BigFix Remote Control Version 10 Readme

Contents

Chapter 1. About this Fix Pack

This readme file provides important information about BigFix Remote Control Version 10.1.0.

What is new in this release

A summary of changes, new features, and enhancements included in BigFix Remote Control v10.1.0.

TLSv1.3 Support

This release includes support for Transport Layer Security (TLS) version 1.3. By default, Remote Control components at 10.1 GA version operate in a backward compatibility mode. In this mode of operation, when the connection is between components at version 10.1, the TLSv1.3 protocol is used. Otherwise, the TLSv1.2 protocol is used.

Components at earlier versions are able to remain operative with no disruption. Also, newly deployed 10.1 components are able to operate within existing pre-10.1 environments. When planning for an upgrade to version 10.1, consider that there are no requirements on the components' upgrade order.

Once all product components are updated to version 10.1 or in case you are deploying a brand new Remote Control environment from scratch, it is possible to configure the product to operate in TLSv1.3 only mode. In this mode of operation, the only possible connection is between components that are at version 10.1.

Cipher suites Hardening

This release of the product adopts a set of cipher suites that are at the time of release rated more secure.

Subject Alternate Name Support

This release includes support for Subject Alternate Names (SAN) in certificate validation.

In past releases, Remote Control components were validating the server identity by means of the certificate Common Name (CN).

Starting from this release, the certificate SAN is also used when validating the server identity. This can be useful, for example, while dealing with Broker certificates when the internal broker name is different than the external broker name. Both DNS and IP Subject Alternate Names are supported.

Serviceability Enhancements

This release includes 4 new Fixlets in the maintenance category to collect log files and configuration for the different components.

- 408 - Collect Logs and Confs on BigFix Remote Control Target
- 409 - Collect Logs and Confs on BigFix Remote Control Gateway
- 410 - Collect Logs and Confs on BigFix Remote Control Broker
- 411 - Collect Logs and Confs on BigFix Remote Control Server

Refer to the fixlet description for usage notes.

Extended Group search for Users and for Target

In case of a complex user group or target group tree structure with many intersecting branches, it is possible that the default group search fails to detect the complete groups membership for a given user or target. These situations are very rare and can be linked to a complex user group structure when importing users from LDAP or when using a complex target group structure to reflect corporate structure.

This product release introduces the possibility to perform a full group search when resolving session policies. This possibility is controlled by the following properties in the *common.prorperties* file.

To enable full user group search, change the value of *user.group.search.full.tree* to *true*.

To enable full user group search, change the value of *target.group.search.full.tree* to *true*

Note: Pay attention when enabling the extended group search in an existing deployment as it may result in changes in session policies that are computed at session time.

Update of WAS Liberty and Java

This product release adopts the following:

- IBM WAS Liberty version is 23.0.0.8
- IBM Java SDK version 8.0-SR8-FP10
- IBM Semeru JRE version 8u382

Starting from this release, the Linux server installer adopts a 64-bit JRE.

Adoption of OpenSSL3

This product release adopts OpenSSL version 3.1.3 with the FIPS module version 3.0.9.

This product release also includes a complimentary copy of the openssl executable in the broker and target packages to aid in problem determination and/or certificate operations. The executable is available in the installation path.

Fixes included in this Fix Pack

BigFix Remote Control Version 10.1.0 contains the following fixes:

- KB0105778: Full User Group/Target Group search for policy determination
- KB0105721: Cannot use the remote CLI commands to run DOS commands on the target
- KB0107056: LDAP Failures during synchronization can cause undesired user deletion
- KB0107954: DB2 Selection in Server Wizard results in Derby Install Instead
- KB0107980: Tasks created with the RC Target Wizard are not visible on the load panel
- KB0108711: Targets with large MAC Address list cannot register to the RC Server

- KB0108239: (Doc) P2P issues with Num-lock and "Send CTRL + ALT + DEL"
- KB0108320: (Doc) Auditing - Accessing Event Viewer
- KB0106436: (Doc) Use of CA certificate for RC single sign-on configuration
- KB0107951: (Doc) Missing information for Apple Silicon architecture support

