NOT EDIT THE FOLLOWING LINES**

```
product=
jndi.context=
```

**YOU CAN EDIT THE FOLLOWING LINES**

```
datasource.context=
```

Modifiable Field	<b>datasource.context</b>
Field Description	Defines the <b>jndi</b> name for the database.
Possible Values	User Defined. For example, <code>jdbc/trcdb</code> .
Value Definition	

```
fips.compliance=
```

Modifiable Field	<b>fips.compliance</b>
Field Description	Used as part of the process for enabling FIPS compliance on the server. For more information about enabling FIPS compliance, see the <i>BigFix® Remote Control Installation Guide</i> .
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>Used as part of the process for enabling FIPS compliance on the server. You must also follow the instructions in the <i>BigFix® Remote Control Installation Guide</i> for enabling FIPS compliance.</p> <p><b>False</b></p> <p>FIPS compliance is not enabled.</p>

```
sp800131a.compliance=
```

Modifiable Field	<b>sp800131a.compliance</b>
Field Description	Used as part of the process for enabling NIST SP800-131A compliance on the server. For more information about enabling NIST SP800-131A compliance, see the <i>BigFix® Remote Control Installation Guide</i> .
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>NIST SP800-131A compliance is enabled. Used as part of the process for enabling NIST SP800-131A compliance on the server. You must also follow the instructions in the <i>BigFix® Remote Control Installation Guide</i> for enabling NIST SP800-131A compliance.</p> <p><b>False</b></p> <p>NIST SP800-131A compliance is not enabled.</p>

```
https.strict.validation=
```

Modifiable Field	<b>https.strict.validation</b>
Field Description	To enable strict validation of HTTPS certificates by the controller component in a managed session.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The controller uses the system truststore to verify HTTPS connections to the server. The connection fails if the certificate is not trusted.</p> <p><b>False</b></p> <p>HTTPS connections are not verified.</p>

```
authentication.LDAP=
```

Modifiable Field	<b>authentication.LDAP</b>
Field Description	Determines whether LDAP authentication is used
Possible Values	True or False
Value Definition	<b>True</b>

	<p>LDAP authentication is used</p> <p><b>False</b></p> <p>LDAP authentication is not used</p>
--	---

```
authentication.LDAP.config=
```

Modifiable Field	<b>authentication.LDAP.config</b>
Field Description	Name of the properties file that contains the LDAP properties
Possible Values	User Defined for example - ldap.properties
Value Definition	

```
sync.LDAP=
```

Modifiable Field	<b>sync.LDAP</b>
Field Description	Use to enable the synchronization of the users and group from Active Directory with the Remote Control database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The LDAP server is synchronized with the Remote Control database to reflect any changes that are made in LDAP.</p> <p><b>False</b></p> <p>No synchronization takes place.</p>

```
sso.enabled=
```

Modifiable Field	<b>sso.enabled</b>
Field Description	Use this option as part of the configuration to enable SAML 2.0 Single Sign-on (SSO). For more information about configuring SSO, see <a href="#">Configure SAML 2.0 authentication on the server (on page 42)</a> . If you change the value of this property, you must restart the Remote Control server service.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>SSO is enabled. However, further configuration is also needed.</p>

**False**

SSO is disabled. This value is the default value.

**DO NOT EDIT THE FOLLOWING**

```

application.log.file
application.resources
default.properties.0=
default.properties.1=
default.properties.2=
default.properties.3=
generic.database.create=
generic.database.directory=
generic.database.populate=
db.scripts.use.new.line=

```

**THE FOLLOWING LINE CAN BE EDITED FOR YOUR ENVIRONMENT:**

```

properties.backup.archive=

```

Modifiable Field	<b>properties.backup.archive</b>
Field Description	Number of copies of the property backups to keep
Possible Values	User-defined Integer
Value Definition	

**DO NOT CHANGE THE FOLLOWING FIELDS**

```

common.schema
auto.increment.keys
automatically.adjust.database
user.table.1
user.table.2

```

**THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:**

```

users.title.required=

```

Modifiable Field	<b>users.title.required</b>
Field Description	Whether the <b>title</b> field is required to be completed on the screens where user information is submitted to the database.



Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>title</b> field must be completed.</p> <p><b>False</b></p> <p>The title is not required.</p>

```
users.forename.required=
```

Modifiable Field	<b>users.forename.required</b>
Field Description	Whether the <b>forename</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>forename</b> field must be completed.</p> <p><b>False</b></p> <p>The given name is not required.</p>

```
users.surname.required=
```

Modifiable Field	<b>users.surname.required</b>
Field Description	Whether the <b>surname</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>surname</b> field must be completed.</p> <p><b>False</b></p> <p>The surname is not required.</p>

```
users.country.required=
```

Modifiable Field	<b>users.country.required</b>
Field Description	Whether the <b>country</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<b>True</b>

	<p>The <b>country</b> field must be completed.</p> <p><b>False</b></p> <p>The country is not required.</p>
--	--

`users.userid.required=`

Modifiable Field	<b>users.userid.required</b>
Field Description	Whether the <b>userid</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>userid</b> field must be completed.</p> <p><b>False</b></p> <p>The user ID is not required.</p>

`users.address_1.required=`

Modifiable Field	<b>users.address_1.required</b>
Field Description	Whether the <b>address1</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>address1</b> field must be completed.</p> <p><b>False</b></p> <p>Information is not required in the <b>address1</b> field.</p>

`users.address_2.required=`

Modifiable Field	<b>users.address_2.required</b>
Field Description	Whether the <b>address2</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>address2</b> field must be completed.</p> <p><b>False</b></p>

Information is not required in the **address2** field.

```
users.email.required=
```

Modifiable Field	<b>users.email.required</b>
Field Description	Whether the <b>email</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>email</b> field must be completed.</p> <p><b>False</b></p> <p>The user's email address is not required.</p>

```
users.town.required=
```

Modifiable Field	<b>users.town.required</b>
Field Description	Whether the <b>town</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>town</b> field must be completed.</p> <p><b>False</b></p> <p>The town is not required.</p>

```
users.postcode.required=
```

Modifiable Field	<b>users.postcode.required</b>
Field Description	Whether the <b>postcode</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>postcode</b> field must be completed.</p> <p><b>False</b></p> <p>The postcode is not required.</p>

```
users.nickname.required=
```

Modifiable Field	<b>users.nickname.required</b>
Field Description	Whether the <b>nickname</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>nickname</b> field must be completed.</p> <p><b>False</b></p> <p>The nickname is not required.</p>

```
users.tel_no.required=
```

Modifiable Field	<b>users.tel_no.required</b>
Field Description	Whether the <b>tel_no</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>tel_no</b> field must be completed.</p> <p><b>False</b></p> <p>The telephone number is not required.</p>

```
users.mob_no.required=
```

Modifiable Field	<b>users.mob_no.required</b>
Field Description	Whether the <b>mob_no</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>mob_no</b> field must be completed.</p> <p><b>False</b></p> <p>The mobile number is not required.</p>

```
users.employeeid.required=
```

Modifiable Field	<b>users.employeeid.required</b>
Field Description	Whether the <b>employeeid</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>employeeid</b> field must be completed.</p> <p><b>False</b></p> <p>The employee ID is not required.</p>

```
users.department.required=
```

Modifiable Field	<b>users.department.required</b>
Field Description	Whether the <b>department</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>department</b> field must be completed.</p> <p><b>False</b></p> <p>The department is not required.</p>

```
users.location.required=
```

Modifiable Field	<b>users.location.required</b>
Field Description	Whether the <b>location</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>location</b> field must be completed.</p> <p><b>False</b></p> <p>The location is not required.</p>

```
users.password.required=
```

Modifiable Field	<b>users.password.required</b>
------------------	--------------------------------

Field Description	Whether the <b>password</b> field is required to be completed on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	<p><b>True</b></p> <p>The <b>password</b> field must be completed.</p> <p><b>False</b></p> <p>The password is not required.</p>


```
sync.LDAP.at_reset_application
```


Modifiable Field	<b>sync.LDAP.at_reset_application</b>
Field Description	Use to enable the synchronization when the reset application is performed.
Possible Values	True, False. Default is True.

```
sync.LDAP.task_run_days
```

Modifiable Field	<b>sync.LDAP.task_run_days</b>
Field Description	Use to enable a fixed time synchronization. The value indicates the frequency in days of the synchronization.
Possible Values	Number of days. Default is 0.
Value Definition	If the value is 0, fixed time synchronization is disabled and the synchronization occurs every scheduled.interval n - days in interval. 1 for daily.

```
sync.LDAP.task_run_time
```

Modifiable Field	<b>sync.LDAP.task_run_time</b>
Field Description	<p>Use to indicate the time of the day the a fixed time synchronization has to occur.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>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 ac-</li> </ul>

	 <p>tual execution time can span from sync.LDAP.task_run_time to sync.LDAP.task_run_time + scheduled.interval</p> <ul style="list-style-type: none"> <li>The server must be restarted to use fixed time synchronization.</li> </ul>
Possible Values	24 hours notation of the time in HH:MM:SS
Value Definition	Example, 02:00:00 to perform the synchronization at 2 AM.

### THE FOLLOWING 9 FIELDS ARE USED FOR COLLECTING ADDITIONAL USER DATA

```
user_info.customX.required=
```

Modifiable Field	<b>user_info.customX.required</b>
Field Description	More User information - X=1 - 9
Possible Values	True or False
Value Definition	True for required False for not required

```
users.display.left.x=
```

Modifiable Field	<b>users.display.left.X</b>
Field Description	Display on the registration screen left side. X = 0 to n
Possible Values	User Defined for example, users.surname
Value Definition	

```
users.display.right.x=
```

Modifiable Field	<b>users.display.right.X</b>
Field Description	Display on the registration screen right side. X =0 to n
Possible Values	User Defined for example, users.surname
Value Definition	

```
limit.recently.accessed=
```

Modifiable Field	<b>limit.recently.accessed</b>
------------------	--------------------------------

Field Description	Max. number of recently accessed targets to display when the recently accessed action is performed
Possible Values	User-Defined integer
Value Definition	User defined

```
sql.messages.maxlen=
```

Modifiable Field	<b>sql.messages.maxlen</b>
Field Description	The maximum number of characters that can be displayed in report-related messages before the messages are truncated.
Possible Values	Any number >= 1
Value Definition	The maximum number of characters are displayed in the message, followed by '...'

#### DO NOT EDIT THE FOLLOWING LINES

```
export.data.directory
file.upload.directory
trc.ticket.expiry
eg2.file.directory
```

## ldap.properties

This section describes the architecture of the **ldap.properties** file.

**This is only used if COMMON.PROPERTIES authentication LDAPconfig is 1**

```
ldap.connectionName =
```

Modifiable Field	<b>ldap.connectionName</b>
Field Description	The username used to authenticate to a read-only LDAP connection. If left blank, an anonymous connection is attempted
Possible Values	User defined for example, administrator@example.com
Value Definition	User defined

```
ldap.connectionPassword =
```

Modifiable Field	<b>ldap.connectionPassword</b>
------------------	--------------------------------



Field Description	The password used to establish a read-only LDAP connection. The password can be entered here in plain text or it can be encrypted.
Possible Values	User defined
Value Definition	User defined

```
ldap.connectionURL =
```

Modifiable Field	<b>ldap.connectionURL</b>
Field Description	URL of the LDAP server
Possible Values	User defined for example: <b>ldap://ldap.server.com</b>
Value Definition	

```
ldap.security_authentication=
```

Modifiable Field	<b>ldap.security_authentication</b>
Field Description	Specifies the security level to use. If this property is unspecified, the behavior is determined by the service provider.
Possible Values	none, simple, strong
Value Definition	String

```
ldap.groupName=
```

Modifiable Field	<b>ldap.groupName</b>
Field Description	LDAP group name
Possible Values	User Defined for example:ldapGroup
Value Definition	

```
ldap.groupNameTrim=
```

Modifiable Field	<b>ldap.groupNameTrim</b>
Field Description	Specifies whether the group name must be trimmed .
Possible Values	True or False
Value Definition	

```
ldap.groupDescription=
```

Modifiable Field	<b>ldap.groupDescription</b>
Field Description	Field for group description
Possible Values	User defined for example : description
Value Definition	

```
ldap.groupMembers=
```

Modifiable Field	<b>ldap.groupMembers</b>
Field Description	Specifies user membership within a group
Possible Values	User Defined
Value Definition	

```
ldap.groupBase=
```

Modifiable Field	<b>ldap.groupBase</b>
Field Description	Defines the starting location for the search of the LDAP groups. The Distinguished Name (DN) specified will indicate the location in the directory structure in which all groups are contained.
Possible Values	User Defined  ldap.groupBase=OU=Groups,OU=MyLocation, DC=MyCompany,DC=com
Value Definition	

```
ldap.groupSearch=
```

Modifiable Field	<b>ldap.groupSearch</b>
Field Description	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.
Possible Values	User Defined for example : ldap.groupSearch=(objectClass=group) = Imports all AD groups to Remote Control. Be aware some environment can have thousands of groups.
Value Definition	

```
ldap.groupSubtree=
```

Modifiable Field	<b>ldap.groupSubtree</b>
Field Description	If set to true, Remote Control will search recursively through the subtree of the element specified in the <b>ldap.groupBase</b> parameter 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).
Possible Values	True or False
Value Definition	

```
ldap.userPassword =
```

Modifiable Field	<b>ldap.userPassword</b>
Field Description	Password field
Possible Values	User Defined
Value Definition	

```
ldap.userEmail=
```

Modifiable Field	<b>ldap.userEmail</b>
Field Description	LDAP field for Email
Possible Values	User Defined for example: userPrincipalName
Value Definition	

```
ldap.userid=
```

Modifiable Field	<b>ldap.userid</b>
Field Description	LDAP field for userid
Possible Values	User Defined
Value Definition	

If the following parameters are defined they is mapped into the local database

```
ldap.forename=
```

Modifiable Field	<b>ldap.forename</b>
Field Description	LDAP field for forename

Possible Values	User Defined
Value Definition	User defined string

```
ldap.surname=
```

Modifiable Field	<b>ldap.surname</b>
Field Description	LDAP field for surname
Possible Values	User defined
Value Definition	User defined string

```
ldap.title=
```

Modifiable Field	<b>ldap.title</b>
Field Description	LDAP field for title
Possible Values	User Defined
Value Definition	User defined string

```
ldap.initials=
```

Modifiable Field	<b>ldap.initials</b>
Field Description	LDAP field for initials
Possible Values	User Defined
Value Definition	User defined string

```
ldap.company=
```

Modifiable Field	<b>ldap.company</b>
Field Description	LDAP field for company
Possible Values	User Defined
Value Definition	User defined string

```
ldap.department=
```

Modifiable Field	<b>ldap.department</b>
Field Description	LDAP field for department

Possible Values	User Defined
Value Definition	User Defined string

```
ldap.telephone=
```

Modifiable Field	<b>ldap.telephone</b>
Field Description	LDAP field for telephone
Possible Values	User defined
Value Definition	User defined string

```
ldap.mobile=
```

Modifiable Field	<b>ldap.mobile</b>
Field Description	LDAP field for userid
Possible Values	User defined
Value Definition	User defined

```
ldap.state=
```

Modifiable Field	<b>ldap.state</b>
Field Description	LDAP field for state
Possible Values	User defined
Value Definition	User defined string

```
ldap.country=
```

Modifiable Field	<b>ldap.country</b>
Field Description	LDAP field for country
Possible Values	User defined
Value Definition	User defined string

```
ldap.userBase=
```

Modifiable Field	<b>ldap.userBase</b>
------------------	----------------------

Field Description	the base of the sub tree containing users. If not specified, the search base is the top-level context.
Possible Values	User Defined  for example <code>ldap.userBase=OU=Users,OU=MyLocation,DC=MyCompany,DC=com</code>
Value Definition	

```
ldap.userSearch=
```

Modifiable Field	<b>ldap.userSearch</b>
Field Description	Pattern to use for searches
Possible Values	for example (userPrincipalName={0}@ActDirTest.SDC.COM)
Value Definition	All users who match the search criteria are imported into the Remote Control database. To limit this further you can use the <b>ldap.userInGroup</b> parameter.

```
ldap.userSubtree =
```

Modifiable Field	<b>ldap.userSubtree</b>
Field Description	Search up the subtree
Possible Values	True or False
Value Definition	True for search the subtree, False do not search

```
ldap.userInGroup =
```

Modifiable Field	<b>ldap.userInGroup</b>
Field Description	Determines whether a user who matches the user search criteria also has to be a member of the groups found in the group search.
Possible Values	True or False
Value Definition	<b>True</b>  only users who match the user search criteria and are members of the groups found in the group search are imported.  <b>False</b>

all users who match the user search criteria regardless of their group membership are imported.



**Note:** Users are imported into the DefaultGroup as well as any other groups that they belong to.

## log4j2.properties

This section describes the architecture of the `Log4j2.properties` file. This file is used in the setup and configuration of logging output and messages from the application.

For more information, see the following two areas:

- <https://logging.apache.org/log4j/2.x/log4j-core/apidocs/org/apache/logging/log4j/core/layout/PatternLayout.html>
- <https://logging.apache.org/log4j/2.x/manual/index.html>

```
appenders =
```

Modifiable Field	<b>appenders</b>
Field Description	Define the name of the appenders
Possible Values	User defined for example - A1, Rolling
Value Definition	

```
rootLogger.level =
```

Modifiable Field	<b>rootLogger.level</b>
Field Description	Defines the level of the logger
Possible Values	Logger has a level of WARN
Value Definition	<p>There are various levels of logger FATAL, ERROR, WARN, INFO, DEBUG, TRACE, ALL</p> <p>For more details, see <a href="https://logging.apache.org/log4j/2.x/manual/index.html">https://logging.apache.org/log4j/2.x/manual/index.html</a></p>

```
rootLogger.appenderRefs =
```

Modifiable Field	<b>rootLogger.appenderRefs</b>
------------------	--------------------------------

Field Description	The name of the Appenders to invoke
Possible Values	User defined for example - stdout
Value Definition	

```
rootLogger.appenderRef.stdout.ref =
```

Modifiable Field	<b>rootLogger.appenderRef.stdout.ref</b>
Field Description	The name of the Appenders type to invoke
Possible Values	User defined for example - STDOUT
Value Definition	

```
appender.A1.type =
```

Modifiable Field	<b>appender.A1.type</b>
Field Description	Defines the output destination that appender A1 will send the formatted messages to
Possible Values	User defined, for example Console sends the messages to the console
Value Definition	

```
appender.A1.name =
```

Modifiable Field	<b>appender.A1.name</b>
Field Description	Defines the name of the appender
Possible Values	User defined for example - STDOUT
Value Definition	

```
appender.A1.layout.type =
```

Modifiable Field	<b>appender.A1.layout.type</b>
Field Description	Used to specify the output format of the log messages
Possible Values	User defined for example - PatternLayout
Value Definition	

```
appender.A1.layout.charset =
```



Modifiable Field	<b>appender.A1.layout.charset</b>
Field Description	Encoding type to be used for the message output
Possible Values	User defined - for example UTF8
Value Definition	

```
appender.A1.layout.pattern =
```

Modifiable Field	<b>appender.A1.layout.pattern</b>
Field Description	Defines the pattern to be used for formatting the output of the log messages
Possible Values	User defined
Value Definition	See <a href="https://logging.apache.org/log4j/2.x/log4j-core/apidocs/org/apache/logging/log4j/core/layout/PatternLayout.html">https://logging.apache.org/log4j/2.x/log4j-core/apidocs/org/apache/logging/log4j/core/layout/PatternLayout.html</a>

```
appender.Rolling.type =
```

Modifiable Field	<b>appender.Rolling.type</b>
Field Description	Defines the output destination that appender Rolling will send the formatted messages to.
Possible Values	User defined, for example RollingFileAppender
Value Definition	

```
appender.Rolling.name =
```

Modifiable Field	<b>appender.Rolling.name</b>
Field Description	The name of the appender Rolling
Possible Values	User defined
Value Definition	

```
appender.Rolling.fileName =
```

Modifiable Field	<b>appender.Rolling.fileName</b>
Field Description	The name of the file that the messages are logged to.
Possible Values	User defined - for example trc.log

Value Definition	
------------------	--

```
appender.Rolling.layout.type =
```

Modifiable Field	<b>appender.Rolling.layout.type</b>
Field Description	Used to specify the output format of the log messages
Possible Values	User defined, for example: PatternLayout
Value Definition	

```
appender.Rolling.layout.charset =
```

Modifiable Field	<b>appender.Rolling.layout.charset</b>
Field Description	Encoding type to be used for the message output
Possible Values	User defined, for example - UTF-8
Value Definition	

```
appender.Rolling.layout.pattern =
```

Modifiable Field	<b>appender.Rolling.layout.pattern</b>
Field Description	Defines the pattern to be used for formatting the output of the log messages
Possible Values	User defined
Value Definition	

```
appender.Rolling.policies.type =
```

Modifiable Field	<b>appender.Rolling.policies.type</b>
Field Description	Defines the Policies for the appender
Possible Values	User defined
Value Definition	

```
appender.Rolling.policies.size.type =
```

Modifiable Field	<b>appender.Rolling.policies.size.type</b>
Field Description	The policy to use to determine if a rollover should occur.

Possible Values	User defined, for example - SizeBasedTriggeringPolicy
Value Definition	

```
appender.Rolling.policies.size.size =
```

Modifiable Field	<b>appender.Rolling.policies.size.size</b>
Field Description	The file size for triggering the rollover
Possible Values	User defined
Value Definition	

```
appender.Rolling.strategy.type =
```

Modifiable Field	<b>appender.Rolling.strategy.type</b>
Field Description	The strategy to use to determine the name and location of the archive file
Possible Values	User defined, for example - DefaultRolloverStrategy
Value Definition	

```
appender.Rolling.strategy.max =
```

Modifiable Field	<b>appender.Rolling.strategy.max</b>
Field Description	Defines the number of back up log files to keep
Possible Values	User defined, for example 4
Value Definition	

```
loggers =
```


Modifiable Field	<b>loggers</b>
Field Description	Define the logger
Possible Values	User defined, for example - rolling
Value Definition	

```
logger.rolling.name =
```

Modifiable Field	<b>logger.rolling.name</b>
------------------	----------------------------

Field Description	The name of the logger
Possible Values	User defined, for example - com.bigfix
Value Definition	

```
logger.rolling.level =
```

Modifiable Field	<b>logger.rolling.level</b>
Field Description	Defines the level of logging information to be output.
Possible Values	<ul style="list-style-type: none"> <li>• TRACE</li> <li>• DEBUG</li> <li>• INFO</li> <li>• WARN</li> <li>• ERROR</li> <li>• FATAL</li> <li>• OFF</li> </ul>
Value Definition	<p>The above values are displayed in order of how much information is logged. Whichever value is set, information for this level and above is logged. For example setting the value to DEBUG means that information from debug messages to fatal messages is logged. For a value of WARN, means that warning information to fatal information is logged.</p> <p> <b>Note:</b> After changing the value for this property and clicking Submit to save the file, you should restart the BigFix® Remote Control Server service.</p>

```
logger.rolling.appenderRef =
```

Modifiable Field	<b>logger.rolling.appenderRef</b>
Field Description	The name of the Appenders to invoke
Possible Values	User defined, for example - Rolling
Value Definition	

```
logger.rolling.appenderRef.Rolling.ref =
```

Modifiable Field	<b>logger.rolling.appenderRef.Rolling.ref</b>
Field Description	The name of the Appenders type to invoke
Possible Values	User defined, for example - LOGFILE
Value Definition	

## appversion.properties

This section describes the architecture of the `appversion.properties` file, which is used to define the version and date of the application

### DO NOT EDIT THE FOLLOWING LINES

```
version.date =
version.number =
```

## controller.properties

Edit the `controller.properties` file to create and configure global properties for the Remote Control controller component to use during a remote control session with a target. The property values apply to the controller component that is used in sessions that are started from the server. The values are the same for every user who runs the controller.