Known problems and limitations

Fix Pack version of BigFix Remote Control V10.1.0 GA	Known problems and limitations
	• **10.1 Broker in FIPS mode no longer supports .p12 keystore type** The following error appears in the Broker log file when the Broker is configured to operate in FIPS mode and a .p12 keystore is used to contain the broker keys. PKCS12_parse: 14460000:error:0308010C:digital envelope routines: inner_evp_generic_fetch:unsupported:crypto\evp\evp_fetch.c:341:Global default library context, Algorithm (PKCS12KDF : 187), Properties (<null>) This is caused by OpenSSL3 that no longer allows PKCS12KDF algorithm when in FIPS mode. The work around for this issue is to convert the .p12 keystore in a .pem keystore. You can use the complimentary openssl executable included along with the broker binaries. The PEM file needs to contain the following items, in the order listed below: ◦ Broker's certificate ◦ Any intermediate certificates, if required ◦ Root certificate ◦ Broker's private key Use the following openssl commands to convert the .p12 in .pem where keystore is your keystore file. Use your existing keystore passwords when prompted. ◦ openssl pkcs12 -nokeys -in keystore.p12 > keystore.pem ◦ openssl pkcs12 -nocerts -in keystore.p12 >> keystore.pem If your keystore.p12 already contains a CA signed certificate the intermediate and root certificate the keystore.pem should contain them, otherwise add them manually to the .pem file. Update the *trc_broker.properties* to reference keystore.pem in place of the keystore.p12.

Fix Pack version of BigFix Remote Control V10.1.0 GA	Known problems and limitations
	You may need to add the path where openssl is to the PATH and to the LD_LIBRARY_PATH environment variables before you can run the complementary openssl depending on the platform. • **Review Existing Broker Configuration after the upgrade to 10.1** A Broker upgrade may overwrite the existing *trc_broker.properties* file. Make a backup copy of the *trc_broker.properties* before proceeding with the upgrade. After the upgrade review your current broker configuration and remove any existing *DefaultTLSCipherList*, *DefaultHTTPSCipherList*, *ServerTLS**, and *UseTLS** properties to ensure that the Broker operates with version 10.1.0 hardened configuration. • **A 10.1 Environment in FIPS mode may experience connection errors using old Controllers.** The following error may appear in the controller log file when a Pre 10.1 Controller attempts to establish a session with a 10.1 Target (Managed or Peer to Peer) CertificateNonNistException: Detected a non RSA certificate when in NIST mode It is recommended to upgrade the controllers first when planning an upgrade to version 10.1 and the environment is configured in FIPS. No restrictions apply if the environment is not configured in FIPS. • **A 10.1 Environment in FIPS mode cannot enable TLSv1.3 Only mode of operation.** The IBM Java JCE FIPS 140-2 Cryptographic Module included in the Remote Control Server does not support the TLSv1.3 protocols. This implies that in a Managed Mode environment configured in FIPS mode it is not possible to operate the product in a TLSv1.3 only mode. In a Remote Control version 10.1.0 environment configured in FIPS the connections between Components will always occur using FIPS certified providers. When the connection occurs between Target, Controller, and Brokers the connection uses the TLSv1.3 protocol. When the connection occurs between the components and the Remote Control Server the connection uses the TLSv1.2 protocol. A future release of Remote Control will include a FIPS Certified Java Cryptographic Module capable of TLSv1.3 as soon as IBM provides one. • **Pre 10.1 Managed Targets may establish a session with a pre 10.1 controller even if TLSv1.3 only mode has been activated**

Fix Pack version of BigFix Remote Control V10.1.0 GA	Known problems and limitations
	A Managed Target of version pre 10.1 that is configured AllowP2P=yes AllowP2P-failover=yes may be able to accept and establish a session from a Controller of version pre 10.1 configured even if the environment is set to operate in TLSv1.3 Only. This is an extremely rare condition that is triggered by an improper activation of the TLSv1.3 only mode and by the managed target call home history at the time of the session establishment. Ensure that all your components are at 10.1 version before activating the TLSv1.3 Only mode.

For other known issues and limitations, see the Release Notes in the BigFix Remote Control Knowledge Center: https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Rel_Notes/r_release_notes_RC10FP8.html

Chapter 2. Installation information

Read the following sections before you install BigFix Remote Control Version 10.1.0.

Prior to installation

Installing the fix pack after installing the version 10 GA level (10.0.0.0029)

If you are installing the fix pack immediately after installing the version 10 GA Level (10.0.0.0029), log on to the GA Level application after it has installed to ensure that the database initialization has completed before applying the fix pack.

Note: It is not necessary to install the GA version prior to installing this fix pack.

Back up your properties and recordings files

If you have the server component installed and running you must backup your existing property files before installing the fix pack and also backup any recordings files that you have.

Back up the following property files:

- common.properties
- ldap.properties
- trc.properties
- controller.properties
- log4j.properties
- ondemand.properties

These files are found in the following path for Windows based systems:

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

These files are found in the following path for Unix based systems :

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

where `[TRCInstallDir]` is the BigFix Remote Control Server installation directory.