For more information about configuring global controller properties for peer-to-peer remote control sessions, see the *BigFix® Remote Control Controller User's Guide*.

Users can also configure a set of properties locally by using the **Configure Controller** feature in the controller UI. The local property values override the global property values. For more information about configuring local properties, see the *BigFix® Remote Control Controller User's Guide*.

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, you must manually edit the `controller.properties` file. For more information about how to edit the file, see [Editing the properties files \(on page 215\)](#).

To set a mandatory property, complete the following steps:

1. Open the `controller.properties` file.
2. For the property that you want to make mandatory, copy the property name and add `.mandatory = true` to the end.

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

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

3. Save the file.
4. Click **Admin > Reset Application**.

The following options can be configured when you edit the `controller.properties` file in the server UI.

### Running tools on the target during a remote control session

Configuration settings to add custom menu items to the controller UI. The menu items are added to the **Perform Action in Target** menu and can be used to run commands on the target during a remote control session.



**Note:** If too many items are added to the **Perform Action in Target** menu, the last items in the menu might extend beyond the bottom of the screen. In particular on a smaller screen size, with no support for scrolling menus.

By default, you can configure seven preconfigured tools in the server UI. Three blank tools are also available by default. To add more tools, manually edit the `controller.properties` file.



**Note:** After you manually edit the file, restart the server service or click **Admin > Reset Application** in the server UI.

Configure the properties by using the following definition formats.

```
prefix.ToolName =
```


Modifiable field	<b>prefix.ToolName</b>
Field Description	Display name that is used in the <b>Perform Action in target</b> menu. Each defined tool name must have a different prefix.
Possible Values	User Defined. For example,  <pre>tool01.ToolName=Command Prompt</pre> <p>The text, <b>Command Prompt</b>, is displayed in the <b>Perform Action in target</b> menu.</p>
Value Definition	

```
prefix.ToolName.$lang$=
```

Modifiable field	<b>prefix.ToolName.\$lang\$</b>
------------------	---------------------------------

Field Description	Display name that is used in the <b>Perform Action in target</b> menu. Translation of display name. <b>\$lang\$</b> is the ISO language code.
Possible Values	User Defined.
Value Definition	


```
prefix.ToolCommand=
```

Modifiable Field	<b>prefix.ToolCommand</b>
Field Description	Command to run the tool, without parameters.
Possible Values	<p>User Defined. For example, tool01.ToolCommand=[SystemFolder]\\control.exe</p> <p>The tool command can be a fully qualified path or just the file name. The file must be on the <b>PATH</b> environment variable of the logged in user. You can specify executable files but also files that are associated with an executable file. Do not use quotation marks, even with a path or file name that contain spaces. For example, tool01.ToolCommand=cmd.exe and tool01.ToolCommand=[SystemFolder]\\cmd.exe are equivalent.</p> <p> <b>Note:</b> When you use a backslash in the path, you must enter two backslashes.</p> <p>You can use the following folder properties when you define Windows™ tools parameters. The target substitutes the values with the actual path on the target system.</p> <p><b>[WindowsFolder]</b></p> <p>The target uses the following path to run the tool. [WindowsVolume]\Windows</p> <p><b>[SystemFolder]</b></p> <p>The target uses the following path to run the tool. [WindowsFolder]\System32</p> <p>Folder properties are not relevant for Linux™ targets. lnxcontrol.ToolCommand = /usr/bin/gnome-control-center</p>
Value Definition	

```
prefix.ToolParameters =
```

Modifiable field	<b>prefix.ToolParameters</b>
Field Description	Optional parameters for the command to run.
Possible Values	User defined
Value Definition	

```
prefix.ToolUser =
```

Modifiable Field	<b>prefix.ToolUser</b>
Field Description	Determines which privileges or credentials the command is run with.
Possible Values	<blank> or admin
Value Definition	<p><b>&lt;blank&gt;</b></p> <p>Run the tool as the logged on user.</p> <p> <b>Note:</b> Might trigger UAC prompts depending on the version of Windows™. This value is the default value.</p> <p><b>admin</b></p> <p>Run the tool with UAC prompt to elevate privileges.</p>

## Preconfigured tools

The following list of tools are preconfigured and can be edited by using the **Edit properties files** option.



**Note:** Although the tools are preconfigured, they are displayed in the **Perform action in target** menu only if the command to run the tool is installed on the target. Therefore, some sessions can display all of the preconfigured tools and other sessions might display a few preconfigured tools. Windows™ tools are displayed only when you are connected to a Windows™ target. Linux™ tools are displayed only when you are connected to a Linux™ target.

```
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 =

```

### Sending key sequences to the target during a session

Configuration settings to add custom key sequence shortcuts to the controller to inject on the target system during a remote control session. For more information about of the supported key codes, see the *BigFix® Remote Control Controller User's Guide*.

```
keyX.KeySequenceName=
```

Modifiable field	<b>keyX.KeySequenceName</b>
Field Description	Display name that is used in the <b>Perform Action in target</b> menu. Each defined key sequence name must have a different prefix. For more information, see the <i>BigFix® Remote Control Controller User's Guide</i> . X = 01 to n.
Possible Values	User Defined. For example,  <pre>key01.KeySequenceName = Inject F1</pre> The text, <b>Inject F1</b> , is displayed in the <b>Perform Action in target</b> menu.

Value Definition	
------------------	--

```
keyX.KeySequenceName.language=
```

Modifiable field	<b>keyX.KeySequenceName.language</b>
Field Description	Translations for the display name. This property is optional. X = 1 to n
Possible Values	User Defined. For example,  <code>key01.KeySequenceName.es = Inyectar F1</code>
Value Definition	

```
keyX.KeySequenceValue=
```

Modifiable Field	<b>keyX.KeySequenceValue</b>
Field Description	Macro sequence. The sequences of keys that are defined here are sent to the target system. X = 1 to n
Possible Values	User Defined. For example,  <code>key01.KeySequenceValue = [F1]</code>
Value Definition	

### End the session if audit messages cannot be uploaded to the server

Configuration setting to automatically end the session if audit messages cannot be uploaded to the server.

```
abort.on.audit.fail=
```

Modifiable field	<b>abort.on.audit.fail</b>
Field Description	During a managed remote control session, when <b>Force session audit</b> is enabled, if the controller fails to send an audit message to the server, the session ends.
Possible Values	true or false
Value Definition	<p><b>true</b></p> <p>The session ends automatically when an audit message cannot be sent to the server.</p> <p><b>false</b></p> <p>The session does not end when an audit message cannot be sent to the server.</p>

## Enabling and Disabling the execution of tools on the target during a remote session

To prevent the execution of tools on the target machine from **Perform Action in target** menu in the controller window, a new property has been added in `trc_controller.cfg` and `controller.properties`. Enabling this feature in the target removes the command entries in the **Perform Action in target** menu.

Property name	Required	Default	Description
allow.user.commands	Yes	True	Display/Hide the command entries under <b>Perform Action in target</b> menu.

To configure this controller property, complete the following steps:

### Peer-to-peer sessions

1. Edit the `trc_controller.cfg` file.

#### Windows systems

```
[controller install dir]\trc_controller.cfg
```

Where `[controller install dir]` is the directory that the controller is installed in.

#### Linux systems

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

2. Configure the property by setting true or false.
3. Save the file.

### Managed sessions

1. Edit the `controller.properties` from the Server console.
2. Configure the property by setting true or false.
3. Save the file.

## OnDemand properties file

Edit the `ondemand.properties` file to create and configure properties for remote control sessions with on-demand targets.

The `ondemand.properties` file is used to configure properties that are used during remote control sessions with on-demand targets.

- You can edit the file from the server UI by clicking **Admin > Edit properties file**.
- You can also edit the file manually. The file is in the following directory:

#### Windows™ operating systems:

`[installdir]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes`. `[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™ operating systems:**

`[installdir]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes`. `[installdir]` is the Remote Control server installation directory. For example, `/opt/Bigfix/server/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes`

- After you edit the file, you must click **Admin > Reset Application**.

## Properties to customize landing page URL

The `ondemand.url` property is set to `https://localhost/trc/ondemand/index.jsp?conncode=%c` by default. Replace `localhost` with the address of your remote control server. To use a reverse proxy, replace `localhost/trc/ondemand` with the public fully qualified domain name of the broker that is configured as a reverse proxy. For example, `https://broker.example.com/index.jsp?conncode=%c`. For more information about configuring a reverse proxy, see On-demand target portal access for internet users. If you do not replace `localhost`, the value that is defined for the `ServerURL` property in the `trc_broker.properties` file is used to create the URL that is displayed to the controller. The `%c` variable is replaced with the session connection code when the URL is displayed in the controller window. The default page requires the session connection code to be entered.

You can also set the property to a URL for your own customized web page.

**Table 8. How the URL is displayed to the controller user.**

<code>ondemand.url=</code>	<code>ServerURL=</code>	URL is displayed as.
<code>http://localhost/trc/ondemand/index.jsp</code>	<code>https://rcserver.com/trc</code>	<code>https://rcserver.com/trc/ondemand/index.jsp</code>
<code>https://mypage.com/trc/ondemand/index.jsp?conncode=%c</code>	<code>https://my-company.com/trc</code>	<code>https://mypage.com/trc/ondemand/index.jsp?conncode=1234567</code> When the connection code is 1234567.
<code>https://broker.example.com/index.jsp?conncode=%c</code>	<code>https://rcserver.com/trc</code>	<code>https://broker.example.com/index.jsp?conncode=1234567</code> When the connection code is 1234567.



**Note:** In this example there are three hostnames:



- **rcserver.com** is the Remote Control Server hostname used when the Server is directly reachable from the Broker
- **mycompany.com** is the proxied hostname used to reach the Remote Control Server through an HTTP proxy.
- **broker.example.com** is the Remote Control Broker public DNS
- **mypage.com** is the public DNS used as virtual hostname to reach the Remote Control Broker through an HTTP proxy

Not all combinations of the four above are shown in the table.

```
ondemand.url=
```

Modifiable field	<b>ondemand.url</b>
Field Description	URL for a page that the target user can access to start the process to download and temporarily install the target software.
Possible Values	User-defined URL. For example, <code>https://broker.example.com/index.jsp?conncode=%c</code>
Value Definition	Default value is <code>https://localhost/trc/ondemand/index.jsp?conncode=%c</code>

### Properties to determine how the on-demand target is downloaded and started

```
ondemand.enable.plugins=
```

Modifiable field	<b>ondemand.enable.plugins</b>
Field Description	Determines whether the plug-ins (Firefox plug-in, Internet Explorer active X, or Java™ Applet) method is used for downloading and starting the on-demand target. For more information about the methods that are used to start the on-demand target, see On-demand target installation methods.
Possible Values	<i>true</i> or <i>false</i>
Value Definition	<p><b>true</b></p> <p>Depending on the browser that is being used, the plug-ins (Firefox plug-in, Internet Explorer active X, or Java™ Applet) method is used for downloading and starting the on-demand target.</p> <p><b>false</b></p> <p>The plug-ins (Firefox plug-in, Internet Explorer active X, or Java™ Applet) method is not used to download and start the on-demand target.</p>

```
ondemand.enable.executable=
```

Modifiable field	<b>ondemand.enable.executable</b>
Field Description	Determines whether the stand-alone executable file is used for downloading and starting the on-demand target. Also, determines whether a failover link to use the executable method is provided if the on-demand target fails to start. This failover link is provided when the plug-ins (Firefox plug-in, Internet Explorer active X, or Java™ Applet) method is used. For more information about the methods that are used to start the on-demand target, see On-demand target installation methods.
Possible Values	<i>true</i> or <i>false</i>
Value Definition	<p><b>true</b></p> <p>If the <b>ondemand.enable.plugins</b> property is set to <i>false</i> the executable file is used to download and start the on-demand target.</p> <p>If the <b>ondemand.enable.plugins</b> property is set to <i>true</i>, and the plug-ins are not detected or the Java™ plug-in is not installed or enabled, the executable method is used.</p> <p>A failover link to use the executable method is provided if the on-demand target fails to start when the plug-in method or Java applet method is used.</p> <p><b>false</b></p> <p>The executable file is not used to download and start the on-demand target. A failover link to use the executable method is not provided if the on-demand target fails to start when the plug-in method or Java applet method is used.</p>

```
ondemand.enable.jnlp=
```

Modifiable field	<b>ondemand.enable.jnlp</b>
Field Description	Determines whether the Java Web Start method is provided as an option for downloading and starting the on-demand target. Also, determines whether a failover link to use the Java Web Start method is provided if the on-demand target fails to start when the plug-in method, Java applet method, or executable method is used. For more information about the methods that are used to start the on-demand target, see On-demand target installation methods.
Possible Values	<i>true</i> or <i>false</i>
Value Definition	<p><b>true</b></p> <p>If <b>ondemand.enable.plugins</b> and <b>ondemand.enable.executable</b> are set to <i>false</i>, the Java Web Start method is used to download and start the on-demand target.</p>

	<p>If <b>ondemand.enable.plugins</b> or <b>ondemand.enable.executable</b> are set to <i>true</i>, a failover link to use the Java Web Start method is provided if the on-demand target fails to start when the plug-in method, Java applet method, or executable method is used.</p> <p><b>false</b></p> <p>A failover link to use the Java Web Start method is not provided if the on-demand target fails to start.</p>
--	--

### Properties to add custom fields to the web page that is accessed from the configured URL

Use the following properties to add custom fields to the web page that is accessed from the URL that is defined in the **ondemand.url** property. Four custom fields are available by default. To add more custom fields, manually edit the `ondemand.properties` file.



**Note:** After manually editing the file, restart the server service to display the new tools on the screen.

```
ondemand.custom.field.x.label=
```

Modifiable field	<b>ondemand.custom.field.x.label</b>
Field Description	<p>Display name that is used for the extra input fields on the default web page that is used to start a session with an on-demand target. x = 1 - 9.</p> <p>If you do not set a value for this property, the field is not displayed. For example, the following sample configuration would result in defining a custom <b>Name</b> field. The definitions for index 1 are discarded because no <b>ondemand.custom.field.1.label</b> is defined:</p> <pre>ondemand.custom.field.0.label=Name ondemand.custom.field.1.required=true ondemand.custom.field.1.label.fr=Numéro de téléphone</pre>
Possible Values	<p>User Defined. For example,</p> <pre>ondemand.custom.field.1.label=Name</pre> <p>The text, Name, is displayed on the web page menu.</p>
Value Definition	

```
ondemand.custom.field.x.required=
```

Modifiable field	<b>ondemand.custom.field.x.required=</b>
Field Description	Determines whether the custom field is a required field.

Possible Values	True, False.
Value Definition	<p><b>True</b></p> <p>The target user must enter data in the field.</p> <p><b>False</b></p> <p>The target user can optionally enter data in the field.</p>

```
ondemand.custom.field.x.label.locale=
```

Modifiable field	<b>ondemand.custom.field.x.label.locale</b>
Field Description	Translation for the custom field label name. x=1 - 9
Possible Values	User Defined. For example,  <code>ondemand.custom.field.1.label.fr=Numéro de téléphone</code>
Value Definition	If no translations are present for the locale of the browser, the value in the <b>ondemand.custom.field.x.label</b> property is displayed.

### Properties to configure Lite Web Portal

```
liteweb.portal.enable=
```

Modifiable field	<b>liteweb.portal.enable</b>
Field Description	This enables the "Lite Web Portal" feature. It determines whether all accesses via the OnDemand channel related to the "Lite Web Portal" are accepted or rejected.
Possible Values	True, False.
Value Definition	<p><b>True</b></p> <p>All accesses via the OnDemand channel related to the "Lite Web Portal" will be accepted.</p> <p><b>False</b></p> <p>All accesses via the OnDemand channel related to the "Lite Web Portal" will be rejected and ignored. Default is False.</p>

```
liteweb.portal.autodetect.url=
```

Modifiable field	<b>liteweb.portal.autodetect.url</b>
Field Description	The "Lite Web Portal" build the response by dynamically resolving the broker that has originated the request.



Possible Values	True, False.
Value Definition	<p><b>True</b></p> <p>Set it to True when using the portal both from within the corporate network and from outside. Default is True.</p> <p><b>False</b></p> <p>When set to false, the <code>liteweb.portal.url</code> is used to build the responses.</p>

```
liteweb.portal.url=
```

Modifiable field	<b>liteweb.portal.url</b>
Field Description	The URL of the Reverse Proxy Broker in the form <code>https://hostname:port</code> .
Possible Values	User-defined URL in the form of <code>https://hostname:port</code> .
Value Definition	Used only when <b>liteweb.portal.autodetect.url</b> is set to False.

## Chapter 26. Reduce the volume of target connections to the server

To reduce the load on the server, you can reduce the number of heartbeats that are sent to the server from a target by using properties in the `trc.properties` file. Use the properties to reduce the volume of unnecessary heartbeats that come from a target, to prevent multiple heartbeats in quick succession, by delaying the actual heartbeat when a heartbeat is triggered, and during the delay merging these into a single heartbeat.

An exception is made for important or urgent heartbeats, for example:

- Reporting a new IP address
- Reporting the start or end of a remote control session
- Reporting status to the server requested by the user
- Restart requested by the controller
- Target going offline

You can control the delay by using the **HeartBeatDelay** property.

**Table 9. HeartBeatDelay property**

Name	Value	Default Value
HeartBeatDelay	Maximum delay in minutes	20

A random factor is also applied to the delay to distribute the heartbeat volume more evenly over time. The target chooses a random delay starting from a quarter of the maximum delay time. With the default setting, the random delay ranges from 5 minutes to 20 minutes.



**Note:** By default, the very first contact the target makes with the server, after the installation is not delayed so that the target can be registered in the server immediately.

If you are carrying out a mass deployment of targets this might cause the server to be overloaded with registrations. To alleviate this you can use the **RegistrationDelay** target property to randomly delay the registration and distribute it evenly through the deployment to avoid too many machines trying to register at the one time.

**Table 10. HeartBeatDelay and RegistrationDelay properties**

Name	Value	Default Value
HeartBeatDelay	Maximum delay in minutes	20

**Table 10. HeartBeatDelay and RegistrationDelay properties (continued)**

<b>Name</b>	<b>Value</b>	<b>Default Value</b>
RegistrationDelay	Maximum delay in minutes	0

You can use the following properties to prevent a heartbeat from being triggered for certain events.

**Table 11. Heartbeat properties to control heartbeats for certain events**

<b>Name</b>	<b>Value</b>	<b>Default value</b>	<b>Description</b>
HeartBeatOnWake	1/0	0	Trigger a heartbeat when the system wakes from standby or hibernation
HeartBeatOnUserChange	1/0	1	Trigger a heartbeat when a user logs on or off
HeartBeatOnChange	1/0	0	Trigger a heartbeat when any of the values included in a heartbeat have changed
HeartBeatOnStop	1/0	0	Trigger a heartbeat when the target is stopped or the system is shutting down

# Chapter 27. Broker configuration

When you install broker support you can use the installed `trc_broker.properties` file to configure your environment for using the broker function.

When the broker support is installed, a configuration file, `trc_broker.properties`, is created which provides examples of the configuration parameters you can use to create a broker configuration to satisfy your network requirements.

In the configuration file you can define default broker setup parameters and also any connections required for your environment.

- The broker supports multiple instances of each connection type
- The configuration directives for each connection have a user defined prefix.

## Configuring the broker properties

You can edit the `trc_broker.properties` file to configure the parameters and connection types required for using brokers in your environment.

To configure the broker to your requirements, edit the `trc_broker.properties` file.

On a windows machine this file is located in the `\Broker` directory within the brokers's working directory.

In a Windows system, the file is located in `\ProgramData\BigFix\Remote Control\Broker\`. In Linux the file is located in the `/etc` directory.



**Note:** Any errors in the configuration file do not stop the broker from starting. Examine the broker log to verify that the broker is running as expected. For more details about configuring logging parameters, see [Logging broker activity \(on page 312\)](#).

## Setting server connection parameters

Edit the `trc_broker.properties` file to set the parameters for the server that the broker authenticates with.

At the start of a broker remote control session, the broker connects to the server to authenticate the session. Use the following parameters to define the server.

### ServerURL

Determines the URL of the server that the broker authenticates the session with. This parameter must be set to the base URL, for example `https://trcserver.example.com/trc`. A trailing / character is allowed. This parameter is a required parameter.



**Note:** The broker requires a connection to the remote control server to authenticate sessions and connection codes. As the broker is typically located outside of the intranet while the server is inside of it, this connection requires a proxy server or a chain of gateways. Use



HTTPS and not HTTP if the connection from the broker to the server passes through an unsecure or untrusted network. Also, use HTTPS if the following properties are enabled in the `trc.properties` file, **enforce.secure.endpoint.callhome**, or **enforce.secure.endpoint.upload**. Otherwise, the target cannot send audit information or status updates to the server. For more information about the **enforce.secure** properties, see [trc.properties \(on page 216\)](#).

### ProxyURL

Add the URL of a proxy server or gateway if you are using one. This parameter is optional. For security purposes, the plain text `userid:password` combination in the URL is now automatically encrypted when the broker starts. For more information, see [Automatic passphrase encryption \(on page 34\)](#).

## Configuring the broker certificate

Use the following parameters to define the location of the certificate, and password for the broker.

### DefaultTLSCertificateFile

Filename or path to the TLS certificate for this broker. For more details on creating and managing broker certificates, see [Certificate management \(on page 327\)](#).

### DefaultTLSCertificatePassphrase

Password for the private key that is associated with the TLS certificate. This parameter is optional. For security purposes, the password is automatically encrypted when you start the broker.

## Allowing endpoints to connect to a broker

To allow the broker to accept connections from controllers and targets you can define and configure inbound connections using the `trc_broker.properties` file.

You can configure multiple inbound connections and define a prefix for each connection parameter to allow the broker to find all required settings for each connection. Configure any inbound connections when configuring the `trc_broker.properties` file. For more details about editing this file, see [Configuring the broker properties \(on page 308\)](#).



### Note:

1. Do not prefix with `#` or `!` as these are reserved for comments in properties files.
2. If you want to include spaces in the prefix you have to escape them with `\` for example: `my connection.ConnectionType` should be defined as `my\connection.ConnectionType`

To configure inbound connections complete the following steps:

1. Configure the following parameters within the `trc_broker.properties` file

#### ConnectionType

Defines the type of connection. Should be set to `Inbound` or `Inbound6` when you are using IPv6 networks. For example: `my\connection.ConnectionType=Inbound`

#### PortToListen

Defines the TCP port that endpoints should use to connect to this broker. The port for listening for inbound connections. Required parameter.

#### AllowEndpoints

Determines whether endpoints can connect to this broker.

##### Yes

Endpoint connections can be made to this broker. This is the default value.

##### No

Endpoint connections cannot be made to this broker.

#### AllowBrokers

Determines whether other brokers can connect to this broker. Set to `No` or `<blank>` means other brokers cannot connect to this broker. If other brokers can connect to this broker, provide a list of brokers that are allowed to connect. For example `broker1.company.com,broker2.company.com,broker3.company.com`.



**Note:** The hostnames listed here must match the certificate and the hostnames used when registering the brokers in the remote control server.

2. Save the file.

If you are configuring multiple brokers in your environment which will connect to each other to complete the connection between the controller and target, you should configure broker connections in the broker properties file. For more details, see [Support for multiple brokers \(on page 310\)](#). When you have finished creating a broker configuration you can register the brokers in the BigFix® Remote Control Server database to be used for facilitating remote control connections across the internet. For more details, see [Registering a broker on the server \(on page 325\)](#).

## Support for multiple brokers

To allow the broker to accept connections from other brokers you can define and configure broker connections using the `trc_broker.properties` file.

When you have multiple brokers defined in your environment you should configure broker control connections and define a prefix for each connection parameter to allow the broker to find all required settings for each connection. Broker connections need to be configured between the brokers that will connect to each other. The brokers use

the network of control connections to determine which broker has the connection from the target. When the target is located, the controller is reconnected to the same broker as the target. Configure any broker connections when configuring the `trc_broker.properties` file.



**Note:**

1. Do not prefix with # or ! as these are reserved for comments in properties files.
2. If you want to include spaces in the prefix you have to escape them with \ for example: `my\connection.ConnectionType` should be defined as `my\connection.ConnectionType`

To configure broker connections complete the following steps.

1. Configure the following parameters within the `trc_broker.properties` file of the broker that will connect to connect to another broker.

**ConnectionType**

Defines the type of connection. Should be set to `Broker` For example: `my`

`\connection.ConnectionType=Broker`

**DestinationAddress**

Defines the hostname of the broker that the connection is being made to. The broker with this address needs to be configured to accept inbound connections. This parameter is required. For

example: `my\connection.DestinationAddress=mybroker.ibm.com`



**Note:** Set the **AllowBrokers** parameter in the configuration file of the broker that this connection is being made to. Set this parameters to allow other brokers to connect to it. For more details, see [Allowing endpoints to connect to a broker \(on page 309\)](#).

**DestinationPort**

Defines the TCP port of the broker to connect to. This parameter is required.

**PublicBrokerURL**

Determines the public address and port for the broker you are currently configuring. When there are multiple brokers configured, if the target connects to this broker and the controller connects to a different broker, the property is used to identify this broker so that the controller can connect to it and then successfully reach the target. This property should be set to `hostname:port` where `hostname` is the hostname of this broker machine and `port` is the port that this broker is listening for connections on. Default value is `<blank>`.



**Note:** The hostname used here should be the same as the hostname used when registering the broker on the Remote Control server.

2. Save the file.

When you have created a broker configuration you can register the brokers in the Remote Control database to be used for facilitating remote control connections across the internet. For more details, see [Registering a broker on the server \(on page 325\)](#).

## Logging broker activity

Broker session activity is saved to the broker log files. These files are named using the following format.

`TRCICB-computername-suffix.log`

where *computername* is the computer name of the broker and *suffix* is determined by the LogRotation and LogRollover settings.

For example, `TRCICB-RCBROKER.example.com-Tue.log`

The broker log files are located in the `\Broker` directory within the brokers's working directory.

In a Windows system, the file is located in `\ProgramData\BigFix\Remote Control\Broker\`. In Linux the file is located in the `/var/opt/bigfix/trc/broker` directory.

To configure logging complete the following steps:

1. Configure the following properties within the `trc_broker.properties` file.

For more information about the properties, see [Properties for configuring logging activity \(on page 425\)](#)

### **LogLevel**

Set the required logging level.

The log level determines the types of entries and how much information is added to the log file.  
Default value is 2.

### **LogRotation**

Controls the period after which an older log file is overwritten. Log rotation can be disabled.  
Default value is Weekly.

### **LogRollOver**



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.

2. Save the file.

## Configuring optional parameters

The following optional parameters can be used to further configure your broker.

### Global parameters

#### FIPSCompliance

Determines whether a FIPS certified cryptographic provider is used for all cryptographic functions. Default value is *No*.

#### SP800131ACompliance

Determines whether **NIST SP800-131A** compliant algorithms and key strengths are used for all cryptographic functions. Default value is *No*.

#### HTTPSStrictValidation

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

### Request Pool

An area of memory that is known as the Request Pool is used to track requests. The connection requests from other brokers are kept in the pool until the pool is full and the oldest requests are recycled. The following parameters can be used to configure the request pool:

#### Request Pool.size

The amount of memory, in kilobytes, to reserve for the request pool. The default is 2048 or 2 megabytes.

#### Request Pool.MinimumTTL

The minimum time, in minutes, before a request can be recycled. The default is 5 minutes.

### RecordingDir

Use RecordingDir to define the directory that the session recording is temporarily stored on the broker if **Force Session Recording** is set to Yes.

For example, `RecordingDir=c:\\tmp`. When you are using a backslash in the path, you must enter two backslashes.

You can also specify relative directories. For example, `RecordingDir=tmp`. The recording is temporarily stored in the tmp directory within the working directory of the broker.

If you do not add `RecordingDir` to the properties file, the recording is temporarily stored in the working directory of the broker.

### Parameters for inbound connections

#### BindTo

Used to accept incoming connections on specific network interfaces.

For example: `my\connection.BindTo=192.0.2.0`

Default is 0.0.0.0.

#### RetryDelay

Defines the time in seconds between attempts to open the configured port for listening for incoming connections. Default is 45 seconds.

#### TLSCipherList

List of allowed ciphers. For more information about allowed ciphers, see [Default configuration parameters \(on page 315\)](#).

### Parameters for broker connections

#### BindTo

This parameter is optional and can be configured to allow the broker to establish the outgoing broker connection from a specific network interface. For example, if a firewall on the network is configured to allow only 1 of the broker's interfaces through. Defines the IP address of the network interface through which the connections are made. For example: `broker.1.BindTo=192.0.2.0` Default is 0.0.0.0.

#### KeepAlive

Defines the time in seconds between keepalive requests. This parameter is optional. Default is 45 seconds.

#### RetryDelay

Defines the time in seconds between attempts to establish or re-establish the control connection. This parameter is optional. Default is 45 seconds.

#### SourcePort

Defines the port that the outgoing broker connection is using. By default the broker uses an unused port.

#### TLSCipherList

List of allowed ciphers. For more information about allowed ciphers, see [Default configuration parameters \(on page 315\)](#).

## Parameter for passphrase encryption

### DisableAutomaticPassphraseEncryption

Determines whether the automatic encryption of plain text passwords in the broker configuration file is disabled. The default value for the property is *No*. For more information about the use of this property, see [Automatic passphrase encryption \(on page 34\)](#).

## Default configuration parameters

### Default parameters

Use the set of default parameters, prefixed with Default to set your configuration, and also configure multiple connections. The parameters have a set of default values that you can be change. The values can be applied to the parameters prefixed with Default and also to the connection parameters.

**Table 12. Default parameter values**

*A three column table that provides the default values that all broker connections use if there are no additional connections defined.*

Keyword	Default Value	Re-quired
ServerURL	<blank>	Yes
ProxyURL	<blank>	No
DefaultPortToListen	<blank>	Yes
DefaultBindTo	0.0.0.0	No
DefaultBindTo6	::	No
DefaultRetryDelay	45	No
DefaultKeepAlive	900	No
DefaultTLSCertificate	server.pem	No
DefaultTLSCertificatePassphrase	<blank>	No
DefaultTLSCipherList	TLSv1.2:AES:!kECDH:!kDH:!RSA:!aNULL:!eNULL:!SRP:!PSK:!CAMELLIA:!3DES:!MD5:!RC4:!EXP:!DES:@STRENGTH	No
DefaultHTTPCipherList	TLSv1.2:AES:!kECDH:!kDH:!RSA:!aNULL:!eNULL:!SRP:!PSK:!CAMELLIA:!3DES:!MD5:!RC4:!EXP:!DES:@STRENGTH	No

The default values can be used to set values for all connections. However, values that are set for specific connections override the default value for that connection.

### Example 1: Using a default value

DefaultKeepAlive = 300

Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8887

Broker.1.ConnectionType = Broker

Broker.1.DestinationAddress = broker1.example.com

Broker.1.DestinationPort = 8887

Broker.2.ConnectionType = Broker

Broker.2.DestinationAddress = broker2.example.com

Broker.2.DestinationPort = 8887

Broker.2.KeepAlive = 100

In this example, the **DefaultKeepAlive** value of 300 is used for the **Inbound.1** connection and the **Broker.1** connection. Setting the default parameter means that you do not need to add the property to each specific connection. However, the **Broker.2** connection uses the KeepAlive value of 100 since the **Broker.2.KeepAlive** property is set. The specific connection value overrides the default value.

### Example 2: Using specific values

Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8887

Inbound.1.KeepAlive = 300

Broker.1.ConnectionType = Broker

Broker.1.DestinationAddress = broker1.example.com

Broker.1.DestinationPort = 8887

Broker.1.KeepAlive = 300

In this example, no **DefaultKeepAlive** value is set. A KeepAlive property value is set for each specific connection.

### Required default parameters

Required parameters do not have a built-in default value. These parameters must be set either to the value given in the file or within the connection configurations. When a required parameter is set in the connection parameters, this value overrides any default values set for the same parameter.

**Table 13. Required parameters values used**

*A three column table that provides values that are used for required parameters, depending on where the parameters are set.*

Default parameter set	Connection parameter set	Value Used
No	No	Not defined, a required parameter must be defined in the configuration.
No	Yes	Connection parameter is used
Yes	No	Default parameter is used.
Yes	Yes	Connection parameter is used.

### Optional default parameters

Optional parameters have a built-in default value. If the parameter is not set within the default parameters or within the connection parameters, the built-in default value is used. If the parameter is set within the default parameters, but is not set within the connection parameters, the default parameter value is used by any connections.

**Table 14. Optional parameters**

*A three column table that provides the values that are used for optional parameters, depending on where the parameters are set.*

Default parameter set	Connection parameter set	Value used
No	No	Built in default value is used
No	Yes	Connection parameter is used
Yes	No	Default parameter is used
Yes	Yes	Connection parameter is used

### Parameter definitions

#### **DefaultPortToListen**

Defines the TCP port that endpoints must use to connect to this broker. The port for listening for inbound connections. Required parameter.

#### **DefaultSourcePort**

Defines the port that the outgoing connection is using. This parameter is optional. Default is 0.

**DefaultBindTo**

This parameter is optional. Defines the IP address that is used to create connections with.

For example: `my\connection.BindTo=192.0.2.0`

Default is 0.0.0.0. Optional parameter.

**DefaultBindTo6**

This parameter is optional. Defines the IP address that is used to create connections with in IPv6 networks. Default is ::. Optional parameter.

**DefaultRetryDelay****inbound connections**

Defines the time in seconds between attempts to open the configured port for listening for incoming connections. Default is 45 seconds.

**broker connections**

Defines the time in seconds between attempts to establish or re-establish the control connection. This parameter is optional. Default is 45 seconds.

**DefaultKeepAlive**

Defines the time in seconds between keepalive requests. This parameter is optional. Default is 900 seconds.

**DefaultTLSCertificateFile**

Filename or path to the TLS certificate for this broker. For more information on creating and managing broker certificates, see [Certificate management \(on page 327\)](#). Default is `server.pem`.

**DefaultTLSCertificatePassphrase**

Password for the private key that is associated with the TLS certificate. This parameter is optional. For security purposes, the password is automatically encrypted when you start the broker.

**DefaultTLSCipherList and DefaultHTTPCipherList**

Use this configuration keyword to override the selection of cipher suites that can be used to secure network connections to or from a broker. A cipher suite is a combination of four cryptographic algorithms that are used together to create a secure communication channel. These algorithms are provided by a cryptographic module included with the broker. This module also includes algorithms for compatibility with an earlier versions, even if they are now considered to offer little or no security. By default, the broker selects only cipher suites that offer strong security. The default selection can be overridden if necessary. This is normally not needed, but can be used, for example, to disable an algorithm against which a new cryptographic attack is discovered. The documentation for the syntax of the cipher list can be found on the OpenSSL website. [http://www.openssl.org/docs/apps/ciphers.html#CIPHER\\_LIST\\_FORMAT](http://www.openssl.org/docs/apps/ciphers.html#CIPHER_LIST_FORMAT)

Default Cipher List

**TLSv1+HIGH**

Only ciphers from the TLSv1 cipher suite with key lengths larger than 128 bits and some cipher suites with 128-bit keys.

**TLSv1**

Only ciphers from the TLSv1 cipher suite.

**!SSLv2**

Permanently remove all ciphers from the SSLv2 cipher suite.

**!aNULL**

Permanently remove all ciphers without authentication.

**!eNULL**

Permanently remove all ciphers without encryption.

**!3DES**

Permanently remove all ciphers that use the triple DES encryption algorithm.

**@STRENGTH**

Order the cipher list in order of encryption algorithm key length.



**Note:** The broker supports only TLSv1. Support for SSLv2 and SSLv3 is disabled due to known vulnerabilities in those versions of the protocol, even if you include SSLv2 or SSLv3 in the cipher list.

### Types of cryptographic algorithms

**Authentication**

Verify the identity of the client or server that is using digital certificates.

**Key Exchange**

Establish shared secrets to be used as encryption keys and message authentication keys for the session.

**Encryption**

Protects the session data from being accessed by unauthorized entities.

**Message authentication**

Protects the session data from being tampered with.

With the version of OpenSSL that is included with the broker component and the default cipher list, the following ciphers can be used:

**Encryption**

- AES key length 256 bits
- AES key length 128 bits

#### Authentication

- RSA
- DSA

#### Key Exchange

- RSA
- Diffie-Hellman

#### Message Authentication

SHA-1

## Broker setup examples

The following example illustrates a broker and gateway setup.

There are 3 networks present, an intranet, a DMZ network and an internet facing network. A firewall between the Intranet and the Internet allows outbound connectivity but blocks all inbound connections. There is also a security policy in force that does not allow connections to be initiated from the DMZ to the intranet or from the Internet Facing network to the DMZ.

Hosts in the Internet Facing network do not have public IP addresses. The internet gateway uses DNAT to map internal IP addresses to public IP addresses, only for the ports needed for specific public services. In this example, the public service is the broker.

The broker requires connectivity to the server, but direct connections from the Internet Facing network to the server are not allowed. A chain of gateways is deployed to allow the broker to connect to the server.

The following tables provide details of the components and settings present in the example environment.

**Table 15. TRC components**

#### *TRC components present on the network*

Network name	Server	Bro-ker	Gate-way	Con-troller	Tar-get
Intranet	Yes	No	Yes	Yes	Yes
DMZ	No	No	Yes	No	No
Internet facing	No	Yes	Yes	No	No



**Table 15. TRC components*****TRC components present on the network*****(continued)**

<b>Network name</b>	<b>Server</b>	<b>Bro-ker</b>	<b>Gate-way</b>	<b>Con-troller</b>	<b>Tar-get</b>
Internet	No	No	No	No	Yes

**Table 16. Networks*****Networks and network addresses present in the environment***

<b>Network name</b>	<b>Subnet Address</b>	<b>Subnet Mask</b>
Intranet	10.1.0.0	255.255.255.0
DMZ	10.2.0.0	255.255.255.0
Internet Facing	10.3.0.0	255.255.255.0

**Table 17. Machines*****Machines present in the environment***

<b>Host name</b>	<b>IP address</b>	<b>Roles</b>
SERVER.example.com	10.1.0.2	TRC server on port 443
BROKER1.example.com	10.3.0.10	TRC broker on port 8887
BROKER2.example.com	10.3.0.11	TRC broker on port 8887
GATEWAY1.example.com	10.1.0.254	TRC gateway
GATEWAY2.example.com	10.2.0.254	TRC gateway on port 8881
GATEWAY3.example.com	10.3.0.254	TRC gateway on port 8881, inbound tunnel on port 8880
CONTROLLER1.example.com	Dynamic IP in 10.1.0.0/24	TRC controller
TARGET1.example.com	Dynamic IP in different networks	TRC target on mobile system

**Table 18. Firewall****Firewall settings in the environment**

Source	Destination	Port	Description
10.1.0.254/255.255.255.255	10.2.0.254/255.255.255.0	8881	Allow GATEWAY1 to connect to GATEWAY2
10.2.0.254/255.255.255.255	10.3.0.254/255.255.255.0	8881	Allow GATEWAY2 to connect to GATEWAY3

**Table 19. DNAT****DNAT settings in the environment**

Public DNS Name	Public IP	va
BROKER1.example.com	203.0.113.23	10.
BROKER2.example.com	203.0.113.24	10.

**Broker Configuration**

Each broker is configured with

- Inbound connection for endpoints to connect
- Connection to the server via a gateway

Broker 1 is configured with an additional inbound connection for control connections from broker 2. Broker 2 is configured with a control connection to broker 1.

The following section provides examples of what would be set in the broker and gateway properties files for each of the relevant components.

**BROKER1.example.com**

PublicBrokerURL = BROKER1.example.com:8887

ServerURL = https://SERVER.example.com/trc/

ProxyURL = trcgw://GATEWAY3.example.com:8880

DefaultTLSCertificateFile = BROKER1.p12

DefaultTLSCertificatePassphrase = \*\*\*\*\*

Inbound1.ConnectionType = Inbound

Inbound1.PortToListen = 8887

Broker2.ConnectionType = Broker

Broker2.DestinationAddress = BROKER2.example.com

Broker2.DestinationPort = 8881

### **BROKER2.example.com**

PublicBrokerURL = BROKER2.example.com:8887

ServerURL = https://SERVER.example.com/trc/

ProxyURL = trcgw://GATEWAY3.example.com:8880

DefaultTLSCertificateFile = BROKER2.p12

DefaultTLSCertificatePassphrase = \*\*\*\*\*

Inbound1.ConnectionType = Inbound

Inbound1.PortToListen = 8887

Inbound2.ConnectionType = Inbound

Inbound2.PortToListen = 8881

Inbound2.AllowEndpoints = no

Inbound2.AllowBrokers = BROKER1.example.com

### **Gateway Configuration**

#### **GATEWAY1**

Gateway 1 is configured with a control connection to gateway 2 and an outbound tunnel connection to the server.

Gateway2.ConnectionType = Gateway

Gateway2.DestinationAddress = 10.2.0.254

Gateway2.DestinationPort = 8881

Server.ConnectionType = OutboundTunnel

Server.DestinationAddress = 10.1.0.2

Server.DestinationPort = 443

## **GATEWAY2**

Gateway 2 is configured with an inbound connection and a control connection to gateway 3.

Inbound.ConnectionType = Inbound

Inbound.PortToListen = 8881

Gateway3.ConnectionType = Gateway

Gateway3.DestinationAddress = 10.3.0.254

Gateway3.DestinationPort = 8881

## **GATEWAY3**

Gateway 3 is configured with an inbound connection and an inbound tunnel connection.

Inbound.ConnectionType = Inbound

Inbound.PortToListen = 8881

Server.ConnectionType = InboundTunnel

Server.PortToListen = 8880

## Chapter 28. Managing brokers

After installing broker support you can register the broker machines in the Remote Control server. When they have been registered you can view the list of brokers, edit the broker details and delete brokers that are no longer required.

The registered broker list is passed from the server to the targets when the targets register, in response to contact from the target, or at the start of a remote control session. The list is stored in the target property **BrokerList**.

When a target user enters a connection code to start a remote control session using a broker, the target machine tries to connect to each broker in the list until it makes a successful connection to one of them. Therefore, when making changes to the broker list you should ensure that there is still one unchanged broker in the list so that the targets can still connect in a remote control session, then when they are in the session they can contact the server and receive the updated broker list.

### Registering a broker on the server

After installing and configuring broker support in your environment you can register a broker in the Remote Control server This section will explain how to add a broker to the server.

To register a broker complete the following steps

1. Select **Admin > New Remote Control Broker**
2. On the **Add Remote Control Broker** screen enter the relevant information

**Fully qualified hostname**

Enter the fully qualified ( DNS) hostname for the broker.

**Port**

Enter the port that the broker will be listening for connections on.

**Description**

Enter a description for the broker. This is optional.

3. Click **Submit**.

The broker is added to the Remote Control database.

### Viewing a list of registered brokers

After you have registered brokers you can view the list of brokers by displaying the **All Remote Control Brokers** report.

To view the registered brokers select **Admin > All Remote Control Brokers**

The list of registered brokers is displayed.

## Editing broker details

After registering a broker on the Remote Control server you can use the edit broker feature to change any of the saved information for the broker .

To edit broker information complete the following steps

1. Select **Admin > All Remote Control Brokers**
2. Select the required broker.
3. Select **Edit Remote Control Broker**.
4. Change the relevant information and click **Submit**.

The broker information is updated and saved to the database.

## Deleting a broker

You can remove Remote Control brokers from the database if they are no longer required.

To remove a broker from the **All Remote Control Brokers** page, complete the following steps

1. Select **Admin > All Remote Control Brokers**
2. Select the required broker.
3. Select **Delete Remote Control Broker**.
4. Click **Confirm** on the Confirm deletion screen.

The selected broker is deleted from the Remote Control database.



**Note:** Click **Cancel** on the confirm deletion screen to return to the previously displayed screen and the broker is not deleted.

# Chapter 29. Certificate management

Remote Control uses certificates in the Server and in the Broker to address the authentication and verification required for ensuring secure connections between the different product components.

Remote Control can use multiple types of Public Key Infrastructure ( PKI)

- A commercial Certificate Authority ( CA)
- An internal CA
- Self-signed certificates

There is no difference between using a commercial CA or an internal CA and it is possible to mix the two kinds. For example, you can run the Remote Control server with a self-signed certificate while running all brokers with CA-signed certificates.

Remote Control provides two levels of certificate validation, strict certificate validation and non-strict certification validation.

## Non-strict certificate validation

- Non-strict certificate validation performs the following checks against the certificate
  - The identity of the certificate matches the hostname of the broker that you are trying to connect to.
  - The certificate is within its validity period.

In non-strict mode, the client does not need a trust store to perform the validation.



**Note:** This type of certificate validation is strongly discouraged for production usage for remote control sessions over the internet, it is only intended for demo and test environments.

## Strict certificate validation

- Strict certificate validation performs one additional check. This additional check requires that the client has a trust store that contains all the root certificates required to validate the certificate chain.

For Certificate operations you can use the IBM Key Management tool (ikeyman), which ships as part of Remote Control, the OpenSSL command line tool or other third party tools. Procedures in this manual show the use of the IBM Key Management tool.

## Creating a self signed certificate

Read this page to learn the procedure to renew or generate self-signed certificates.

To generate the certificate for a broker you can use the IBM Key Management tool. This tool is provided with the Remote Control application and with IBM WebSphere Application Server.

1. Open a command prompt window.
2. Go to the Remote Control Server installation directory.
3. Change to the [installdir]\java\jre\bin subdirectory on a Windows™ system or the [installdir]/java/jre/bin subdirectory on a Linux™ system.
4. Run `ikeyman.sh` on a Linux™ system or `ikeyman.exe` on a Windows™ system.
5. Select **Key Database File > New**
6. Select the database type. (Use PKCS12 for Broker Certificate. Use PKCS12 or JKS for the Server certificate)
7. Click **Browse**, navigate to the location you want to store the keystore, type a filename for your file and click **Save**.
8. Click **OK**.
9. Enter and confirm a password to protect the keystore and click **OK**.
10. Select **Create > New Self-Signed Certificate**
11. Enter a name for the **Key Label**.  
For example, the hostname of the broker.  
This is the name that will be displayed in the Personal Certificates list in the key management tool GUI.
12. Select **X509 V3** for the **Version**.
13. Select a **Key Size** value.  
Recommended value is 2048.
14. Select a **Signature Algorithm**  
This is a cryptographic algorithm for digital signatures and should be left as the default value SHA256WithRSA.
15. Type a **Common Name** .  
Set to the DNS host name and domain of your broker.  
For example `trcbroker.example.com`
16. Type the **Subject Alternate Name**.