The video recordings folder is defined in the rc.recording.directory property in the trc.properties file. The default locations are:

In manual Installations on Windows:

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\rc_recordings
```

In automated Installations:

- In Linux: `[TRCInstallDir]/wlp/usr/servers/trcserver/rc_recordings`
- In Windows: `[TRCInstallDir]\wlp\usr\servers\trcserver\rc_recordings`

Back up any certificate files

This step is necessary only if you have previously manually installed a certificate. It applies only to an automated server installation.

The certificates are stored by default in a keystore file `key.jks` in the following paths:

- Windows:

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

- Linux:

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

If the default keystore file location or keystore password are changed, also back up the file `memory.xml` stored in the following paths:

- Windows:

  ```
  [TRCInstallDir]\wlp\usr\servers\trcserver\memory.xml
  ```

- Linux:

  ```
  [TRCInstallDir]/wlp/usr/servers/trcserver/memory.xml
  ```

Installing

Although it is not required, it is suggested that when you apply a fix pack that you upgrade all of your components to the latest level.

BigFix Remote Control 10.0.0 Windows Server Installation with a WebSphere Application Server 19.0.0.11 Liberty Profile

1. Decompress BigFix_Rem_Cntrl_V10_Image3.tar and navigate to `trc_server_setup.exe`
2. Run `trc_server_setup.exe`
3. Follow the instructions displayed on your screen to install the fix pack
4. If more detailed information is required, refer to the BigFix Remote Control Installation Guide and the chapter that describes installing the server using the server installer:

   https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_server_installer.html

BigFix Remote Control 10.0.0 Linux Server Installation with a WebSphere Application Server 19.0.0.11 Liberty Profile

1. Untar BigFix_Rem_Cntrl_V10_Image_3.tar and navigate to `trc_server_setup.bin`
2. Run `trc_server_setup.exe`
3. Follow the instructions displayed on your screen to install the fix pack
4. If more detailed information is required, refer to the BigFix Remote Control Installation Guide and the chapter that describes installing the server using the server installer:

   https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_server_installer.html

Manual Installation

If you are using BigFix_Rem_Cntrl_V10_Image_3.tar to perform a manual installation of this release, note:

A manual installation can only be performed on a system that has the previous release of BigFix for Remote Control already installed.

The following sections describe the different manual installations.

BigFix Remote Control 10.0.0 WebSphere Application Server (WAS), AIX, Linux, Solaris and Windows Server Installation

❗ **Important:** Back up your video recordings and customized properties files

Untar BigFix_Rem_Cntrl_V10_Image_3.tar and navigate to \Disk1\InstData\[platform]\VM where [platform] is relevant to your operating system. For example:

```
\Disk1\InstData\windows\VM
```

- AIX: Run `trc_additional_setup.bin`
- Linux: Run `trc_additional_setup.bin`
- Solaris: Run `trc_additional_setup.bin`
- Windows: Run `trc_additional_setup.exe`

For AIX, Linux, and Solaris:

1. Run `trc_additional_setup.bin`.
2. Follow the instructions in the BigFix Remote Control Installation Guide in the chapter that describes how to extract the component installation files: https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst-addiitional_install.html

   The new war file will be saved to a place of your choice or the InstallAnywhere default location.

3. Use the WAS Administrative Console to update the war file.
4. Follow the steps in the Post installation section to perform the necessary tasks after the installation.

Note: After a manual installation of the BigFix Remote Control Server on an AIX system, the default admin id and password are case sensitive and should be typed as follows :