Most recent browsers use the Subject Alternate Name to validate the certificate in place of (or in addition to) the Common Name. Make sure you provide a matching subject alternate name. For example `server.example.com`.



**Note:** Java based certificate tools (like ikeyman) do not support Subject Alternate Names with domain names that start with a number. For example, `server.8xxx.com`. In this case you need to use OpenSSL or another external tool to create the certificate.

17. Enter any additional optional information as required.
18. Enter a **Validity Period**.  
This is the number of days that the certificate will be valid for. Default is 365 days.
19. Click **OK**.

#### **Self-signed certificate**



If you plan to use the self-signed certificate, you need to extract the certificate at this point by performing the following steps. You can then copy and paste the content of this file where applicable.

- a. Click **Extract Certificate**.
- b. Use the default Data type Base64-encoded ASCII data.
- c. Enter a file name and location for saving the certificate file to.
- d. Click **OK**.

### CA-Signed certificate

If you plan to use CA Signed certificate, you need to create the CSR at this point performing the following steps.

- a. Create a Certificate Signing Request
  - i. Select Recreate Request
  - ii. Indicate the location where to save the certreq.arm file
  - iii. Press OK.

A certreq.arm file is generated and saved to the location specified. This file must be sent to the certificate authority to be signed.

For more information to complete the CA signing process, see [Creating Certificate Authority signed certificates \(on page 331\)](#).

The .p12 (or .jks) file is created with the name and selected location chosen.



**Note:** The key store contains the private key for the certificate and this must be kept secure at all times. It is recommended that the original copy of the keystore is stored in a secure disk, for example an encrypted USB storage device or similar. Keeping a secure backup of the original keystore is also recommended.

## Configuring the keystore on the broker

After you have created the keystore which holds the private key and certificate for the broker, it should be copied to the broker machine and the broker properties configured accordingly.

To configure the keystore on the broker complete the following steps:

1. Copy the .p12 or .pem file to the working directory of the broker machine.
2. Edit the `trc_broker.properties` file and configure the **TLSCertificateFile** property, setting it to the name of the .p12 or .pem file.



**Note:** Use **DefaultTLSCertificateFile** to configure the certificate used for all connections to this broker. Each inbound or broker connection can also be configured to use a different certificate.

3. Use the **TLSCertificatePassphrase** property to define a password for the keystore.

4. Save the properties file.
5. Restart the broker service.

#### Windows systems

- a. Navigate to **Control Panel > Administrative tools > Services**
- b. Right click **Remote Control-Internet Connection Broker** and select **Restart**.

#### Linux systems

Depending on the type of Linux operating system that you are using, you can use one of the following commands to restart the broker service.

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

The broker will use the indicated keystore when providing server identity information.

## Strict Certificate Verification on Broker Connections

The Remote Control controller and target, instructed by the remote control server, uses strict certificate validation by default when connecting to a broker. This verification requires a trust store that contains the trusted certificate.

The target downloads and caches the trust store when registering, during the call home process with the server, during a remote control session or when configured using the BigFix Console Remote Control target configuration wizard. The controller downloads the trust store at the start of the remote control session.

The trust store must contain the Certificate Authority's root certificates when using a CA signed certificate, or the broker certificate when using self-signed certificate. In this case the certificate needs to be exported from the keystore and uploaded to the Remote Control.

The use of strict certificate validation is determined by the **broker.trusted.certs.required** property in the `trc.properties` file on the remote control server.

#### Set to Yes

Strict certificate validation is enabled. This is the default value.

#### Set to No

Strict certificate validation is disabled.



**Note:** Disabling strict verification is not recommended. When strict verification is disabled, the Remote Control controller and target will trust all valid certificates, whether they were generated by you or by a potentially malicious third party.

## Extracting the certificate from the keystore

When using strict certificate verification, the certificate needs to be extracted from the keystore before being uploaded to the Remote Control server.

To extract the certificate complete the following steps:

1. Open a command prompt window.
2. Go to the Remote Control installation directory.
3. Change to the [installdir]\java\jre\bin subdirectory on a Windows™ system or the [installdir]/java/jre/bin subdirectory on a Linux™ system.
4. Run ikeyman.sh on a Linux™ system or ikeyman.exe on a Windows™ system.
5. Select **Key Database File > Open**
6. Select **PKCS12** for **Key database type** depending on your keystore type.
7. Click **Browse**, navigate to and select the required file.
8. Click **Open** then **OK**.
9. Enter the password for the file and click **OK**.
10. For **Key database content** select **Personal Certificates**.
11. Select the required certificate.
12. Click **Extract Certificate**.
13. Use the default Data type **Base64-encoded ASCII data**.
14. Enter a file name and location for saving the certificate file to.
15. Click **OK**.

The certificate file, with extension .arm, will be extracted to the chosen location.

## Creating Certificate Authority signed certificates

Read this page to learn the procedure to renew or generate CA signed certificate.

The process of obtaining a CA signed certificate requires the creation of a Certificate Signing Request (CSR) that must be provided to the Certificate Authority. The CA will return a signed certificate that then needs to be imported in the keystore.

To accomplish this procedure, you can use the IBM Key Management tool. This tool is provided with the Remote Control application and with IBM WebSphere Application Server.

1. Open a command line window.
2. Go to the Remote Control Server installation directory.
3. Change to the [installdir]\java\jre\bin subdirectory on a Windows™ system or the installdir]/java/jre/bin subdirectory on a Linux™ system.
4. Run ikeyman.sh on a Linux™ system or ikeyman.exe on a Windows™ system.
5. In the GUI window, select Key Database File > Open.
6. Go to the directory where the keystore is located and open the existing keystore.

### To open the Server Default Keystore:

- a. The Keystore is in [installdir]/wlp/usr/servers/trcserver/resources/security directory, where [installdir] is the Remote Control Server installation directory.
- b. Select the file named key.jks.

- c. Click open.
- d. Enter the password `TrCWebAS`.

**To open another Keystore:**



**Note:** If you are running a Remote Control Server 10.0.0.0512 or earlier and if you want to generate the PKCS12 (.p12 or .pfx) using OpenSSL 3, you need to add the option `-legacy` to the command. For example: `openssl pkcs12 -export -out keystore.p12 -inkey key.pem -in cert.pem -legacy`.

- a. Select the directory where the keystore is located.
  - b. Select the keystore file name and Type.
  - c. Click open.
  - d. Enter the password.
7. Create a Certificate Signing Request
- a. Select Recreate Request
  - b. Indicate the location where to save the `certreq.arm` file
  - c. Press OK.
  - d. A `certreq.arm` file is generated and saved to the location specified. This file must be sent to the certificate authority to be signed.

The `certreq.arm` is a base-64 encoded ASCII representation of the certificate request. You may have to copy the content of this file and paste it in in your CA certificate sing interface where requested to provide the CSR.

8. Receive the CA signed certificate.

The CA may return the signed certificate in different formats.

It can return a base-64 encoded ASCII representation of the certificate (with a `.pem` or `.arm` extension) or it may return the certificate in a PKCS7 format with a `.p7b` extension.

Regardless of the format you must import the signed certificate as follow:

- a. When you receive the signed certificate, select Receive.
  - b. Browse to your `cert.arm` signed file or your `file.p7b` file.
  - c. Click OK.
9. Save and overwrite the file. Enter the password when you are prompted.

The `.p12` (or `.jks`) file is updated with the signed certificate and with the root and intermediate certificate if present in the `.p7b` file.



**Note:** The key store contains the private key for the certificate, and this must be always kept secure. It is recommended that the original copy of the keystore is stored in a secure disk, for example an encrypted USB storage device or similar. Keeping a secure backup of the original keystore is also recommended.

## Truststore configuration

The Remote Control server holds the truststore that is used for verifying the broker certificates.

This truststore is provided to the controller system when a remote control broker session is initiated. It is sent also to the target system after the target contacts the server. The certificates that are contained in the truststore are not generated by the server. They are imported into the truststore by an administrator.

You can carry out the following actions on the certificates:

- Add a certificate to the truststore
- View the certificates in the truststore
- Edit the certificates
- Delete certificates



**Note:** The truststore received in the response from the server is stored on the target in the directory that is defined in the **TrustStoreDir** target property.

## Adding a certificate to the truststore

Certificates are used for verifying the remote control connections that are established by using the Internet Connection Broker. You must add the certificates to the truststore on the remote control server.

If you are using self-signed certificates, you must extract the certificate from the keystore file. For more information about extracting the certificate, see [Extracting the certificate from the keystore \(on page 330\)](#). If you are using a CA certificate, you are required only to add the root certificate to the server.

You can add a certificate to the truststore by completing the following steps:

1. Log on to the Remote Control server with a valid admin ID and password.
2. Open the certificate file in a text editor. Select the certificate and copy it to the clipboard.  
Select everything, including the BEGIN CERTIFICATE and END CERTIFICATE lines.
3. Select **Admin > New Trusted Certificate**.
4. Paste the certificate data from the clipboard into the **Certificate** field.
5. Click **Submit**.  
The certificate details are shown.
6. Verify that the correct certificate is shown and click **Submit**.

The certificate is added to the server truststore.



**Note:** After you add certificates to the truststore, all targets must be forced to contact the server so that they update their local truststore. Otherwise, the target cannot access those brokers for which it does not have a certificate. If there are any brokers for which the target does have a certificate, it can still use those brokers.



The target automatically updates the truststore during the session and can use the new certificate in the future.

## Viewing certificates in the truststore

After you have added certificates to the truststore, you can view the list of certificates from the Remote Control server UI.

To view the list of certificates in the truststore, select **Admin > All Trusted Certificates**.

The list of certificates is displayed.

## Editing a trusted certificate

After you add certificates to the truststore on the Remote Control, you can edit the certificate details.

To edit a certificate, complete the following steps:

1. Select **Admin > All Trusted Certificates**.
2. Select the relevant certificate.
3. Select **Edit certificate**.
4. Edit the certificate details.
5. Click **Submit**.
6. Verify that the certificate details are correct and click **Submit**.

The certificate details are changed.



**Note:** After you edit certificates in the truststore, all targets must be forced to contact the server so that they update their local truststore. You must make sure that the certificates on the broker also contain the new details. Otherwise, the target cannot access those brokers whose certificate you changed. The target will then automatically update the truststore during the session and can use the new certificate details in the future.

## Deleting a trusted certificate

You can remove certificates from the truststore on the Remote Control server when they are no longer required.

To delete one or more certificates, complete the following steps:

1. Select **Admin > All Trusted Certificates**.
2. Select the relevant certificate.
3. Click **Delete certificate**.
4. Click **Submit** on the **Confirm Deletion** screen.

The certificates are deleted from the truststore.

## Chapter 30. Migrating to a new certificate

If your existing certificates are due to expire, you can create new certificates. Distribute the new certificates to the relevant endpoints so that they can continue to successfully establish remote control sessions through the broker.

Migrating to a new certificate is required when you are using self-signed certificates and you enable the **broker.trusted.certs.required** property in the `trc.properties` file. For more information about signed certificates, see [Strict Certificate Verification on Broker Connections \(on page 330\)](#).

When you are using CA signed certificates, only the root certificate must be in the server truststore. Root certificates typically have a long lifespan, with typical current CA certificates not expiring until after 10 or 20 years at the time of writing. The SSL certificates signed by the CA usually expire after one year. However, you must update only the SSL certificate on the broker. There is no need to update the truststore on all of the endpoints if any of the following conditions are true.

- The new SSL certificates for the broker are issued by the same CA.
- The root certificate for the CA is already in the truststore on the server and it has been passed to all of your endpoints,

Create your self-signed certificate and distribute it to all the endpoints before you install it on the broker. To migrate to a new certificate, complete the following steps:

1. Generate the new certificate before the old certificate expires.  
For more information about creating a certificate, see [Creating a self signed certificate \(on page 327\)](#). When to do this is determined by how long, you think it takes to update the endpoints with the new certificate. Leave the broker running with the old certificate until just before the expiration date.
2. Add the new certificate to the truststore on the server.  
For more information about adding a certificate, see [Adding a certificate to the truststore \(on page 333\)](#).
  - Targets that call home from inside the intranet automatically receive the new certificate from the server and update their truststore.
  - Targets that successfully start a session through a broker also automatically update the truststore. Therefore, the broker must continue running with the old certificate because the target trusts this certificate. The target does not yet trust the new certificate, and therefore would be unable to start a session through the broker.
3. Install the new certificate on the broker before the old certificate expires,  
For more information about installing a certificate, see [Configuring the keystore on the broker \(on page 329\)](#).
4. Remove the old certificate from the truststore after it expires.

When the old certificate expires, all targets that updated their truststore, can establish a remote control session by using the broker.

# Chapter 31. Configuring the session connection code

You can define the number of characters required and the timeout value, for the connection code used when starting a remote control session through a broker.

When starting a remote control session involving one or more brokers, a connection code is required as part of the session authentication to match the correct controller with the correct target. For more information on starting a remote control session using a broker, see the *BigFix® Remote Control Controller User's Guide*. You can globally configure properties for this code within the Remote Control server UI. To configure the broker session connection code complete the following steps

1. Select **Admin > Edit properties file**
2. Select **trc.properties**
3. Set the connection code length.

### **broker.code.length**

Determines the number of characters required to be entered for the connection code, in the connection code window, when starting a remote control session through an Internet Connection Broker. Default is 7.



**Note:** There is no limit to the number of characters that can be set however you should use your own discretion when setting this value.

4. Set the connection code timeout value

### **broker.code.timeout**

Determines the number of seconds the connection code timer will count down from, for the connection code options available when you are starting a broker session as a controller user. Default is 900.

5. Click **Submit**

You should reset the application in order for the new values to take effect by clicking **Admin > Reset Application**.



# Chapter 32. Target registration before a remote control session

When you have targets that are on the internet or third-party networks and cannot register directly with the Remote Control server you can configure server properties to allow the target to register with the server. When the target registers, you can start a remote control session with the target, by using a broker.

You can also configure the target properties to assign the target to specific target groups when it registers with the server.

## Server properties

Use the server property **rc.create.assets.from.brokers** to determine whether targets can register with the remote control server when the target user enters the connection code at the start of the remote control session. For details about starting a remote control session by using a broker, see the *BigFix® Remote Control Controller User's Guide*.

The **rc.create.assets.from.brokers** property is defined in the `trc.properties` file and is set to **true** by default. For details of the `trc.properties` file see, [trc.properties \(on page 216\)](#).

### **rc.create.assets.from.brokers**

#### **true**

Targets can register with the server at the start of a broker remote control session. When they register, they are assigned to the **DefaultTargetGroup** by default.

#### **false**

Targets cannot register with the server.

## Target properties

The following target property values must be set to allow the target to register with the server.

- **Managed** = Yes
- **ServerURL** = the host name or IP address of the server that you want the target to register with.
- **BrokerList** = 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`.



**Note:** You must restart the target service when you change target property values so that the new values take effect.

For more information about how to assign targets to target groups, see [Assign targets to target groups \(on page 67\)](#).

## Assigning targets to target groups when they register

You can assign the target to other target groups when it registers, instead of the **DefaultTargetGroup**, in two ways.

### Using the target group override option.

Set the **allow.target.group.override** property to true to assign the target to the groups listed in the **GroupLabel** target property, instead of the **DefaultTargetGroup**.

1. Edit the `trc.properties` file and set `allow.target.group.override = true`.
2. Save the file.
3. Edit the target properties and set **GroupLabel** to a list of target groups.



**Note:** These groups must already be defined in the server.

The target is assigned to the target groups listed in **GroupLabel**, when it registers.

#### **Using target membership rules.**

Using the **target membership rules** function, create rules that the targets match on to assign them to specific target groups.

If you define rules and the target group override function is also enabled, the target is assigned to the target groups that are defined for both of these options when it registers.

There can be cases where the remote control session cannot start for the following reasons.

- The target was not assigned to any groups.
- The group assignment configuration is incorrect.
- The target is assigned to a group that the controller user does not have permissions to access targets from.

In all cases, no policies can be derived for the session, so even though the target is registered in the server, the session is rejected.

# Chapter 33. Configure target properties

When a target takes part in a peer to peer remote control session, its properties determine what functions are available during the session. Target properties can be configured by creating and running a target configuration task in the BigFix® console. For more information, see the *BigFix® Remote Control Console User's Guide*. You can also edit the target properties manually. To edit the target properties, you must have administrator rights. Enter your admin password when you are prompted.

## Editing the target properties on a Windows™ target

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.

## Editing the target properties on a Linux™ target

1. Edit the `trc_target.properties` file.
2. Modify the required properties.
3. Save the file.
4. Restart the target service.

## Editing the target properties on an BigFix® Remote Control Target for macOS

To edit the target properties, 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`

After you modify properties, you can type the following command to see a list of current property values.

```
defaults read com.bigfix.remotecontrol.target.plist
```

You do not need administrator rights to run the read command. Therefore, sudo is not required at the start of the read command.

## Specifying a target IP address for connecting to the server

When a target has multiple IP addresses, use the target property, **LocalIPInterface**, to specify which IP address should be used by the target for remote control sessions and for reporting to the server.

### Specifying an IP address for a windows target

Use the, **LocalIPInterface**, property to specify the IP address that the Windows target will use for connecting to the Remote Control server.

Modify this parameter within the Windows® registry by completing the following steps:

1. At a command prompt type `regedit`.
2. Navigate to `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Remote Control\Target`
3. Right-click **LocalIPInterface** and select **Modify**.
4. Enter the required IP address in the **Value data** field and click **OK**.
5. Restart the target service.

The windows target will use the defined IP address for remote control sessions and for reporting to the Remote Control server.

### Specifying an IP address for a Linux target

Use the, **LocalIPInterface**, property to specify the IP address that the Linux target will use for connecting to the Remote Control server.

Modify this parameter within the Remote Control Linux target configuration file by completing the following steps

1. Edit the `trc_target.properties` file
2. Set the value of **LocalIPInterface** to the required IP address and save the file.
3. Restart the target service.

## Joining or Disconnecting a session

You can configure peer to peer targets so that a controller user can join or disconnect the remote control session that the target is already connected to. For more details of how to use these function see the *BigFix® Remote Control Controller User's Guide*. Configure the following target properties to enable these features.

### Join the session

- Managed = No
- CheckUserLogin=Yes



**Note:** Collaboration should also be started for the join feature to be enabled.

### Disconnect the session

- Managed = No
- CheckUserLogin=Yes
- AllowForceDisconnect = Yes

#### **AllowForceDisconnect**

##### **Set to Yes**

A **Disconnect session** button is available in the message window that is displayed when you attempt to connect to the target.

##### **Set to No**

No **Disconnect session** button is available when you attempt to connect to the target.

**CheckUserLogin** must be set to Yes and **Managed** set to No for **AllowForceDisconnect** to take effect.

#### **ForceDisconnectTimeout**

Number of seconds you must wait for the current controller to respond to the prompt to disconnect the current session. If they do not respond in the given time, they will be automatically disconnected from the session . The timer takes effect only when **AllowForceDisconnect** and **CheckUserLogin** are set to Yes. The default value is 45.

## Logging target activity

Use properties to determine how much information and what type of information is written to the target log.

Target session activity is saved to the target log files. Use properties to configure the logging level and how often the target log file is renewed. When you install the target by using the installer, the properties are configured with default values that produce a log file at *Info* level. You can configure the properties when you run a custom installation of the target. For more information, see the *BigFix® Remote Control Installation Guide*. You can also configure the properties

after you install the target. For more information about how to edit target properties, see [Configure target properties \(on page 339\)](#).

Configure the following properties.

**LogLevel**

The log level determines the types of entries and how much information is added to the log file. Default value is 2.

**LogRotation**

Controls the period after which an older log file is overwritten. Log rotation can be disabled. Default value is Weekly.

**LogRollover**

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.

For more information about the properties, see [Properties for configuring logging activity \(on page 425\)](#)

# Chapter 34. Importing data from other sources

As well as adding user and target data to the database using the server UI you can also import this data into the database either through synchronizing with an LDAP server or by importing a text file.

## 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 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.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 (x86)\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 \(on page 163\)](#).

#### **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://myldapservers.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_authentication=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
```

### **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

sAMAccount 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 user's 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.

#### **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://myldapsrver**

# 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**

## Import data from csv files into the Remote Control database

Use comma-separated text files to import numerous records of information into the Remote Control database instead of adding the records individually. Using these files with *import templates*, that are used to map the data in your file to the relevant columns in the database tables. You can import the data into the database in one go. For example, multiple users details can be imported into the database from a csv file rather than having to be entered individually.

To import data from a csv file, complete the following procedures.

- Create a csv file
- Create an import template
- Import the csv file by using an import template

### Creating a csv file

You can create a csv file to list the details of the various items to be imported. These files can be created and saved as type CSV or TSV, with or without a header row, which is a set of column headings corresponding to specific column names within the tables in the database. Each row of the file should have the information, that is added to each column in the database table, separated by a comma for a CSV file or tab for a TSV file.

Below is an example of the content of a CSV file with a header included

```
FORENAME,SURNAME,EMAIL
```

```
Fred,Bloggs,Fbloggs@example.com
```

```
John,Smith,JSmith@example.com
```

```
David,Brown,DBrown@example.com
```

```
Mary,Smith,MSmith@example.com
```

Below is an example of the content of a CSV file with no header

```
Fred,Bloggs,Fbloggs@example.com
```

```
John,Smith,JSmith@example.com
```

```
David,Brown,DBrown@example.com
```

```
Mary,Smith,MSmith@example.com
```



When you have created your csv file, map this data to the Remote Control database using a template that will import the data into the correct tables in the database.

## Mapping data in a csv file to the Remote Control database.

To ensure that the data in your csv file is added to the correct tables in the database, you must map the columns in your file to specific columns and tables. Create an import template to import the data. Use the template to define the correct format to be used for reading your file. You can select which columns of data in your file are to be added to the database and where the data is added to in the database. If the data that you are adding does not refer to an item already in the database, you can create a new item in the database. For example, if you are adding user data and the user data is not already in the database, select to create a new user with the data. A knowledge of the database tables and their structure is important for creating import templates. For more information about the database tables, see [Database table and column descriptions \(on page 366\)](#).



**Note:** When user or target data is being imported, you must supply at least one of the following columns for import from the csv file

### Targets

From the ASSET table, **SERIAL\_NO**, **UUID**, or **COMPUTERNAME**.

### Users

From the USERS table, **USERID**, **EMAIL**, or **EMPLOYEEID**.



**Note:** **USERKEY** is not the same as **USERID**, it is **USERID** that must be used.

To create a new Import Template, complete the following steps:

1. Click **Admin > Import Data > Create new import template**.  
The **Edit Data Import Template** screen is displayed.
2. Type the relevant information.

### Name

Type a name for your template.

### File Header

This field is used if the file that you are importing has a set of column headings that correspond to specific database table column names. Type a comma-separated set of column names. If there is no header in the file, this field is left blank.

for example: `USERID, FORENAME, SURNAME`

### Number of Columns

Type the number of columns of data that is in your csv file. If you decide to change this value, click **Update** to change the numbers that are shown in the Column Number list.



**Note:** If you click **Update** after you select the file encoding, you must check that the required encoding is still selected. If it is not, select the encoding value.

### File Delimiter

Type the character that separates the columns in the file.

```
for example: , or
```

### File Encoding

Used to select the file encoding that applies to your CSV file so that it can be interpreted correctly. Choose the appropriate method for selecting the file encoding.

- Select the required file encoding from the list.
- Type in all or part of the file encoding name and click **Search**.
- Leave the field with no selection and the ASCII UTF-8 file encoding is used.

### Date Format

If you require dates to be imported, follow the instructions on screen for determining the format.

### Create Assets?

#### **true**

If the data that you are importing applies to a target that is not already in the ASSET table, create a target. The ASSET table contains the details of already registered targets.

#### **false**

If the data that you are importing applies to a target that is not already in the ASSET table, do not import the data into the database.

### Create Users?

#### **true**

If the data that you are importing applies to a user that is not already in the database, create a user.

#### **false**

If the data that you are importing applies to a user that is not already in the database, do not import the data into the database.

### Column Number / Table / Column

The list of input fields under the column headings are used to determine where the data in your import file is placed in the database. Follow the on screen instructions for the database column types that must be specified for importing target and user data.

- From the **Column Number** list, select the number of the column in your file that contains the data to import.
- Click the ? icon next to the **Table** field.
- Select the relevant table from the tables list.
- Select the relevant column from the column list.
- Click **OK**
- Repeat these steps for each column in the file that you are importing.



**Note:** Select only the columns that you want to import the data for, you do not have to import every column.

For example: If your file contained the following data

```
USERID, FORENAME, SURNAME, LOCATION
awilson, Alan, Wilson, Greenock
```

and you only wanted to import the FORENAME and LOCATION  
you would select only 2 and 4 for Column Number.

### Test Browse

You can use this function to check that a test csv file, similar to the one to be uploaded, is correctly read and mapped by the import template. The result of the test shows whether the columns and header are mapped and read correctly and if the chosen file encoding reads the characters correctly.

To use this function, complete the following steps:

- Create a test csv file similar in layout to the file to be uploaded, including the header if your file has one.
- Click **Browse** and select the test csv file.
- Click **Test**.
- The results of the test are shown in a new window and provide the following details.
  - If you include a header in your file, a message about the header is shown.
  - A table that shows the database columns that are defined for each column in the file.
  - The data that is mapped from the csv file.

From the results, you can see whether the import template handles the data correctly. If not, you can change the template before you save it.



**Note:**



- i. You have not imported any data at this stage. Complete step 3 ([on page 364](#)) to save the import template.
- ii. Check that the required encoding is still selected. If not, select the encoding before you save the template.

3. On the **Edit Data Import Template** screen click **Submit**

The import template is created. Use the template to import a csv file and map the data in the csv file correctly to the relevant tables in the database. For more information about importing a csv file, see [Importing a csv file \(on page 365\)](#).

## Viewing the list of defined Import Templates

When you have created import templates you can view the list of all templates that have been defined. To view the list of defined import templates click **Admin > Import Data > All templates**.

The **Show all import templates** screen is displayed.

## Changing the details of an Import Template

After you have created an import template you can update or change any of the information defined for it. For example you may wish to change its name or add another column to be imported. To change the details for an import template complete the following steps :

1. Click **Admin > Import Data > All Templates**
2. Select the required email template.
3. From the **Admin** menu OR from the **Action list** select **Edit selected template**  
The Edit Data Import Template screen is displayed
4. Make the required changes



**Note:** If you click the update button after you have selected the file encoding, you will need to check that the required encoding is still selected, if not re select the encoding.

5. Click **Submit**

The details for the selected import template are updated.

## Deleting Import Templates

You can delete any import templates that you no longer need.

To delete an import template complete the following steps :

1. Click **Admin > Import Data > All Templates**
2. Select the required email templates
3. From the **Admin** menu OR from the **Action list** select **Delete Selected templates**

The selected import template is removed and is no longer listed in the **All Templates** report.

## Importing a csv file

After you have created a csv file and an import template, you can use the import file function to add the data from your file into the Remote Control database. This is useful for adding numerous records of data to the database at once instead of having to add the items individually.

To add the data into the database, complete the following steps :

1. Click **Admin > Import Data > Import File.**

The **Import Existing Data** screen is displayed

2. Choose the appropriate method for selecting your csv file.

- a. Click **Browse** to navigate to and select the required csv file.

- b. Type in the path and name of the file that you wish to import

for example : `c:\myfiles\test.csv` on Windows™ systems

`/myfiles/test.csv` on UNIX®-based systems

3. If your file has no header row, select an import template from the list that will be used to map your data to the relevant database table.



**Note:** If your file has a header in it, it will match automatically with a defined template and therefore no selection is required.

4. Click **Submit**

The message `File has been queued for processing` is displayed

Your data is added to the database. You can check this by displaying the relevant report for this data. For example if you have added user data, you can use the **All users** report to check that the data has been added correctly.

# Chapter 35. Database table and column descriptions

The BigFix® Remote Control Server program comes with a built-in database. By default, the database provides several tables that contain a variety of target and user information. Understanding the information provided with this database can help you perform advanced functions such as creating a custom report. Although you will primarily need to understand tables with target and user information, internal system table information is also included here.

The following information is provided to help you understand the overall structure of the built-in database and to help you understand how information is divided into each table.



**Note:** Some of the tables described in this section are not used by the current version of Remote Control and are considered deprecated. They might be removed in future versions of the product.

## ASSET schema tables

Table 20. ACCESSREQUEST table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ACCESSREQUEST	ACCESSREQUESTKEY	INTEGER	4	No
	ADMINNOTES	VARCHAR	500	Yes
	ANONYMOUS	INTEGER	4	Yes
	ASSETGROUPKEY	INTEGER	4	Yes
	CREATED	TIMESTAMP	10	No
	EMAIL	VARCHAR	256	Yes
	EXPIRED	INTEGER	4	Yes
	GRANTEND	TIMESTAMP	10	Yes
	GRANTSTART	TIMESTAMP	10	Yes
	PASSKEY	VARCHAR	128	Yes
	REQUESTEND	TIMESTAMP	10	Yes
	REQUESTNOTES	VARCHAR	500	Yes
	REQUESTSTART	TIMESTAMP	10	Yes
	REQUESTTYPE	INTEGER	4	Yes
	STATUS	INTEGER	4	Yes
	USERGROUPKEY	INTEGER	4	Yes
	USERKEY	INTEGER	4	Yes

Table 21. ACCESSREQUESTTARGETS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ACCESSREQUESTTARGETS	ACCESSREQUESTKEY	INTEGER	4	No
	CREATED	TIMESTAMP	10	Yes
	HWKEY	INTEGER	4	Yes
	TARGETGROUPKEY	INTEGER	4	No

Table 22. ASSET table - Main Target table for storing the majority of the Target information

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET	HWKEY	INTEGER	4	No
	MAX_REVISION	INTEGER	4	No
	MAX_PROCESSED_REVISION	INTEGER	4	No
	IS_PC_ASSET	CHARACTER	1	No
	USERKEY	INTEGER	4	No
	UUID	VARCHAR	32	Yes
	SERIAL_NO	VARCHAR	64	No
	MANUFACTURER	VARCHAR	64	Yes
	MODEL	VARCHAR	64	Yes
	COMPUTERNAME	VARCHAR	64	Yes
	CUR_USER	VARCHAR	64	Yes
	ENCLOSURE	VARCHAR	64	Yes
	DOMAIN_NAME	VARCHAR	64	Yes
	MAC_ADDRESSES	VARCHAR	128	Yes
	IP_ADDRESSES	VARCHAR	64	Yes
	DATE_TIME	TIMESTAMP	10	No
	FIRST_OWNED_DATE	TIMESTAMP	10	Yes
	IS_LPAR	INTEGER	4	No
	PARENT_HWKEY	INTEGER	4	No
	TOKENDATA	VARCHAR	64	Yes



**Note:** This table may be removed in future releases.

**Table 23. ASSET\_AUTHENTICATION\_KEY table**

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET_AUTHENTICATION_KEY	HWKEY	INTEGER	4	No
	KEY_TYPE	INTEGER	4	No
	UNIQUE_KEY	VARCHAR	50	Yes
	CREATED	TIMESTAMP	10	No

**Table 24. ASSET\_INFO table - Table for storing additional Asset information. Holds the full demographic information and 9 custom fields**

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET_INFO	HWKEY	INTEGER	4	No
	DESCRIPTION	VARCHAR	30	Yes
	COMPANY	VARCHAR	40	Yes
	LOCATION	VARCHAR	60	Yes
	DEPARTMENT	VARCHAR	30	Yes
	FLOOR	VARCHAR	40	Yes
	ROOM	VARCHAR	40	Yes
	ADDRESS_1	VARCHAR	50	Yes
	ADDRESS_2	VARCHAR	50	Yes
	TOWN	VARCHAR	40	Yes
	POSTCODE	VARCHAR	10	Yes
	COUNTRY	VARCHAR	25	Yes
	STATE	VARCHAR	25	Yes
	ASSETTAG	VARCHAR	30	Yes
	ASSETTYPE	VARCHAR	30	Yes
	STATUS	VARCHAR	30	Yes
	DESK	VARCHAR	8	Yes
	CUSTOM1	VARCHAR	250	Yes
	CUSTOM2	VARCHAR	250	Yes
	CUSTOM3	VARCHAR	250	Yes
CUSTOM4	VARCHAR	250	Yes	
CUSTOM5	VARCHAR	250	Yes	
CUSTOM6	VARCHAR	250	Yes	
CUSTOM7	VARCHAR	250	Yes	



Table 24. ASSET\_INFO table - Table for storing additional Asset information. Holds the full demographic information and 9 custom fields (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	CUSTOM8	VARCHAR	250	Yes
	CUSTOM9	VARCHAR	250	Yes
	INSTALLED_DATE	TIMESTAMP	10	Yes
	CATEGORY	VARCHAR	64	Yes
	IBM_OWNED	VARCHAR	1	Yes
	IBM_ASSETTAG	VARCHAR	30	Yes
	USER_VERIFIED	VARCHAR	10	Yes
	STATUS_DATE	TIMESTAMP	10	Yes
	LAST_INSPECTION_DATE	TIMESTAMP	10	Yes



**Note:** This table may be removed in future releases.

Table 25. ASSET\_OWNED table - Table for storing Asset purchase information

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET_OWNED	HWKEY	INTEGER	4	No
	PURCHASE_DATE	TIMESTAMP	10	Yes
	INITIAL_VALUE	DECIMAL	5	No
	DEPRECIATION_PERIOD	INTEGER	4	Yes
	PURCHASER	VARCHAR	50	Yes
	SUPPLIER	VARCHAR	50	Yes
	PO_NO	VARCHAR	50	Yes
	WARRANTY_EXPIRY	TIMESTAMP	10	Yes



**Note:** This table may be removed in future releases.

Table 26. CALLED\_HOME table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CALLED_HOME	HWKEY	INTEGER	4	No
	UUID	VARCHAR	32	Yes
	SERIAL_NO	VARCHAR	64	Yes

Table 26. CALLED\_HOME table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	MANUFACTURER	VARCHAR	64	Yes
	MODEL	VARCHAR	64	Yes
	COMPUTERNAME	VARCHAR	64	Yes
	IP_ADDRESS	VARCHAR	15	Yes
	MAC_ADDRESS	VARCHAR	128	Yes
	SUBNET	VARCHAR	15	Yes
	FIRST_CALLHOME	TIMESTAMP	10	No
	LAST_CALLHOME	TIMESTAMP	10	No
	HWCRC	VARCHAR	8	Yes
	SWCRC	VARCHAR	8	Yes



**Note:** This table may be removed in future releases.

Table 27. CHAT\_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CHAT_LOG	CHATKEY	BIGINT	8	No
	USERKEY	INTEGER	4	No
	MSG_DATA	VARCHAR	512	Yes
	DATE_TIME	TIMESTAMP	10	No



**Note:** This table may be removed in future releases.

Table 28. CURRENT\_IPADDRESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CURRENT_IPADDRESS	HWKEY	INTEGER	4	No
	IPADDRESS	VARCHAR	15	Yes
	LAST_UPDATED	TIMESTAMP	10	No

Table 29. EMAIL\_TEMPLATE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
EMAIL_TEMPLATE	EMAILKEY	VARCHAR	4	No
	LOCALE	VARCHAR	5	No
	NAME	VARCHAR	100	No
	DESCRIPTION	VARCHAR	400@	Yes
	EMAIL_FROM	VARCHAR	70	Yes
	TITLE	VARCHAR	240	Yes
	CONTENT	VARCHAR	3000	No
	CREATOR	VARCHAR	20	Yes
	CREATED	TIMESTAMP	10	No

Table 30. IMPORT\_TEMPLATE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
IMPORT_TEMPLATE	IMPORTKEY	INTEGER	4	No
	NAME	VARCHAR	55	No
	ENCODING	VARCHAR	20	Yes
	HEADER	VARCHAR	100	No
	COLS	INTEGER	4	No
	DELIMITER	VARCHAR	10	No
	REVISION_HANDLER	INTEGER	4	No
	APPEND_HANDLER	INTEGER	4	No
	CREATE_ASSETS	INTEGER	4	No
	CREATE_USERS	INTEGER	4	No

Table 31. IMPORT\_TEMPLATE\_COLS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
IMPORT_TEMPLATE_COLS	IMPORTKEY	INTEGER	4	No
	COL_NO	INTEGER	4	No
	TABLE_NAME	VARCHAR	20	No
	COL_NAME	VARCHAR	30	No
	UPDATE_COL	SMALLINT	2	No
	ASSET_FIELD	SMALLINT	2	No

Table 31. IMPORT\_TEMPLATE\_COLS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	LPAR_FIELD	SMALLINT	2	No

Table 32. MEMBERSHIP\_RULES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MEMBERSHIP_RULES	RULEKEY	INTEGER	4	No
	PRIORITY	INTEGER	1	No
	CREATED	TIMESTAMP	10	No
	CREATED_BY	VARCHAR	4	No
	LAST_MODIFIED	TIMESTAMP	10	No
	LAST_MODIFIED_BY	INTEGER	4	No
	STOP_PROCESSING	CHAR	1	No
	IP_RANGE_START	VARCHAR	39	No
	IP_RANGE_END	VARCHAR	39	No
	COMPUTER_NAME	VARCHAR	512	No
	COMMENT	VARCHAR	1024	No

Table 33. MEMBERSHIP\_RULES\_GROUPS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MEMBERSHIP_RULES_GROUPS	MRGKEY	INTEGER	4	No
	RULEKEY	INTEGER	4	No



**Note:** This table may be removed in future releases.

Table 34. NET\_ADAPTERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
NET_ADAPTERS	HWKEY	INTEGER	4	No
	REVISION	INTEGER	4	No
	DEVICE_ID	VARCHAR	50	Yes
	NAME	VARCHAR	100	Yes
	TYPE	VARCHAR	50	Yes
	DESCRIPTION	VARCHAR	150	Yes

Table 34. NET\_ADAPTERS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	MAC_ADDRESS	VARCHAR	20	Yes
	MANUFACTURER	VARCHAR	50	Yes
	SERVICENAME	VARCHAR	50	Yes



**Note:** This table may be removed in future releases.

Table 35. QUEUE\_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUEUE_LOG	EVENT_ID	INTEGER	4	No
	DESCRIPTION	VARCHAR	256	Yes
	PROCESS_TIME_MS	BIGINT	8	No
	HIGH_PRIORITY	INTEGER	4	No
	DATE_TIME	TIMESTAMP	10	Yes

Table 36. RC\_GATEWAYS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
RC_GATEWAYS	GATEWAY.KEY	INTEGER	4	No
	HOSTNAME	VARCHAR	256	Yes
	CONNECTIVITY	VARCHAR	512	Yes
	DESCRIPTION	VARCHAR	256	Yes

Table 37. RC\_BROKERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
RC_BROKERS	BROKERKEY	INTEGER	4	No
	HOSTNAME	VARCHAR	256	No
	PORT	INTEGER	4	No
	DESCRIPTION	VARCHAR	256	Yes

Table 38. REGTOKEN table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
REGTOKEN	REGTOKENKEY	INTEGER	4	No

Table 38. REGTOKEN table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	USERKEY	INTEGER	4	No
	TOKENDATA	VARCHAR	256	No
	DESCRIPTION	VARCHAR	256	Yes
	VALIDFROM	TIMESTAMP	10	No
	VALIDTO	TIMESTAMP	10	No
	CREATED	TIMESTAMP	10	No

Table 39. REVISIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
REVISIONS	HWKEY	INTEGER	4	No
	REVISION	INTEGER	4	No
	PROCESSED	CHARACTER	1	No
	DATE_TIME	TIMESTAMP	10	No

Table 40. SERVER\_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SERVER_LOG	EVENT_ID	INTEGER	4	No
	DESCRIPTION	VARCHAR	176	Yes
	DATE_TIME	TIMESTAMP	10	No

Table 41. TASK table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TASK	TASKKEY	INTEGER	4	No
	TYPE	VARCHAR	30	No
	NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	255	Yes
	SCHEDULED	INTEGER	4	No
	MENU	VARCHAR	50	Yes
	ACTIVE	INTEGER	4	No
	RUNONCE	INTEGER	4	No
	START_DATE	TIMESTAMP	10	Yes

Table 41. TASK table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	END_DATE	TIMESTAMP	10	Yes
	PERIOD	INTEGER	4	No
	USER_QUERY	INTEGER	4	No
	USERLIST	VARCHAR	100	Yes
	QUERY	INTEGER	4	No
	QUERY2	INTEGER	4	No
	QUERY3	INTEGER	4	No
	QUERY4	INTEGER	4	No
	CUSTOM_QUERY	INTEGER	4	No
	CUSTOM_QUERY2	INTEGER	4	No
	MAIL_TEMPLATE	INTEGER	4	Yes
	SUBREPORT	INTEGER	4	No
	NEXT_TASKKEY	INTEGER	4	No
	CREATOR	VARCHAR	20	Yes
	CREATED	TIMESTAMP	10	No

Table 42. TASK\_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TASK_LOG	TASKKEY	INTEGER	4	No
	USERKEY	INTEGER	4	Yes
	USER_LIST	VARCHAR	2000	Yes
	USER_COMMENT	VARCHAR	200	Yes
	DATE_TIME	TIMESTAMP	10	Yes

Table 43. TASK\_SELECTED table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TASK_SELECTED	TASKKEY	INTEGER	4	No
	MENU_NAME	VARCHAR	50	Yes
	DESCRIPTION	VARCHAR	250	Yes



**Note:** This table may be removed in future releases.

Table 44. TRANSFERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TRANSFERS	HWKEY	INTEGER	4	No
	IS_PC_ASSET	CHARACTER	1	No
	OLD_USERKEY	INTEGER	4	No
	NEW_USERKEY	INTEGER	4	No
	APPROVED	CHARACTER	1	No
	USER_COMMENT	VARCHAR	30	No
	REASON	VARCHAR	30	Yes
	CREATED	TIMESTAMP	10	No
	PROCESSED	TIMESTAMP	10	Yes

Table 45. TX\_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TX_LOG	USERKEY	INTEGER	4	No
	HWKEY	INTEGER	4	Yes
	TX_ID	INTEGER	4	No
	TX_DATA	VARCHAR	500	No
	TABLE_COLUMN	VARCHAR	128	Yes
	OLD_VALUE	VARCHAR	128	Yes
	NEW_VALUE	VARCHAR	128	Yes
	TX_TIME	INTEGER	4	Yes
	DATE_TIME	TIMESTAMP	10	No



**Note:** This table may be removed in future releases.

Table 46. XML\_LOOKUP table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
XML_LOOKUP	SCHEMA_NAME	VARCHAR	64	No
	TABLE_NAME	VARCHAR	64	No
	COLUMN_NAME	VARCHAR	64	No



Table 46. XML\_LOOKUP table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	TEXT	INTEGER	4	No
	FILETYPE	VARCHAR	20	No
	VERSION	VARCHAR	20	No
	PARENT_XPATH	VARCHAR	255	Yes
	XPATH	VARCHAR	255	Yes
	DEFAULT_VALUE	VARCHAR	255	Yes
	NODETYPE	VARCHAR	10	No
	ISKEY	CHARACTER	1	Yes
	PROBE_SET	INTEGER	4	No
	PRIORITY	INTEGER	4	No

## COMMON schema tables

Table 47. ACTIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
<b>ACTIONS</b>	ACTIONKEY	INTEGER	4	No
	ACTION_GROUP_ID	INTEGER	4	Yes