```
id = Admin                    password = password
```

For Windows:

1. Run trc_additional_setup.exe.
2. Follow the instructions in the BigFix Remote Control Installation Guide in the chapter that describes how to extract the component installation files.

   https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst-addiitional_install.html. The new war file will be saved to a place of your choice or the InstallAnywhere default location.
3. Use the WAS Administrative Console to update the war file.
4. Follow the steps in the Post installation section to perform the necessary tasks after the installation.

Component Installation

For more information about installing the components, see https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_comp_install.html

Windows components:

1. Unzip BigFix_Rem_Cntrl_V10_Image_3.tar
2. Use the relevant installation files to install the components.

- **Target:** `trc_target_setup.exe` or `trc_target.msi`
- **Controller:** `trc_controller_setup.exe` or `trc_controller.msi`
- **Gateway:** `trc_gateway_setup.exe or trc_gateway.msi`
- **Broker:** `trc_broker_setup.exe or trc_broker.msi`
- **CLI:** `trc_cli_setup.exe or trc_cli.msi`

Linux components:

1. Extract the additional setup utility file from BigFix_Rem_Cntrl_V10_Image_3.tar
2. Run the file that is relevant to the operating system that you will run the utility on. See the installation guide for a description about how to extract the component installation files:

   https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst-addiitional_install.html

3. Use the following files to install the components.
    - **Target:** `trc-target-10.0.0.i386.rpm or trc-target-10.0.0.src.rpm`
    - **Controller:** `trc-controller-10.0.0.noarch.rpm and trc-controller-jre-10.0.0.i386.rpm`
    - **Gateway:** `trc-gateway-10.0.0.i386.rpm or trc-gateway-10.0.0.src.rpm`
    - **Broker:** `trc-broker-10.i386.rpm or trc-broker-10.src.rpm`
    - **CLI:** `trc-cli-10.i386.rpm or trc-cli-10.src.rpm`
4. Restart the component service for the component that you upgraded. For more information about restarting the component services, see the BigFix Remote Control Installation Guide:

    https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_manage_linux_comps.html

BigFix Console Installation

You can use the BigFix Console to deploy the upgraded version of BigFix Remote Control. The Fixlets are available on Remote Control site 55.

The Update node in the Remote Control navigation tree provides two sub-nodes which are operating system specific. These sub-nodes provide the latest levels of the target, controller, CLI and gateway components. If you have an older version of the BigFix Remote Control components already installed in your environment, you can use the Update node to upgrade these components to a newer version.

To upgrade the server component you can create and run a new server installation task by using the BigFix Remote Control Server Installer Wizard.

See the BigFix Remote Control Console Users Guide in the BigFix Remote Control Knowledge Center and the section that describes creating the server installation tasks.

https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_TEMUser_Guide/rcusrmanageconfig.html

Post installation tasks

Complete one or more of these tasks after installation completes, depending on your configuration.

Edit the properties files

After completing the update and confirming that 10.0.0.0029 is installed, edit the new trc.properties and ldap.properties files and update them with the values in your saved files.

Restore your other saved properties files and video recordings.

Note: It is only necessary to update the properties files after a manual upgrade or if the properties files have not been successfully restored after an automated upgrade.

Restore Certificate files

Note: This section should only be carried out if you have previously manually installed a certificate. It also only applies to an automated BigFix Remote Control server installation.

Restore the saved keystore file key.jks. If using the default keystore, it must be restored to:

Windows

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

Linux

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

If the password or the location of the keystore were changed, modify the file memory.xml and set the parameters of the element <keyStore> with the same values as the memory.xml file that was backed up as instructed previously.

The `memory.xml` file can be found at:

Windows

```
[TRCInstallDir]\wlp\usr\servers\trcserver
```

Linux

```
[TRCInstallDir]/wlp/usr/servers/trcserver
```

Chapter 3. Uninstallation information

Read the following sections to uninstall this fix pack.

Uninstallation Steps

To uninstall this fix pack, perform the following steps:

1. Back up and save your properties files. These files are located in the following directories:
   - **Windows based systems:** `[TRCInstallDir]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes\`
   - **UNIX based systems.**`TRCInstallDir]/wlp/usr/servers/trcserver/apps/ TRCAPP.ear/trc..war/WEB-INF/classes/`

   where `TRCInstallDir` is the BigFix Remote Control server installation directory.
2. Back up your database by following the standard procedure as documented by your database provider.
3. Uninstall the BigFix Remote Control Server. To uninstall the Server, complete one of the following steps:
   a. Within Add/Remove programs select to Uninstall BigFix Remote Control - Server
   b. Run the uninstall application:

      Run the `Uninstall BigFix Remote Control-Server.exe` file which can be found in the BigFix Remote Control server installation directory.
4. Install the previous version of BigFix Remote Control.

   For installation instructions, see the BigFix Remote Control Installation Guide: https://help.hcltechsw.com/bigfix/10.0/lifecycle/Lifecycle/Remote_Control/RC_Install_Guide/rcinst_introduction.html
5. Stop the BigFix Remote Control service.
6. Restore your properties files and database.
7. Start the BigFix Remote Control Service.

Appendix A. Support

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

- BigFix V10.0 Lifecycle Documentation
- HCL Software Support
- HCL portal for BigFix Support
- BigFix Developer
- BigFix Forum

Appendix B. Notices and trademarks

The following section includes important information about this document and its use.

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.