	ACTION_INTERNAL_NAME	VARCHAR	100	No
	ACTIONNAME	VARCHAR	100	No
	ACTIONDESC	VARCHAR	1024	Yes
	ACTION_LABEL_PROP	VARCHAR	100	Yes
	ACTION_TYPE	INTEGER	4	Yes

Table 48. ASSETPERMISSIONSDEFAULT table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
<b>ASSETPERMISSIONSDEFAULT</b>	ASSETPERMDEFKEY	INTEGER	4	No
	ACTIONKEY	INTEGER	4	No
	ACTIONSTATE	INTEGER	4	Yes
	INT_VALUE	INTEGER	4	Yes
	STR_VALUE	VARCHAR	255	Yes

Table 49. ASSETPERMISSIONSDEFAULTNAME table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSETPERMISSIONSDEFAULTNAME	ASSETPERMDEFKEY	INTEGER	4	No
	DEFDESC	VARCHAR	1024	Yes

Table 50. CACHE\_GROUPASSET table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CACHE_GROUPASSET	HWKEY	INTEGER	4	No
	GAKEYS	VARCHAR	128	Yes
	EXPIRES	TIMESTAMP	10	Yes

Table 51. CACHE\_GROUPUSER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CACHE_GROUPUSER	USERKEY	INTEGER	4	No
	GUKEYS	VARCHAR	128	Yes
	EXPIRES	TIMESTAMP	10	Yes

Table 52. CONFIGURATION table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CONFIGURATION	NAME	VARCHAR	128	No
	VALUE	VARCHAR	256	Yes

Table 53. CUSTOM\_QUERY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CUSTOM_QUERY	CUSTOM_QUERYKEY	INTEGER	4	No
	NAME	VARCHAR	50	No
	MENU_NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	120	Yes
	SQL_DATA	CLOB	524288	No
	CREATOR	INTEGER	4	Yes
	CREATED	TIMESTAMP	10	No

Table 54. CUSTOM\_QUERY\_GROUP\_ACCESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CUSTOM_QUERY_GROUP_ACCESS	CUSTOM_QUERYKEY	INTEGER	4	No
	GROUPKEY	INTEGER	4	No

Table 55. CUSTOM\_QUERY\_USER\_ACCESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CUSTOM_QUERY_USER_ACCESS	CUSTOM_QUERYKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No

Table 56. FAVOURITES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
FAVOURITES	USERKEY	INTEGER	4	No
	HWKEY	INTEGER	4	No

Table 57. GROUPASSET table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPASSET	GAKEY	INTEGER	4	No
	NAME	VARCHAR	50	Yes
	GADESC	VARCHAR	1024	Yes
	ASSETPERMDEFKEY	INTEGER	4	Yes
	CREATED	TIMESTAMP	10	Yes

Table 58. GROUPASSETGROUPMEMBER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPASSETGROUPMEMBER	GAKEY	INTEGER	4	No
	GAPARENTKEY	INTEGER	4	No

Table 59. GROUPASSETMEMBER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPASSETMEMBER	GAKEY	INTEGER	4	No
	GAPARENTKEY	INTEGER	4	No

Table 60. GROUPATTRIBUTES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPATTRIBUTES	ATT_DEFN	INTEGER	4	No
	GROUPTYPE	INTEGER	4	No
	GROUPKEY	INTEGER	4	No
	STR_VALUE	VARCHAR	255	Yes
	INT_VALUE	INTEGER	4	Yes

Table 61. GROUPATTRIBUTEDEFNS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPATTRIBUTEDEFNS	ATT_DEFN_KEY	INTEGER	4	No
	GROUPTYPE	INTEGER	4	No
	ATT_INTERNAL_NAME	VARCHAR	100	No
	ATT_NAME	VARCHAR	100	No
	ATT_DESC	VARCHAR	1024	Yes
	ATT_LABEL_PROP	VARCHAR	100	Yes
	ATT_DATA_TYPE	INTEGER	4	No
	ATT_RULE	INTEGER	4	No

Table 62. GROUP\_HOMEPAGE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUP_HOMEPAGE	GHKEY	INTEGER	4	No
	GROUPKEY	INTEGER	4	No
	CUSTOM_QUERYKEY	INTEGER	4	Yes
	LAST_UPDATED	TIMESTAMP	10	No

Table 63. GROUPUSERGROUPMEMBER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPUSERGROUPMEMBER	GROUPKEY	INTEGER	4	No
	GUPARENTKEY	INTEGER	4	No

Table 64. GROUP\_MEMBERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUP_MEMBERS	GROUPKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No

Table 65. LIVEPOINTS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
LIVEPOINTS	HWKEY	INTEGER	4	No
	PORT	INTEGER	4	No
	HOSTNAME	VARCHAR	64	Yes
	DOMAIN_NAME	VARCHAR	64	Yes
	CUSTOM1	VARCHAR	128	Yes
	CUSTOM2	VARCHAR	128	Yes
	CUSTOM3	VARCHAR	128	Yes
	IP_ADDRESS	VARCHAR	64	Yes
	LOGGED_USER	VARCHAR	48	Yes
	USER_LANGUAGE	VARCHAR	48	Yes
	OS_NAME	VARCHAR	50	Yes
	OS_LANGUAGE	VARCHAR	48	Yes
	TIMEZONE	VARCHAR	48	Yes
	SCREENSAVER	VARCHAR	300	Yes
	RC_STATE	VARCHAR	128	Yes
	RC_CONTROLLER	VARCHAR	128	Yes
	CUSTOM_REGKEY	VARCHAR	128	Yes
	INT_MODE	VARCHAR	48	Yes
	ENDPOINT_ID	VARCHAR	64	Yes
	TARGET_ID	VARCHAR	64	Yes
LAST_UPDATE	VARCHAR	10	Yes	

Table 66. MENU\_ACTIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MENU_ACTIONS	QUERYKEY	INTEGER	4	No
	MENU	VARCHAR	30	No

Table 66. MENU\_ACTIONS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	NAME	VARCHAR	30	No
	COL1	VARCHAR	60	No
	COL2	VARCHAR	60	No
	COL3	VARCHAR	60	No
	COL4	VARCHAR	60	No
	MENU_ACTION	VARCHAR	150	Yes
	LOGO	VARCHAR	40	Yes
	MULTIPLE	VARCHAR	15	No
	CLICK_TYPE	CHARACTER	1	No
	DESCRIPTION	VARCHAR	200	Yes
	AUTHORITY	CHARACTER	1	No
	AUTH_PROPERTY	VARCHAR	100	Yes

Table 67. MENU\_LINKS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MENU_LINKS	QUERYKEY	INTEGER	4	No
	MENU	VARCHAR	30	No
	COL1	VARCHAR	60	No
	COL2	VARCHAR	60	No
	COL3	VARCHAR	60	No
	COL4	VARCHAR	60	No
	MULTIPLE	VARCHAR	15	Yes
	QUERYKEY2	INTEGER	4	No

Table 68. MENU\_STATIC\_ITEMS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MENU_STATIC_ITEMS	MENUKEY	INTEGER	4	No
	MENU	VARCHAR	30	Yes
	SUB_MENU	VARCHAR	30	Yes
	NAME	VARCHAR	60	No
	MENU_URL	VARCHAR	150	Yes

Table 68. MENU\_STATIC\_ITEMS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	LOGO	VARCHAR	40	Yes
	DESCRIPTION	VARCHAR	200	Yes
	PRIORITY	INTEGER	4	No
	AUTHORITY	CHARACTER	1	No
	AUTH_PROPERTY	VARCHAR	100	Yes
	CONDITIONS	VARCHAR	50	Yes
	CLICK_TYPE	CHARACTER	1	No

Table 69. MENU\_STATIC\_LINKED\_ITEMS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
<b>MENU_STATIC_LINKED_ITEMS</b>	QUERYKEY	INTEGER	4	No
	MENU	VARCHAR	30	No
	MENU_NAME	VARCHAR	30	No
	NAME	VARCHAR	30	No
	COL1	VARCHAR	60	No
	COL2	VARCHAR	60	No
	COL3	VARCHAR	60	No
	COL4	VARCHAR	60	No
	DESCRIPTION	VARCHAR	200	Yes
	AUTHORITY	CHARACTER	1	No
	AUTH_PROPERTY	VARCHAR	100	Yes



**Note:** This table may be removed in future releases.

Table 70. ORGANISATION table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
<b>ORGANISATION</b>	ORGKEY	INTEGER	4	No
	DEPT_ID	VARCHAR	50	No
	NAME	VARCHAR	128	No
	REAL_DEPT	VARCHAR	250	Yes
	REAL_DEPT_ID	VARCHAR	100	Yes

Table 70. ORGANISATION table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	PARENT_ORGKEY	INTEGER	4	No
	PARENT_DEPT_ID	VARCHAR	50	Yes
	OWNER_USERKEY	INTEGER	4	No
	OWNER_EMPLOYEEID	VARCHAR	50	Yes
	"TYPE"	VARCHAR	128	Yes
	ADDRESS_1	VARCHAR	128	Yes
	ADDRESS_2	VARCHAR	128	Yes
	CITY	VARCHAR	128	Yes
	STATE	VARCHAR	128	Yes
	POSTCODE	VARCHAR	10	Yes
	COUNTRY	VARCHAR	128	Yes
	CLOSE_STATUS	SMALLINT	2	No
	OPEN_DATE	TIMESTAMP	10	No
	CLOSE_DATE	TIMESTAMP	10	Yes

Table 71. PASSWORDS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PASSWORDS	USERKEY	INTEGER	4	No
	PASSWORD	VARCHAR	100	No
	UPDATED	TIMESTAMP	10	No

Table 72. PERMISSIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PERMISSIONS	PERMISSIONKEY	INTEGER	4	No
	DEFAULTEXPLICIT	INTEGER	4	No
	GROUPKEY	INTEGER	4	No
	GAKEY	INTEGER	4	Yes
	ACTIONKEY	INTEGER	4	No
	DENYACCEPT	INTEGER	4	No
	START_DATE	TIMESTAMP	10	Yes
	END_DATE	TIMESTAMP	10	Yes



Table 72. PERMISSIONS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	REPEATS	INTEGER	4	Yes
	WEEK_DAYS	VARCHAR	40	Yes
	STR_VALUE	VARCHAR	255	Yes
	INT_VALUE	INTEGER	4	Yes
	LIVE_STATE	INTEGER	4	Yes

Table 73. PERMISSIONSET table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PERMISSIONSET	ACTIONKEY	INTEGER	4	No
	ACTIONSTATE	INTEGER	4	No
	INT_VALUE	INTEGER	4	Yes
	LIVE_STATE	INTEGER	4	Yes
	PRIORITYLEVEL	INTEGER	4	Yes
	SETNAMEKEY	INTEGER	4	Yes
	STR_VALUE	VARCHAR	10	Yes

Table 74. PERMISSIONSETNAMES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PERMISSIONSETNAMES	CREATED	TIMESTAMP	10	No
	SETNAME	VARCHAR	80	Yes
	SETNAMEKEY	INTEGER	4	No

Table 75. QUERY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUERY	QUERYKEY	INTEGER	4	No
	NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	120	Yes
	SQL_DATA	CLOB	524288	No
	FONTSIZE	INTEGER	4	No
	AUTHORITY	CHARACTER	1	No
	DISPLAY	INTEGER	4	No

Table 75. QUERY table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	REFRESH	INTEGER	4	No
	CREATOR	VARCHAR	20	Yes
	CREATED	TIMESTAMP	10	No

Table 76. QUERY\_COL\_INFO table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUERY_COL_INFO	QUERYKEY	INTEGER	4	No
	NAME	VARCHAR	30	No
	DISPLAYCOL	INTEGER	4	No
	DISPLAYDATA	INTEGER	4	No
	"ALIAS"	VARCHAR	30	Yes
	ACTION1	VARCHAR	150	Yes
	ACTION2	VARCHAR	150	Yes
	ACTION3	VARCHAR	150	Yes
	ACTION_LOGO	VARCHAR	20	Yes
	ACTION_LOGO2	VARCHAR	20	Yes
	ACTION_LOGO3	VARCHAR	20	Yes
	ACTION_POPUP	VARCHAR	200	Yes
	ACTION_POPUP2	VARCHAR	200	Yes
	ACTION_POPUP3	VARCHAR	200	Yes
	COLOUR	VARCHAR	10	Yes
	ALIGN	VARCHAR	10	Yes
	SUMMARY	VARCHAR	10	Yes
	POPUP	VARCHAR	200	Yes
	DELETEABLE	INTEGER	4	Yes
	AUTHORITY	CHARACTER	1	No

Table 77. QUERY\_GROUP table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUERY_GROUP	QUERYKEY	INTEGER	4	No
	GROUP_NAME	VARCHAR	50	No

Table 78. REMOTE\_INSTALL table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
REMOTE_INSTALL	INSTALLKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No
	INSTALL_TIME	TIMESTAMP	10	No
	TARGET	VARCHAR	100	No
	TARGET_USER	VARCHAR	40	No
	TARGET_PLATFORM	CHAR	7	No
	TARGET_GROUP	VARCHAR	40	No
	SERVER_URL	VARCHAR	200	No
	LISTENING_PORT	INTEGER	4	No
	INSTALL_FOLDER	VARCHAR	255	No
	TEMP_FOLDER	VARCHAR	255	No
	USE_FIPS	INTEGER	4	No
	ALLOW_P2P	INTEGER	4	No
	ALLOW_P2P_FAILOVER	INTEGER	4	No
	PROXY_ADDRESS	VARCHAR	200	Yes
	PROXY_PORT	INTEGER	4	Yes
	PROXY_USER	VARCHAR	40	Yes
	STATUS	VARCHAR	20	No
ERROR	CLOB	Unlimited	Yes	

Table 79. SESSIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSIONS	SESSIONKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No
	HWKEY	INTEGER	4	No
	REQUEST_TIME	TIMESTAMP	10	Yes
	START_TIME	TIMESTAMP	10	Yes
	END_TIME	TIMESTAMP	10	Yes
	DESCRIPTION	VARCHAR	512	Yes

Table 80. SESSIONS\_ACTIVE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSIONS_ACTIVE	SESSIONKEY	INTEGER	4	No
	SESSION_TOKEN	VARCHAR	265	Yes
	CONTROLLER_NAME	VARCHAR	256	Yes
	HWKEY	INTEGER	4	No
	STATUS	SMALLINT	2	No
	COLLAB_IP	VARCHAR	255	Yes
	COLLAB_PORT	INTEGER	4	Yes

Table 81. SESSION\_AUDIT table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_AUDIT	AUDITEVENTKEY	INTEGER	4	No
	SESSIONKEY	INTEGER	4	No
	LOCALTIMESTAMP	TIMESTAMP	10	Yes
	ORIGINATOR	SMALLINT	2	Yes
	EVENTID	VARCHAR	25	Yes
	ARGUMENT0	VARCHAR	255	Yes
	ARGUMENT1	VARCHAR	255	Yes
	ARGUMENT2	VARCHAR	255	Yes
	ARGUMENT3	VARCHAR	255	Yes
	ARGUMENT4	VARCHAR	255	Yes
	ARGUMENT5	VARCHAR	255	Yes
	ARGUMENT6	VARCHAR	255	Yes
	ARGUMENT7	VARCHAR	255	Yes
	ARGUMENT8	VARCHAR	255	Yes
ARGUMENT9	VARCHAR	255	Yes	

Table 82. SESSION\_BROKER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_BROKER	SESSIONID	VARCHAR	64	No
	REQ_USERID	INTEGER	4	No
	REQ_IP	VARCHAR	64	Yes

Table 82. SESSION\_BROKER table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	TARGET_HWKEY	INTEGER	4	No
	REQ_TIME	TIMESTAMP	10	Yes

Table 83. SESSION\_POLICIES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_POLICIES	SESSIONKEY	INTEGER	4	No
	POLICY_NAME	VARCHAR	25	No
	POLICY_VALUE	VARCHAR	25	Yes

Table 84. SESSION\_RECORDING table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_RECORDING	RECORDINGKEY	INTEGER	4	No
	SESSIONKEY	INTEGER	4	No
	FILENAME	VARCHAR	255	Yes

Table 85. TRANSLATIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TRANSLATIONS	NAME	VARCHAR	48	No
	"LOCALE"	VARCHAR	16	No
	VALUE	VARCHAR	128	No

Table 86. TRUSTED\_CERTS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TRUSTED_CERTS	SUBJECT	VARCHAR	256	No
	PEM_DATA	VARCHAR	1500	No
	CERTKEY	INTEGER	4	No

Table 87. USERPERMISSIONSDEFAULT table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USERPERMISSIONSDEFAULT	USERPERMDEFKEY	INTEGER	4	No
	ACTIONKEY	INTEGER	4	No

Table 87. USERPERMISSIONSDEFAULT table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	ACTIONSTATE	INTEGER	4	Yes
	INT_VALUE	INTEGER	4	Yes
	STR_VALUE	VARCHAR	255	Yes

Table 88. USERPERMISSIONSDEFAULTNAME table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USERPERMISSIONSDEFAULTNAME	USERPERMDEFKEY	INTEGER	4	No
	DEFDESC	VARCHAR	1024	Yes

Table 89. USERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USERS	USERKEY	INTEGER	4	No
	USERID	VARCHAR	70	No
	EMAIL	VARCHAR	70	No
	TITLE	VARCHAR	5	Yes
	FORENAME	VARCHAR	30	Yes
	SURNAME	VARCHAR	30	Yes
	INITIALS	VARCHAR	30	Yes
	NICKNAME	VARCHAR	30	Yes
	COMPANY	VARCHAR	40	Yes
	LOCATION	VARCHAR	60	Yes
	DEPARTMENT	VARCHAR	60	Yes
	FLOOR	VARCHAR	40	Yes
	ROOM	VARCHAR	40	Yes
	TEAM	VARCHAR	60	Yes
	ORG	VARCHAR	60	Yes
	EMPLOYEEID	VARCHAR	30	Yes
	MAILPOINT	VARCHAR	10	Yes
	ADDRESS_1	VARCHAR	100	Yes
	ADDRESS_2	VARCHAR	100	Yes
	TOWN	VARCHAR	40	Yes

Table 89. USERS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	POSTCODE	VARCHAR	10	Yes
	COUNTRY	VARCHAR	25	Yes
	STATE	VARCHAR	25	Yes
	REGION	VARCHAR	25	Yes
	TEL_NO	VARCHAR	25	Yes
	MOB_NO	VARCHAR	25	Yes
	CID	VARCHAR	8	Yes
	BUILDING	VARCHAR	64	Yes
	CITY	VARCHAR	64	Yes
	GEO	VARCHAR	64	Yes
	AUTHORITY	CHARACTER	1	Yes
	COST_CENTRE	VARCHAR	30	Yes
	"LOCALE"	VARCHAR	30	Yes
	PASSWORD	VARCHAR	100	No
	EXPIRED	CHARACTER	1	No
	DEMOGRAPHICS_STALE	INTEGER	4	No
	PASSWORD_CHANGED	TIMESTAMP	10	Yes
	LAST_UPDATE	TIMESTAMP	10	Yes
	CREATED	TIMESTAMP	10	No
	ASSIGNMENT_DATE	TIMESTAMP	10	Yes
	START_DATE	TIMESTAMP	10	Yes

Table 90. USER\_ACCESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_ACCESS	USERKEY	INTEGER	4	No
	SUCCESS	INTEGER	4	Yes
	DATE_TIME	TIMESTAMP	10	No

Table 91. USER\_ACCOUNTS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_ACCOUNTS	HWKEY	INTEGER	4	No

Table 91. USER\_ACCOUNTS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	REVISION	INTEGER	4	No
	USERID	VARCHAR	100	No
	USERNAME	VARCHAR	100	Yes
	PW_SET	VARCHAR	7	Yes
	PW_AGE	INTEGER	4	Yes
	USER_PRIVILEGE	VARCHAR	100	Yes
	DISABLED	VARCHAR	7	Yes
	PW_NOT_REQUIRED	VARCHAR	5	Yes
	CANNOT_CHANGE_PW	VARCHAR	5	Yes
	LOCKED_OUT	VARCHAR	5	Yes
	PW_NEVER_EXPIRES	VARCHAR	5	Yes
	PW_EXPIRED	VARCHAR	5	Yes

Table 92. USER\_AUTHENTICATION\_KEY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_AUTHENTICATION_KEY	USERKEY	INTEGER	4	No
	KEY_TYPE	INTEGER	4	No
	UNIQUE_KEY	VARCHAR	50	Yes
	CREATED	TIMESTAMP	10	No

Table 93. USER\_AUTHORITY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_AUTHORITY	USERKEY	INTEGER	4	No
	AUTHTYPE	VARCHAR	20	No
	AUTHORITY	CHARACTER	1	No

Table 94. USER\_GROUP table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_GROUP	GROUPKEY	INTEGER	4	No
	NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	128	Yes



Table 94. USER\_GROUP table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	HASRULE	SMALLINT	2	No
	RULE	VARCHAR	128	Yes
	CREATED	TIMESTAMP	10	No
	USERPERMDEFKEY	INTEGER	4	Yes

Table 95. USER\_INFO table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_INFO	USERKEY	INTEGER	4	No
	CUSTOM1	VARCHAR	250	Yes
	CUSTOM2	VARCHAR	250	Yes
	CUSTOM3	VARCHAR	250	Yes
	CUSTOM4	VARCHAR	250	Yes
	CUSTOM5	VARCHAR	250	Yes
	CUSTOM6	VARCHAR	250	Yes
	CUSTOM7	VARCHAR	250	Yes
	CUSTOM8	VARCHAR	250	Yes
	CUSTOM9	VARCHAR	250	Yes

Table 96. USER\_PREFERENCE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_PREFERENCE	USERKEY	INTEGER	4	No
	ATTRIBUTE	VARCHAR	100	No
	VALUE	VARCHAR	100	No

# Chapter 36. Troubleshooting and Help

This section is intended to help you solve problems that might occur when using the BigFix® Remote Control Server program. Error Messages which might occur during a remote control session can be found in the *BigFix® Remote Control Console User's Guide*

## Recovering when the program is not running

If, after typing the Remote Control URL in your browser, the logon page does not display, you can check to see if the Remote Control-server service is running on the BigFix® Remote Control Server by doing the following :

- Within **Control Panel**, select **Administrative Tools** then **Services**
- Scroll down to the entry for Remote Control- server and check if its status is **Started**
- If not, right-click this entry and select **Start**
- If the status is Started, right-click, select **Stop** then restart it again as above
- Type the Remote Control URL in your browser. The logon page should be displayed.

## Login failure

When you cannot log on to the Remote Control server you can try the following options.

### **Login failure when there is no LDAP/AD authentication**

- Verify that the database is up and confirm that the application can connect to it. If there is a connection issue, this is logged in the `trc.log` file

This file can be found in the Remote Control server installation directory, specified at installation. For details, see the BigFix® Remote Control Installation Guide .

- Restart the database, then restart the Remote Control server service

### **Login failure when LDAP /AD authentication is enabled**

Verify that the Remote Control admin account can log on locally . If the admin user can logon locally then there may be a connectivity problem between Remote Control and LDAP. Again the `trc.log` file can be accessed to see what errors have occurred.



**Note:** The default admin userid within the Remote Control Application will always authenticate against the Remote Control database regardless of whether LDAP authentication is enabled.

## Log distribution task of the scheduler

Some details about the log distribution task of the Remote Control scheduler.

The value "scheduled.interval" contains a value expressed in "scheduled.**interval**.period" unit of time (mins, hours). This is the amount of time that the scheduler spends sleeping. In the log file, this is reported by the message "Scheduler: Sleeping for ...". After the sleeping time elapses, the scheduler wakes up and checks if there is any task that must be run. The amount of time that defines how frequently a task is run is defined in the table ASSET.TASK of the database, more precisely in the column PERIOD. The value expressed in that column is specified in "scheduled.**task**.period" (mins, hours) unit of time. The suggested value for "scheduled.**interval**.period" and "scheduled.**task**.period" is "mins".



**Note:** If the value on the PERIOD column is 0, the task is run every time that the scheduler wakes up. That is the amount of time defined in the "scheduled.**interval**" property. \*\*.

In order to change the PERIOD for a specific task, you must run the following query:

```
UPDATE ASSET.TASK
SET PERIOD=X
WHERE TASKKEY=Y;
```

The task key associated to the specific task can be retrieved by running the following query:

```
SELECT TASKKEY, TYPE, NAME, SCHEDULED, ACTIVE, PERIOD
FROM TRCDB.ASSET.TASK
```

For example:

#### **SYNCLDAP**

Is the task related to the LDAP synchronization.

#### **LOGDISTN**

Is the task related to the log distribution.

#### **CLEANACCESSREQUEST**

Is the Access Request Cleanup (Clean expired Access Requests).



**Note:** Ensure that the value X used in the query is expressed in minutes if "scheduled.**task**.period"="mins".

## Using log files to solve a problem

The Remote Control components have log files which can provide extra information when troubleshooting an issue.

### Obtaining the server log files

You can use the log file in the BigFix® Remote Control Server program to troubleshoot problems you encounter.

To view a log of all server and database activities, click **Admin > View Application Log**. The content of the Application Log is displayed on the screen. To see the most recent activities, scroll to the bottom of the file.



**Note:** From the Admin menu, select **Send Application Log**, to open or save the application log file, `trc.log`, for attaching to an email.

### **Log4j logging**

The log4j package is used to provide additional logging information and this can be useful when trying to debug a problem using the application log file. The level of logging can be controlled by the property values in the `log4j2.properties` file. For more details, see [Editing the properties files \(on page 215\)](#). The following levels of logging are available:

- ALL
- DEBUG
- INFO . This is the default value
- WARN
- ERROR
- FATAL
- OFF

To obtain more information for debug purposes complete the following steps

1. Click **Admin > Edit properties file**.
2. Select **log4j2.properties** from the list.
3. Set **logger.rolling.level=DEBUG**,  
Set this value to log information from debug messages to fatal messages.
4. Click **Submit**.
5. Click **Admin > Reset Application**.
6. Restart the Remote Control- server service.
7. Perform the steps that are causing a problem with the application.
8. Click **Admin > View Application Log** to view the log information or select **Send Application Log** to save the log file.

There might be multiple copies of trc log files. All of these log files are helpful when debugging a problem and can be sent to the support team when you have a problem. The value of **log4j.logger.com.bigfix** must be set back to **INFO** when finished.

## Obtaining the controller log files

For debug purposes, you can create a log file on the controller system in multiple ways.

Choose the method for enabling debug.

### **Enable debug in the local controller configuration**

1. Edit the `trc.properties` file that is in your home directory. The file is in the following directory.

#### Windows systems

`USERHOMEDIR\.trc\trc.properties`, where `USERHOMEDIR` is the home directory of the logged on user.

#### Linux or macOS systems

`USERHOMEDIR/.trc/trc.properties`, where `USERHOMEDIR` is the home directory of the logged on user.

2. Set `debug.trace=true`.
3. Save the file and restart the controller.

#### Enable debug by creating a system variable

Create a system variable on the controller system with the name `TRC_TRACE` and set it to `Yes`.

To create a log file for debug purposes, complete the following steps:

1. Start a session with the required target.
2. Complete the steps that produce the problem and end the session.
3. On the controller system, go to the home directory to access the `trctrace_XXXXX.log` file. The file name contains the date and time stamp of when the file was created. For example, `trctrace_20170309_124230.log`

## Obtaining the target log files

You can create debug log files on the target system for debugging a problem by configuring target properties. To enable the debug log, complete the steps that are relevant to your operating system. You must have admin authority.

#### Windows® systems

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 **LogLevel** and select **Modify**
3. Set the value to `4` and click **OK**.
4. Restart the target service.
5. Start a session with the target and run the steps that are required for creating the problem.
6. End the session.

The log files are found in the location that is defined by the **WorkingDir** property in the target registry.

### Linux® systems

1. Edit the `/etc/trc_target.properties` file
2. Set the value of **LogLevel** to 4 and save the file.
3. Restart the target service.
4. Start a session with the target and run the steps that are required for creating the problem.
5. End the session.

The log files are found in the location that is defined by the **WorkingDir** property in the `trc_target.properties` file.

### macOS systems

1. Click **Go > Utilities > Terminal**.
2. Enter `sudo defaults write /Library/Preferences/com.bigfix.remotecontrol.target.plist LogLevel 4`.
3. Enter your password if prompted.
4. 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`
5. Start a session with the target and run the steps that are required for creating the problem.
6. End the session.

Part of the log files that originate from the daemon process are found in the working directory of the target `~/Library/Application Support/com.bigfix.remotecontrol.target`

The log files that originate from processes running under the logged user authority are found in `/Users/<user>/Library/Application Support/com.bigfix.remotecontrol.target`. Log files like `trc_gui` and `trc_ft` are found in this folder.

The log files are created with names in the following format:

- On Windows® and Linux® systems:

`trc_[comp]_[SUFFIX].log` where `[SUFFIX]` is determined by the **LogRollOver** and **LogRotation** settings and `[comp]` is base, dsp, or gui.

For example, `trc_base_Mon.log`, `trc_gui_Thu.log`

- On macOS systems:

trc\_target\_*[SUFFIX]*.log where *[SUFFIX]* is determined by the **LogRollOver** and **LogRotation** settings.

For example, `trc_target_Mon.log`.



**Note:** When you finish gathering log files, set the value of **LogLevel** back to 2. Restart the target service.

For more information about the logging properties, see [Properties for configuring logging activity \(on page 425\)](#)

## Obtaining the gateway log files

The gateway log file can be used for debug purposes when you have an issue in your environment and gateways have been configured.

The name of the log file is `TRCGATEWAY-hostname-suffix.log` where *hostname* denotes the computer name or host name of the system hosting the gateway and *suffix* denotes the date and time, depending on which rotation and rollover settings are being used. For more information about the log, see [Logging gateway activity \(on page 206\)](#).

The log file is located in the following directories:

### Windows® systems

```
\ProgramData\BigFix\Remote Control\Gateway
```

### Linux® systems

```
/var/opt/bigfix/trc/gateway
```

## Obtaining the broker log files

The broker log file can be used for debug purposes when you have an issue in your environment and brokers have been configured.

The name of the log file is `TRCICB-hostname-suffix.log` where *hostname* denotes the computer name or host name of the system hosting the broker and *suffix* denotes the date and time, depending on which rotation and rollover settings are being used. For more information about the log, see [Logging broker activity \(on page 312\)](#).

The broker log files are located in the `\Broker` directory within the broker's working directory.

### Windows® systems

```
\ProgramData\BigFix\Remote Control\Broker
```

### Linux® systems

```
/var/opt/bigfix/trc/broker
```

## Obtaining the smart card feature log files

Use the smart card log files for debugging purposes when you use a smart card during a session and encounter an issue.

Two log files are available at the end of the session: the `trcsmc_debug.log` file on the controller and the `trc_vscr_ctrl_[SUFFIX].log` file on the target, where `[SUFFIX]` is determined by the values that are set for the **LogRollOver** and **LogRotation** properties on the target. For example, `trc_vscr_ctrl_Wed.log`. For more information about setting logging parameters in the target, see [Obtaining the target log files \(on page 397\)](#).

The controller log file is in the following directory:

`\Users\username`, where `username` is the user name of the controller user that was logged on during the session.

The target log file is in the following directory:

`\ProgramData\BigFix\Remote Control.`

Use the smart card log files and the controller and target log files to help you debug issues in a session where a smart card was used.

## Obtaining the smart card Fixlet log files

When you run the Fixlets to install or remove the device driver for the virtual smart card reader or the Fixlet to install the certificates, use the following log files for debugging purposes when an error is reported:

### `VSCDriverInstall.log`

Created when you run the **Install Remote Control Virtual Smart Card Reader Driver version 9.1.4.0500 and certificates** task.

### `VSCDriverUninstall.log`

Created when you run the **Uninstall Virtual Smart Card Reader Driver for Remote Control** task.

### `VSCCertsInstall.log`

Created when you run the **Install Remote Control Certificates for the Virtual Smart Card Reader Driver version 9.1.4.0500** task.

The log files are in the target installation directory.

## Setting up the Trusted Sites zone

If you encounter problems loading the Remote Control Web pages while running Windows® XP with Service Pack 2, you may need to add your BigFix® Remote Control Server IP address to your Trusted Sites list.

To add the Remote Control program to the Trust Sites zone, perform the following steps:



1. In Internet Explorer, click **Tools > Internet Options**.
2. Click the **Security** tab.
3. Click **Trusted sites**.
4. Click the **Sites...** button.
5. Clear the check box beside "**Require server verification (https:) for all sites in this zone**".
6. Type the server address in the "**Add this Web site to the zone:**" field.
7. Click **Add**.
8. Click **OK** and then load or reload the BigFix® Remote Control Server pages.

## Targets unable to contact the server successfully and a session cannot be established with these targets

### Symptom

Targets cannot contact the server successfully and a session cannot be established with the targets.

### Causes

The target may not have the correct web address for the server or the host name part of the web address, which it uses to contact the server, does not match the common name in the server's SSL certificate.

### Solution

After you install the target software the target tries to contact the server. It uses http or https, and the server web address that you 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 needs to have the correct web address for the server.
- The host name part of the web address must match the common name in the server's SSL certificate.

When you install the BigFix® Remote Control Server by using the installation program, you must ensure that you enter the correct values in the **Web server parameters** window. The **upload data to server** field takes the computer name from the Windows® operating system settings. The server installer program uses the field value to generate the server URL and the SSL certificate. The server URL is used to set the **url** property value in the `trc.properties` file. Therefore, you must specify the correct 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 address to contact the server in the future. If the web address that is sent to the target is incorrect, the symptoms you will see are that the target can register once and then is unable 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 server address with which to authenticate an incoming session.

The common name that is in the server's SSL certificate has to be a host name that actually resolves to the IP address of the server. If the SSL certificate, for example, has *mytrcserver*, but on the target there is no way to translate 'mytrcserver' to the IP address of the server, then your environment is not correctly configured. The only names that are correctly supported for this are fully qualified domain names that are registered in the DNS, for example, *mytrcserver.location.uk.example.com*. If you use only *mytrcserver*, then that will only work if the server and target are 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 computername and IP address.

```
For example: At a command prompt type the following commands
```

```
C:\>nslookup
```

```
Default Server:  gbibp9ph1--31ndcr.wan.example.com
```

```
Address:  192.0.2.21
```

```
Type in the hostname of your server
```

```
> mytrcserver.location.uk.example.com
```

```
Server:  gbibp9ph1--31ndcr.wan.example.com
```

```
Address:  192.0.2.21
```

```
Name:    mytrcserver.location.uk.example.com
```

```
Address:  192.0.2.25
```

```
Type in the ip address of your server
```

```
> 192.0.2.25
```

```
Server:  gbibp9ph1--31ndcr.wan.example.com
```

```
Address:  192.0.2.21
```

```
Name:    mytrcserver.location.uk.example.com
```

```
Address:  192.0.2.25
```

In the example you can see that the server hostname resolves to the correct IP address.

## Remotely installed targets cannot contact the server

### Symptom

Remotely installed targets cannot contact the server.

### Causes

The **URL** property in the `trc.properties` file does not contain the correct web address for the Remote Control server.

### Solution

It is important to make sure that the **URL** property in the `trc.properties` file contains the correct web address for the Remote Control server as this property is used when targets contact the server and for determining the server to use during a remote target installation. If the **URL** property value is not correct the remote targets will not be able to contact the server successfully. Edit the `trc.properties` file and make sure that the correct value is set.



**Note:** If the IP address of the Remote Control server changes at any time this is not reflected in the Remote Control application, therefore it is important to make sure that the **URL** property in `trc.properties` is updated and the server restarted as the targets will try to contact the old IP address till the change to the property is made.

## Extending the time period before you are logged out of the server due to inactivity

When you are logged on to the BigFix® Remote Control Server and there is no activity, you are logged out after a time period. You can increase this time interval.

A default time period of 30 minutes is set in the `WEB.XML` file that is installed with the server. You can increase the timeout value by editing the `WEB.XML` file.

For a server that is installed by using the server installer, the file is in the following directory, `\[server installation directory]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF`.

For a server that is installed on a Linux™ operating system.

```
/[server installation directory]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF.
```

For a server that is installed on WebSphere® Application Server version 8.5.

```
\[server installation directory]\trc_war.ear\trc.war\WEB-INF.
```

To increase the timeout value, complete the following steps.

1. Edit the `WEB.XML` file.
2. Edit the following property.

```
<session-config>  
<session-timeout>30</session-timeout>  
</session-config>
```

3. Set the timeout value to the number of minutes.
4. Save the file.
5. Restart the server service.

## Gray screen on a Windows 2003 system

When a remote desktop user uses the `/admin` or `/console` option to start a remote desktop session with a Windows® Server 2003 system and a remote control user starts a remote control session before, during or after the remote desktop session, the target display cannot be captured. The result is that a gray screen is displayed in the controller window. This issue is a limitation in Windows® Server 2003 operating system. Use the **Automatically reset the console after a Remote Desktop console session** attribute as a workaround to reset the Windows® session either after each remote desktop session ends, or before a remote control session starts, depending on the value that is selected.



**Note:** The attribute is not set to any value by default.

To configure this attribute and for a definition of its values see [Creating target groups \(on page 71\)](#).



**Note:**

1. The workaround is defined through a target group attribute and not a policy. Therefore, if you start a session immediately after you change the setting, it might not be updated in the target yet.
2. If a target belongs to more than one target group with different values for this attribute, the higher value takes precedence with **After console is logged out** having the highest value.

For example:

A target belongs to groups A and B. The value of the attribute is set to **At session start** for group A and **After console is logged out** for group B. Therefore, the final value that is applied to any sessions with this target is **After console is logged out**.

3. If an admin or console remote desktop session is in progress when the controller attempts to connect to a target, a message is displayed on the controller. The message provides details of the remote desktop user and the IP address or computer name that the session is running from.
4. The workaround can also be configured in the `trc.properties` file by using a server policy. If both the server property and target group attribute is set to different values, the target group value takes precedence over the server value.

The following messages are displayed depending on the value that selected for the properties and whether a user is logged at the target computer.

**Table 97. Workaround messages**

Message #1	Message ID	Message text	Message parameters
1	workaround.w2k3rdp.console.unavailable	Remote Control is unable to control this target system because the Windows® console is in a Remote Desktop session with user {0} connected from {1} ({2})	{0} Remote Desktop Client's user name {1} Remote Desktop Client's computer name {2} Remote Desktop Client's IP address
2	workaround.w2k3rdp.console.reset	Remote Control is unable to control this target system because the Windows® console is unavailable while it is being reset. This might take a few minutes. You can stop the Remote Control session at any time.	
3	workaround.w2k3rdp.disabled	Remote Control is unable to control this target system because the Windows® console is unavailable and the automatic reset is not enabled.	
4	target.capture.failed.start	Remote Control is unable to control this target system because the display capture process failed to start.	

The following table details when the message is displayed.

**Table 98. When the workaround messages are displayed**

Message #1	Session 0 - user logged in	Session 0 - user logged off
The workaround is disabled	Message #1	Message #3
Reset session automatically when a remote control session is started.	Message #1	Message #2 and reset session
Reset session automatically when the remote desktop user has logged out.	Message #1	Message #2 if the reset was less than 2 minutes ago
Target not running on Windows® Server 2003 - workaround does not apply #4	Message #4	Message #4

## Files not visible during a file transfer session

Some folders or files stored in the `C:\Windows\System32` directory are not visible during a file transfer session.

This problem is caused by the file system redirector which automatically redirects the accesses from `%windir%\System32` to `%windir%\SysWOW64` for all 32-bit processes running on a 64-bit platform. The problem applies to the Controller and the Target because they are both running as a 32-bit application (the Controller runs on a 32-bit Java Virtual Machine).

This problem is described in the following Microsoft article: <https://docs.microsoft.com/en-us/windows/desktop/winprog64/file-system-redirector>

Both local and remote files during a file transfer session show the path `C:\Windows\System32` while the real path used is `C:\Windows\SysWOW64`.

As a workaround for this issue, you can access the following hidden folder:

```
C:\Windows\Sysnative
```

in order to view the same files and folders structure listed in the command line or displayed in the File Explorer.

## Getting control of a mac OS target after the screen is locked

If you encounter the following issue:

1. Open a remote session to a mac OS target by using a Controller or a VNC Client, or be in front of the mac OS target.
2. Lock the screen and ensure that the user name and password prompt is displayed.
3. Close the controller/VNC client if opened on the other computer.
4. Wait for 5-10 minutes and avoid pressing both the physical mouse and the keyboard. Also avoid opening VNC sessions to the mac OS target.
5. Open the Remote Control Controller and connect to the mac OS target.
6. The screen is black and you cannot take control of the mac OS target.

To prevent this issue, perform these steps:

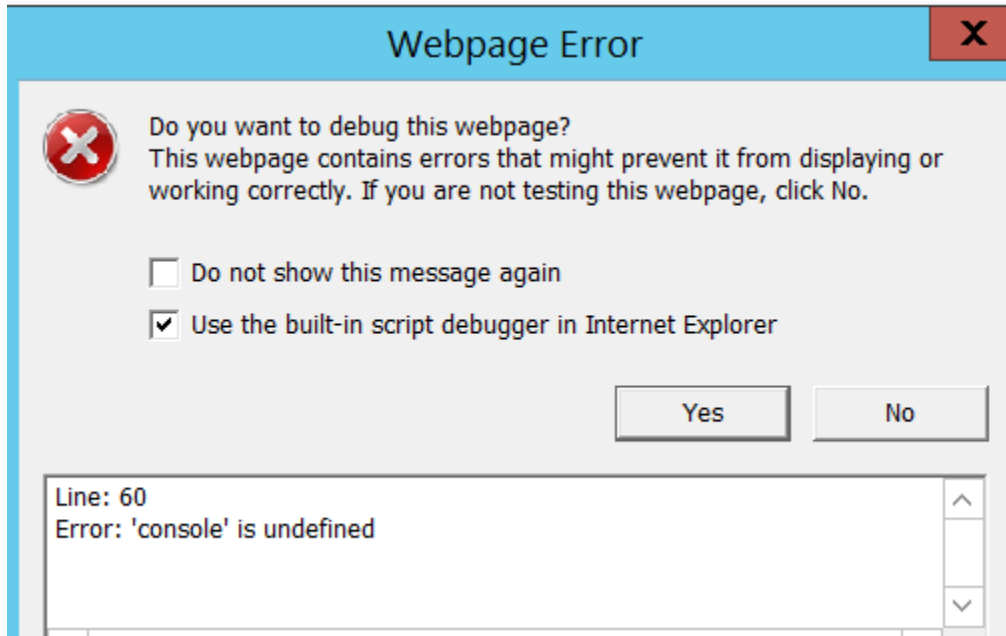
1. On the mac OS target, open the **Energy Saver** panel.
2. Select the check box named **Prevent computer from sleeping automatically when the display is off**.

## Issues with visualization of RC Server 10 with IE

### Problems found in the visualization of RC Server 10 with IECondition

## Cause

The error reported in the following image occurs because the browser makes the console emulating a previous version of IE. This seems to occur mostly in Win 2012, while in Win10 IE11 rendering mode is set as default.



## Remedy

To change the type of display, press F12 > Emulation Tab > Document Mode > Set IE11 as Default.

## Getting Help

If you have a problem with the BigFix® Remote Control Server program or have questions about a specific feature, a variety of sources are available to help you including

- Documentation
- Web Pages

## Using the Documentation

Many problems can be solved without contacting HCL® for assistance. If you experience a problem or have a question about the operation or functionality of the Remote Control program, begin with the online documentation

To access the online documentation, do the following

- Click **Help > Online Documentation**

You are taken to the Remote ControlHelp Center where you can select the required documents.

## Accessing the Remote Control product documentation

The Remote Control documentation site provides the latest technical information and any downloadable updates that are available.

To access the documentation, use the following web address

The list of Remote Control documents are listed. Explore the relevant document.

## Broker troubleshooting and FAQs

This section provides some answers to questions that might arise when you are installing or using the broker functions.

### Why should I install broker support in my environment?

If a target is situated outside of your enterprise network and it requires support, you must install broker support so that remote control connections can be made across the internet to the target.



**Note:** It should be noted that the targets should be managed by a remote control server.

### What method can I use to install broker support?

If you have access to the BigFix® console you can use the deployment node to deploy the broker support relevant to your operating system. For more details about deploying from the console, see the *BigFix® Remote Control Console User's Guide*.

You can also use the BigFix® Remote Control Console User's Guide installation files to install broker support. For more details, see the *BigFix® Remote Control Installation Guide*.

### After I install broker support, what do I do next?

After you install the broker support, you must complete the following steps.

1. Create a broker configuration. For more information about configuring brokers, see [Broker configuration \(on page 308\)](#).
2. Register your brokers in the Remote Control server. For more information about broker registration, see [Registering a broker on the server \(on page 325\)](#).
3. Obtain the required certificates for your broker. For more information about certificates, see [Creating Certificate Authority signed certificates \(on page 331\)](#). You can create self-signed certificates for each broker that you install. For more information about self-signed certificates, see [Strict Certificate Verification on Broker Connections \(on page 330\)](#).
4. Add the certificates to the broker. For more information about adding the certificates, see [Configuring the keystore on the broker \(on page 329\)](#).
5. Upload the certificates to the server truststore. For more information about uploading the certificates, see [Truststore configuration \(on page 333\)](#).

### Is only one broker allowed?



No, you can install multiple brokers in your environment to suit your specific requirements. For example, a possible motivation would be to provide service failover so that new sessions can continue to be serviced while one of the brokers goes down. When you have installed the brokers, you must configure them. Add the relevant connection parameters that are required to allow connections to be made between your brokers and controllers and targets. For more information about configuring endpoint connections, see [Allowing endpoints to connect to a broker \(on page 309\)](#). For details about connections between a broker and other brokers, see [Support for multiple brokers \(on page 310\)](#).

#### How do I select a target and connect to a broker?

When you start broker remote control session, do not select a target. You must use the **Start a Broker session** option in the Remote Control server GUI to initiate the session and connect to a broker. Pass the connection code to the target user. The target user can start a broker remote control session and use the connection code to make the correct connection. For more information about starting a broker session, see the *BigFix® Remote Control Controller User's Guide*.

#### If there are multiple brokers installed which broker do I connect to?

You do not connect to a specific broker. When multiple brokers are registered in the remote control server, the list of brokers is known as the brokerlist. When you start a broker remote control session, the controller system tries to connect to each broker in the list until it makes a successful connection to one. The target system also does the same when it is connecting to a broker. If the controller and target connect to different brokers, the controller disconnects and connects to the same broker as the target. To make the connection, the controller uses the host name that is defined in the broker property **PublicBrokerURL**, on the broker that the target is connected to.



**Note:** The host name that is defined in **PublicBrokerURL** must match the host name that is defined in the certificate for the broker. It must also match the host name that you use to register the broker in the remote control server.

For more information about broker properties, see [Configuring the broker properties \(on page 308\)](#).

#### What session modes are available for remote control sessions that connect through a broker?

When you start a remote control session through a broker, an Active session is initiated by default. However, if Active mode is not enabled in the session policies that are defined for the session, the next available session mode is used. The following order of precedence applies, Guidance, Monitor, Chat, File transfer. In addition, if user acceptance is enabled for the session, the target user can select a different session mode to start from the acceptance window. For more details about starting a broker session, see the *BigFix® Remote Control Controller User's Guide*.

#### How do I create a certificate?

If you are using a Certificate Authority (CA) certificate, you must consult their documentation to see how the root certificate and any relevant intermediate certificates can be obtained. For self-signed certificates, you can use the key management tool iKeyman. This tool is included with Remote Control

and is also available through IBM WebSphere Application Server. For more information about creating certificates, see [Creating a self signed certificate \(on page 327\)](#).

**What do I do if my certificate is about to expire?**

You can add a certificate to the broker and to the truststore on the server. However, to allow the target to start a session through the broker it must continue to use the old certificate. The reason for this is that the target does not yet trust the new certificate, therefore it would be unable to start a session. For more information about changing to a new certificate, see [Migrating to a new certificate \(on page 335\)](#).

# Appendix A. Gateway sample scenarios

This appendix illustrates the gateway installation and configuration in three different network scenarios to ensure communication between the three Remote Control components (target, server and controller) across firewalls and NAT environments.

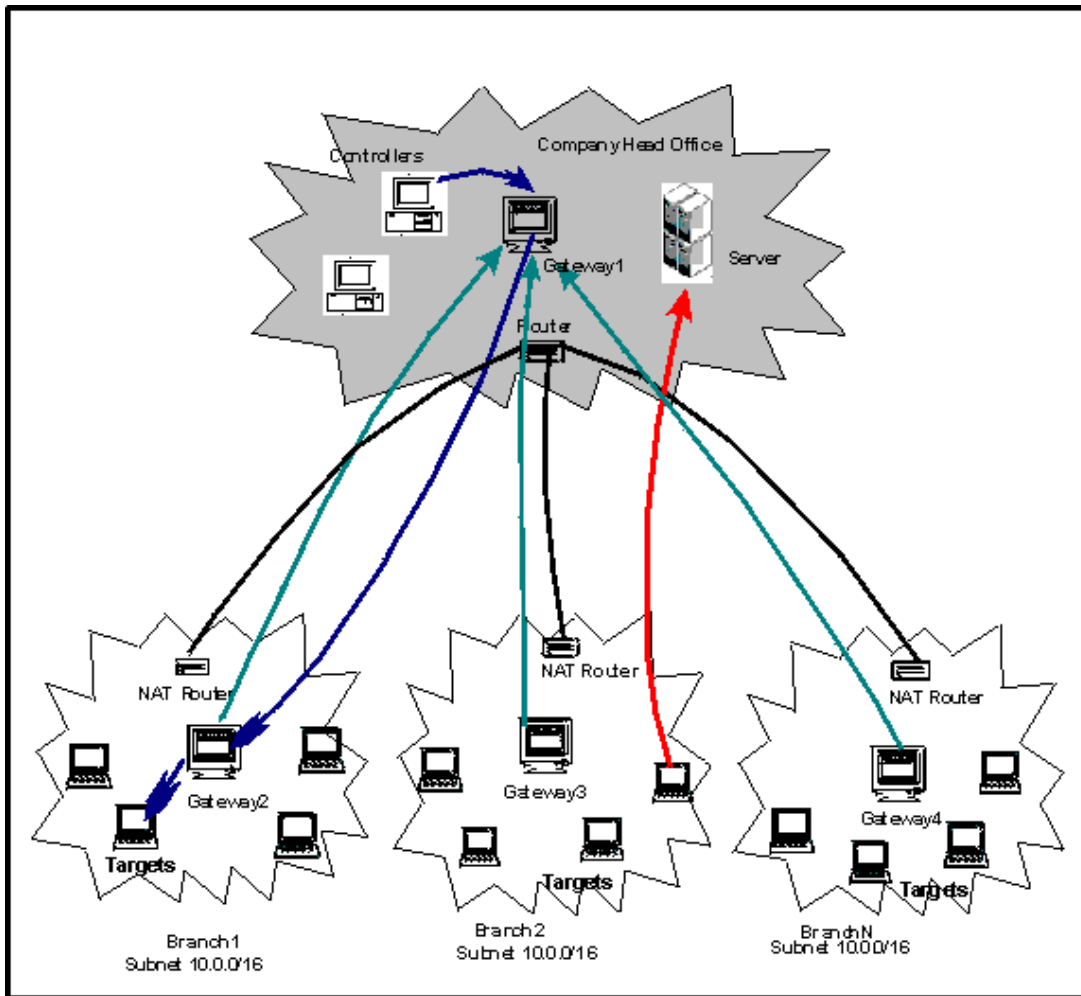
## Overview

There are three types of connections used between the TRC components:

- The target uses HTTP connections to the server for registration and heartbeats.
- The controller uses TRC's own protocol for remote control sessions to the target. By default, the target uses port 888.
- The controller uses HTTP connections to launch a session.

## Scenario 1 - Several networks using Network Address Translation (NAT)

Figure 7. Several networks using NAT



In this scenario, there are multiple networks with targets in all of the networks and the controllers all in the Company Head Office. The NAT routers in the branches prevent the controllers from connecting directly to the targets in the branches and therefore, a gateway must be installed in each network.

Similarly, Gateway 1 cannot connect directly to the gateways in the branches and therefore, Gateway 2, 3 and 4 must connect to it first.

In such a scenario, Gateway 1 must be able to accept the connections from the other gateways and from controllers trying to initiate remote control sessions against targets located in other networks.

However, Gateways 2, 3, and 4 must establish a connection to Gateway 1, and must be able to locate targets in their networks.

### Gateway 1 roles:

- Accept remote control connections from gateways 2, 3 and 4. The gateways in each of the branches will connect to gateway 1.
- Accept connection requests from controllers in the head office so that they can be forwarded to the gateways in the branches to allow them to locate the correct target.
- Therefore the configuration file for, *Gateway 1* will contain the following entries:

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = true
```

Nothing else is required for Gateway 1.

The inbound connection, named **Inbound.1** in this example, will allow connections from the other gateways on port 8881. The optional parameters can be configured as required.

AllowGateways set to true, configures the gateway to accept connections from gateways 2, 3 and 4. While AllowEndpoints determines if the gateway is also going to receive controllers requests and therefore, should forward these requests to other gateways in order to locate the right target in their respective networks.

#### Gateway 2, 3 and 4 roles:

- Create control connection to Gateway 1.
- Locate endpoints in the branch network.
- Therefore the configuration file for, *Gateway 2*, *Gateway 3* and *Gateway 4* will contain the following entries:

```
Gateway.1.ConnectionType = Gateway

Gateway.1.DestinationAddress = gateway1_ipaddress

Gateway.1.DestinationPort = 8881

# Optional:

# Gateway.1.BindTo = 0.0.0.0
```

```
# Gateway.1.SourcePort = 0

# Gateway.1.RetryDelay = 45

# Gateway.1.KeepAlive = 900

# Gateway.1.Timeout = 90

# Gateway.1.Passphrase =

Endpoint.1.ConnectionType = Endpoint

# Optional

# Endpoint.1.SubnetAddress = 0.0.0.0

# Endpoint.1.SubnetMask = 0.0.0.0

# Endpoint.1.BindTo = 0.0.0.0

# Endpoint.1.SourcePort = 0

# Endpoint.1.Timeout = 90
```

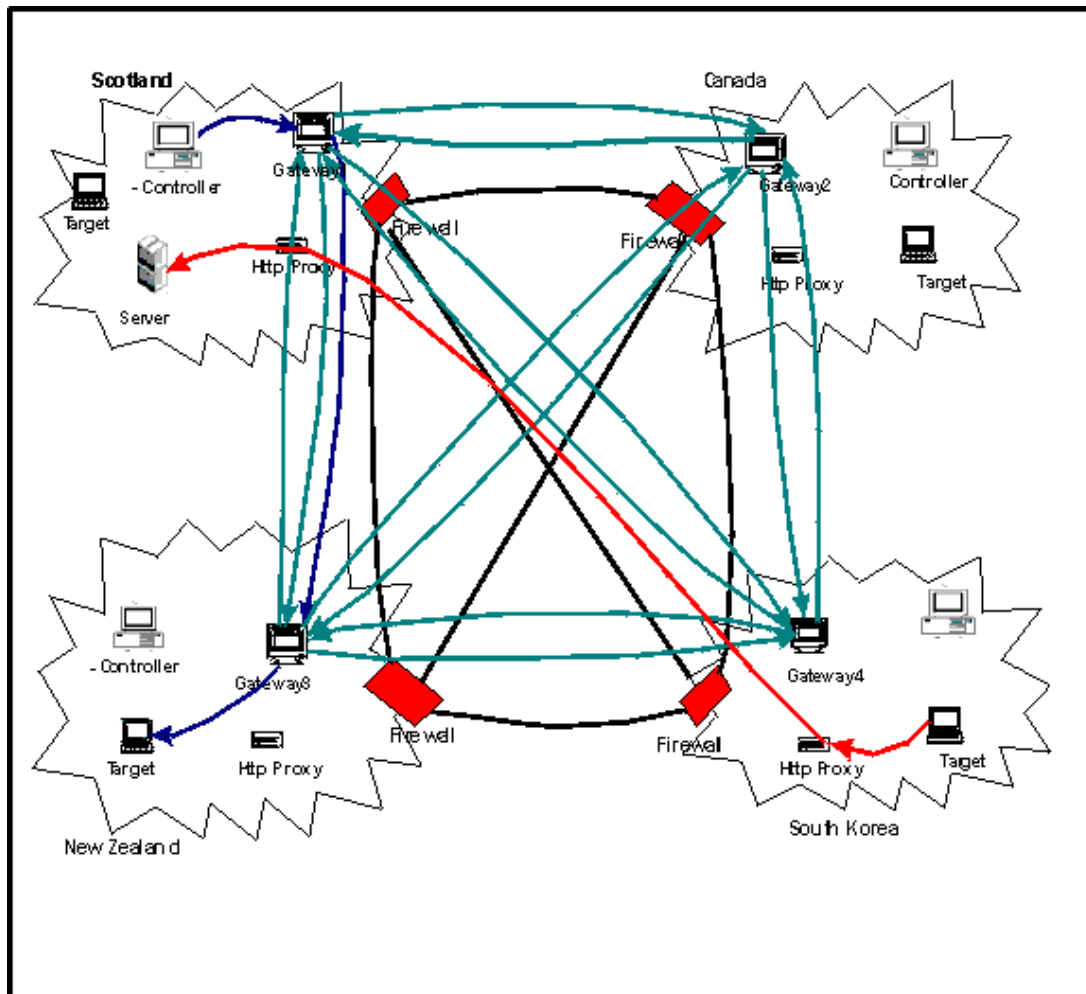
In this case, there are no inbound connections because there are no controllers or gateways connecting to Gateways 2, 3 and 4. These gateways are connecting to Gateway1 and this is defined by the **Gateway.1** connection which has a connection type, gateway. The DestinationAddress of Gateway.1 is set to the IP address for Gateway1 and DestinationPort must match whatever is defined in Gateway 1 PortToListen. AllowEndpoints is set to true.

Another type of connection must be defined for these gateways, an endpoint connection (named Endpoint.1 in this example). This type of connection configures the gateway to search for a target that a controller may want to initiate a remote control session with. It is recommended to specify the subnet address and mask to reduce the amount of network traffic generated by the gateway. With the default values for the subnet, the gateway will try to connect to every single endpoint for which a request is received, even if the endpoint is in a remote network and is unreachable by the gateway.

In the trc server, you would also add **Gateway1** by clicking on **Admin > New TRC Gateway**. The port number would be the one defined in the **Inbound.1.PortToListen** property.

## Scenario 2 - Meshed Networks

Figure 8. Meshed networks



In this scenario the targets and controllers are distributed over several locations, all of which are protected by a firewall. The firewalls prevent the controllers from connecting directly to the target in remote locations, but they do allow the gateways to connect to *gateways and gateways only*, in remote locations. The existing HTTP Proxy servers, allow the targets to connect to the server.

In this scenario, all of the gateways have the same roles:

- Create a control connection to the 3 other gateways.
- Accept control connections from the 3 other gateways.
- Accept requests from the controllers in the local network.
- Locate endpoints in the local network.

Therefore the configuration file for the gateways will contain the following entries:

```
Inbound.1.ConnectionType = Inbound
```

```
Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = true
```

Then for each of the gateways it has to connect to:

```
Gateway.X.ConnectionType = Gateway

Gateway.X.DestinationAddress = gatewayX_ipaddress

Gateway.X.DestinationPort = 8881

# Optional:

# Gateway.X.BindTo = 0.0.0.0

# Gateway.X.SourcePort = 0

# Gateway.X.RetryDelay = 45

# Gateway.X.KeepAlive = 900

# Gateway.X.Timeout = 90

# Gateway.X.Passphrase =

Endpoint.1.ConnectionType = Endpoint

# Optional

# Endpoint.1.SubnetAddress = 0.0.0.0

# Endpoint.1.SubnetMask = 0.0.0.0

# Endpoint.1.BindTo = 0.0.0.0

# Endpoint.1.SourcePort = 0

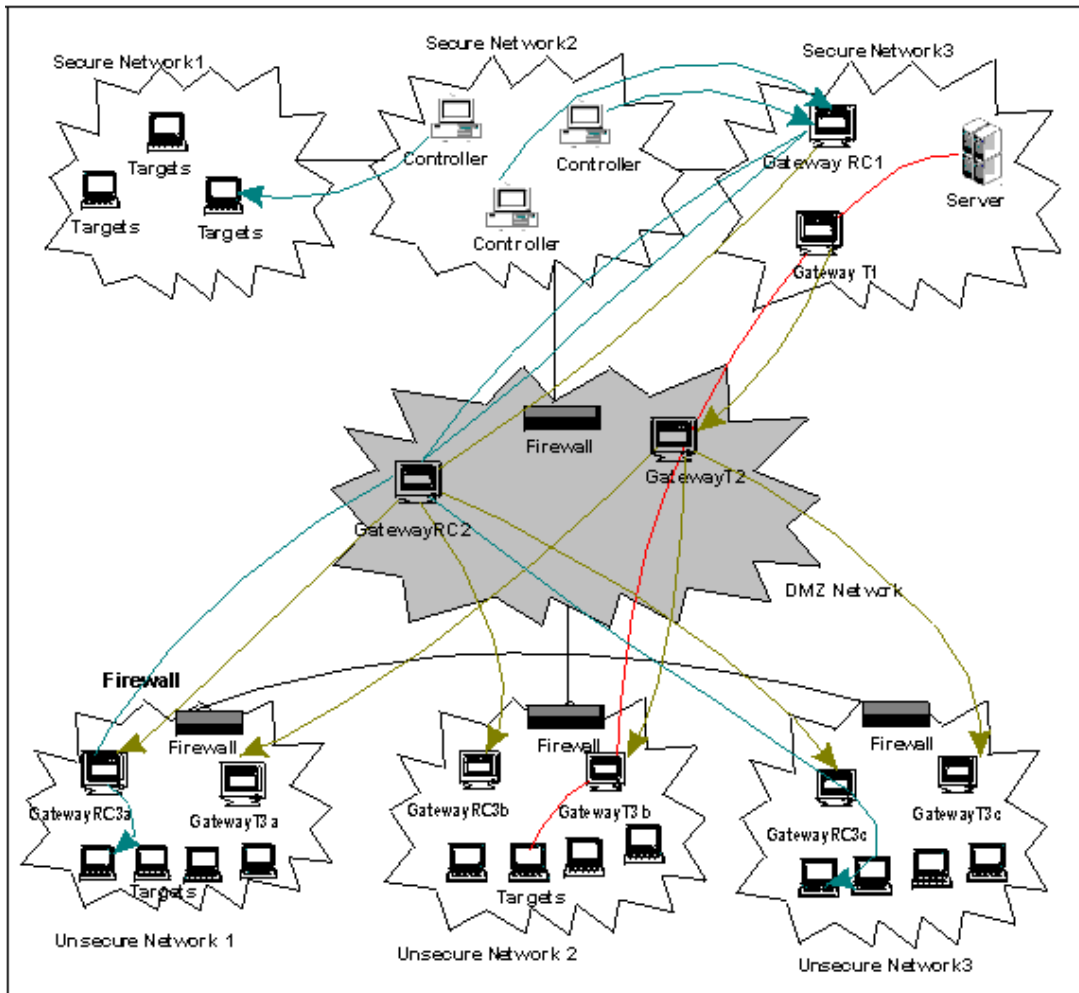
# Endpoint.1.Timeout = 90
```



In this scenario also, all of the gateways will be added to the server.

## Scenario 3 - Web hosting

Figure 9. Webb hosting scenario



In this scenario there are two well defined networks, a secure network where the server is installed and the controllers machines are located and an unsecure network, it could be a web facing network, where servers need to be accessed for maintenance and problem resolution.

The two networks are linked by a DMZ network where two gateways, each with a specific purpose, are installed.

Additionally, HTTP proxies are not available in order to enable the targets in the unsecure network to register in the server in the secure network therefore the gateways need to establish a **tunnel** connection to allow this communication.

There are two possible scenarios:

### Scenario A:

A gateway in the DMZ network is allowed to connect directly to the targets in the secured network (this scenario requires Gateway T1, Gateway T2, T3x and Gateway RC2)

In this scenario, we would add gateway RC1 to the TRC server.

#### **Scenario B:**

No traffic is allowed to the DMZ network and the gateway is NOT allowed to connect directly to the targets in the secured network (this scenario requires Gateway T1, Gateway T2, Gateway T3x, Gateway RC1, Gateway RC2 and Gateways RC3x)

In this scenario, we would add gateway RC1 to the TRC server.

The configuration for each scenario would be as follows:

#### **Configuration common to both scenarios**

##### **Gateway T1:**

- Create a control connection to Gateway T2 to be used for the tunnel.
- Create connections to the server for tunnel connections.

```
Gateway.3.ConnectionType = Gateway
```

```
Gateway.3.DestinationAddress = gatewayT2_ipaddress
```

```
Gateway.3.DestinationPort = 8881
```

```
# Optional:
```

```
# Gateway.3.BindTo = 0.0.0.0
```

```
# Gateway.3.SourcePort = 0
```

```
# Gateway.3.RetryDelay = 45
```

```
# Gateway.3.KeepAlive = 900
```

```
# Gateway.3.Timeout = 90
```

```
# Gateway.3.Passphrase =
```

Since the targets in the unsecure network cannot connect directly to the server, a **tunnel** connection must be created that will forward the heartbeats from the targets to the server:

```
Outbound.1.ConnectionType = OutboundTunnel
```

```
Outbound.1.DestinationAddress = trc_server_ip_address
```

```
Outbound.1.DestinationPort = 80
```

```
# Optional
```

```
# Outbound.1.TunnelID = TRCSERVER
```

```
# Outbound.1.BindTo = 0.0.0.0
```

```
# Outbound.1.Timeout = 90
```

Where the DestinationAddress and DestinationPort are the IP address and port of the TRC server.

### Gateway T2:

Therefore the configuration file for Gateway T2 will contain the following entries, regardless of the type of scenario:

- Create connections to Gateways T3x
- Accept control connections from gateway T2.

A gateway connection must be defined for each T3 gateway, that is GatewayT3a, GatewayT3b and GatewayT3c.

```
Gateway.T3x.ConnectionType = Gateway
```

```
Gateway.T3x.DestinationAddress = gatewayT3x_ipaddress
```

```
Gateway.T3x.DestinationPort = 8881
```

```
# Optional:
```

```
# Gateway.T3x.BindTo = 0.0.0.0
```

```
# Gateway.T3x.SourcePort = 0
```

```
# Gateway.T3x.RetryDelay = 45
```

```
# Gateway.T3x.KeepAlive = 900
```

```
# Gateway.T3x.Timeout = 90
```

```
# Gateway.T3x.Passphrase =
```

```
Inbound.1.ConnectionType = Inbound
```

```
Inbound.1.PortToListen = 8881
```

```
# Optional:
```

```
# Inbound.1.BindTo = 0.0.0.0
```

```
# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = false
```

### Gateways T3x:

The configuration file for Gateways T3x will contain the following entries, regardless of the type of scenario:

- Accept control connections from gateway T2.
- Accept requests from endpoints for tunnel connections to the server.

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = false

InboundTunnel.1.ConnectionType = InboundTunnel

InboundTunnel.1.PortToListen = 8880

# Optional

# InboundTunnel.1.TunnelID = TRCSERVER

# InboundTunnel.1.BindTo = 0.0.0.0

# InboundTunnel.1.RetryDelay = 45
```

Since the targets in the unsecure network cannot connect directly to the server, a **tunnel** connection must be created that will forward the heartbeats from the targets to the server.

**PortToListen** specifies the port that the target should connect to when connecting to the server via a tunnel. For the targets to use the tunnel, the target configuration must set the ProxyURL to:

```
trcGateway.://<gateway address>:8880
```

## **Scenario A**

### **Gateway RC2**

Gateway RC2 will have the following configuration:

- Accept requests from controllers in the secure network.
- Locate endpoints in the unsecure networks.

```
Inbound.1.ConnectionType = Inbound
```

```
Inbound.1.PortToListen = 8881
```

```
# Optional:
```

```
# Inbound.1.BindTo = 0.0.0.0
```

```
# Inbound.1.RetryDelay = 45
```

```
# Inbound.1.Passphrase =
```

```
Inbound.1.AllowGateways = false
```

```
Inbound.1.AllowEndpoints = true
```

```
Endpoint.1.ConnectionType = Endpoint
```

```
# Optional
```

```
# Endpoint.1.SubnetAddress = 0.0.0.0
```

```
# Endpoint.1.SubnetMask = 0.0.0.0
```

```
# Endpoint.1.BindTo = 0.0.0.0
```

```
# Endpoint.1.SourcePort = 0
```

```
# Endpoint.1.Timeout = 90
```

## **Scenario B**

In this scenario, no traffic other than the gateways traffic is allowed outside the secure network. So we need a new gateway RC1 that will accept the requests from the controllers and pass them to RC2. Similarly, we need a new gateway RC3x in each of the unsecure networks to locate the right target.

### Gateway RC1:

Gateway RC1 will have the following configuration:

- Accept requests from controllers in the secure network.
- Connect to Gateway RC2 to forward the connections requests.

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = false

Inbound.1.AllowEndpoints = true

Gateway.RC2.ConnectionType = Gateway

Gateway.RC2.DestinationAddress = gatewayRC2_ipaddress

Gateway.RC2.DestinationPort = 8881

# Optional:

# Gateway.RC2.BindTo = 0.0.0.0

# Gateway.RC2.SourcePort = 0

# Gateway.RC2.RetryDelay = 45

# Gateway.RC2.KeepAlive = 900

# Gateway.RC2.Timeout = 90

# Gateway.RC2.Passphrase =
```

## Gateway RC2

In this scenario Gateway RC2 will have the following configuration:

- Accept control connections from gateway RC1.
- Connect to Gateways RC3x to forward the connections requests.

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = false
```

A gateway connection must be defined for each RC3 gateway (RC3a, RC3b, RC3c) where x = a, b or c.

```
Gateway.RC3x.ConnectionType = Gateway

Gateway.RC3x.DestinationAddress = gatewayT3x_ipaddress

Gateway.RC3x.DestinationPort = 8881

# Optional:

# Gateway.RC3x.BindTo = 0.0.0.0

# Gateway.RC3x.SourcePort = 0

# Gateway.RC3x.RetryDelay = 45

# Gateway.RC3x.KeepAlive = 900

# Gateway.RC3x.Timeout = 90

# Gateway.RC3x.Passphrase =
```

## Gateway RC3x

These gateways are now required to locate the endpoints that before were directly accessible to Gateway RC2. The configuration file for the gateways will contain the following entries:

```
Inbound.1.ConnectionType = Inbound
```

```
Inbound.1.PortToListen = 8881
```

```
# Optional:
```

```
# Inbound.1.BindTo = 0.0.0.0
```

```
# Inbound.1.RetryDelay = 45
```

```
# Inbound.1.Passphrase =
```

```
Inbound.1.AllowGateways = true
```

```
Inbound.1.AllowEndpoints = false
```

```
Endpoint.1.ConnectionType = Endpoint
```

```
# Optional
```

```
# Endpoint.1.SubnetAddress = 0.0.0.0
```

```
# Endpoint.1.SubnetMask = 0.0.0.0
```

```
# Endpoint.1.BindTo = 0.0.0.0
```

```
# Endpoint.1.SourcePort = 0
```

```
# Endpoint.1.Timeout = 90
```



## Appendix B. Properties for configuring logging activity

Use properties to determine what type of information and how much is written to the broker, gateway, and target component log files.

### LogLevel

The log level determines the types of entries and how much information is added to the log file. Default value is 2.

Logging level	Description
0	Minimal logging.
1	Error
2	Info
4	Debug information



**Note:** Use LOGLEVEL= 4 only by request from HCL software support.

### LogRotation

Controls the period after which an older log file is overwritten. Log rotation can be disabled. Default value is Weekly.

**A four-column table that shows the LogRotation parameter values and their definitions.**

LogRotation	Description	Suffix for hourly rollover	Suffix for daily rollover
Daily	Overwrite log files after 1 day	00H to 23H	Not valid
Weekly	Overwrite log files after 1 week.	Mon-00H to Sun-23H	Mon - Sun
Monthly	Overwrite log files after 1 month.	01-00H to 31-23H	01 - 31
Disabled	LogRotation is disabled	YYYY-MM-DD-hh	YYYY-MM-DD

The suffix is used in the name of the component log file. For example, `TRCICB-RCBROKER.example.com-Mon-14H.log`.

### LogRollover

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.

**A three-column table that shows the LogRollover parameter values and their definitions.**

<b>LogRollover</b>	<b>Description</b>	<b>Comments</b>
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.	Default setting.

# 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.