BigFix Application Control Version 1.0 Readme

Contents

Chapter 1. About this Release

This readme file provides important information about BigFix Application Control Version 1.0.0.

What is new in this release

A summary of new features, changes, and enhancements included in BigFix Application Control V1.0.0.

BigFix® Application Control V1.0.0

Features that are introduced in Application Control V1.0.0

BigFix® Application Control is a lightweight, native enforcement system designed for comprehensive management of application execution across enterprise endpoints. The solution addresses the critical need for native, policy-driven application control within BigFix environments, enabling IT administrators to enforce application usage policies with real-time monitoring and exception management capabilities.

What's New in Application Control V1.0.0

This release focuses on providing a robust, stable, and secure foundation for application control.

Centralized Policy and Rule Management

Configure and deploy the solution from the BigFix console. Create powerful Allow Rules (for default-deny policies) or Block Rules (for default-allow policies) to control application execution. Rules can also include time constraints to grant temporary access.

Bulk Ruleset Management

Easily upload a CSV file containing a set of rules to apply a baseline policy across all subscribed computers.

Endpoint Visibility

See the effective control policy (the complete set of rules) for any endpoint directly from the BigFix Console. Approved exceptions can be viewed using BigFix® Web Reports.

Real-time Block Notifications

When a process is blocked, a notification utility instantly appears, informing the user that the application is not permitted to run.

Application Control Policy

The collection of individual rules and CSV rulesets that are applied to an endpoint to restrict or allow application execution.

Seamless Exception Request Work-flow

The notification utility allows users to request a temporary exception. They can provide a business justification and a desired expiration date, which is then sent directly to ServiceNow to create an exception request ticket.

For Security and Performance

Endpoint Policy Encryption Ensures Secure Monitoring and Immutable Rules

The effective policy on the endpoint is encrypted, ensuring that a user, even one with administrative privileges cannot modify the rules.

Lightweight Endpoint Service

A compiled C# *watcher service* enforces policies in real-time with minimal CPU and memory overhead, ensuring no impact on user productivity.

Log Retention

Endpoint logs are stored for 10 days to provide an audit trail of local activity.

This release contains the following key features:

Table 1. Key Features Application Control Release V1.0.0

Features	Description
Compliance Enforcement	Block unauthorized applications to meet corporate and regulatory requirements.
Policy Deployment	Administrators can add rules to block or allow apps using file paths or registry rules.
Process Monitoring	The Process Monitoring service on endpoints polls for policies and enforces them in real-time. When a blocked app is accessed, it is terminated, a notification is shown, and a log entry is created.
Exception Request Handling	Allow temporary, audited access to blocked applications with proper approval through your ITSM system.

ServiceNow Integration Workflow

Application Control integrates with ServiceNow to manage the exception Lifecycle:

1. **Setup**: A BigFix operator installs the Application Control UpdateSet XML in ServiceNow.
2. **Request**: The endpoint utility calls a ServiceNow REST API to create an exception request when a user submits one. Distributed Denial-of-Service (DDoS) protection is active, rate-limiting requests to 60 per hour.
3. **Approval**: The exception manager approves or denies the request within ServiceNow.
4. **Fulfillment**: Upon approval, ServiceNow calls the BigFix Action API to create and deploy a temporary allow rule to the specific endpoint. The ServiceNow ticket is then updated with a "fulfilled" status.

Additional information about this release

Published Site Versions:

Site Name	Site Version
Application Control	1.0.0

BigFix Application Control Documentation links:

- https://help.hcl-software.com/bigfix/11.0/lifecycle/lifecycle_application_control.html
- https://help.hcl-software.com/bigfix/10.0/lifecycle/lifecycle_application_control.html

Chapter 2. Installation information

You can perform the installation of BigFix Application Control in two steps by executing the specific Fixlet and tasks on the desired endpoints. First identify the endpoints that do not yet have Application Control on them. Second, run the installer Fixlet for BigFix Application Control on the desired endpoints to install Application Control on them.

Identifying Endpoints Not Configured for Application Control

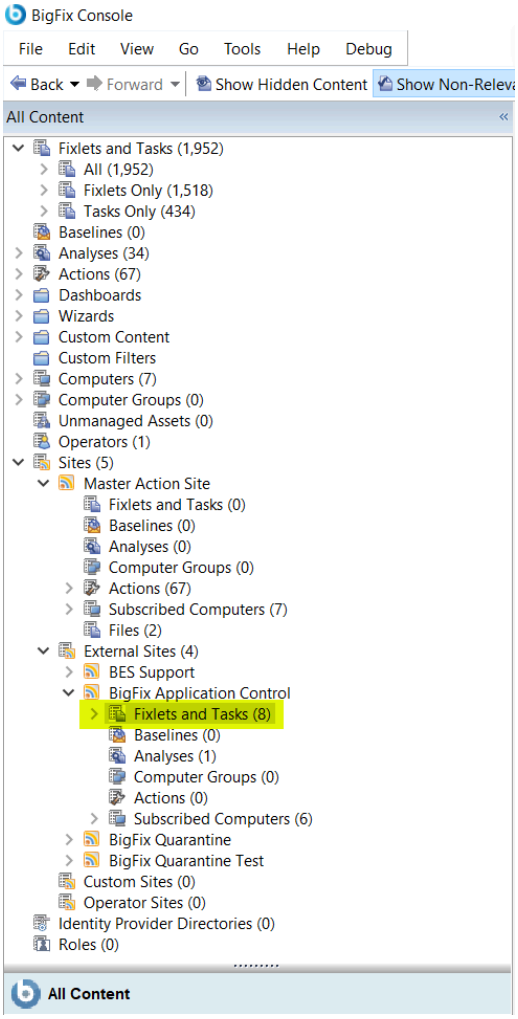
Use this Fixlet to identify endpoints that are not configured for Application Control, serving as a prerequisite for installation. This Fixlet lists devices that are not protected by the application but are subscribed to the external site, allowing administrators to assess endpoint readiness.

Use this Fixlet to identify endpoints that are not yet configured for BigFix Application Control.

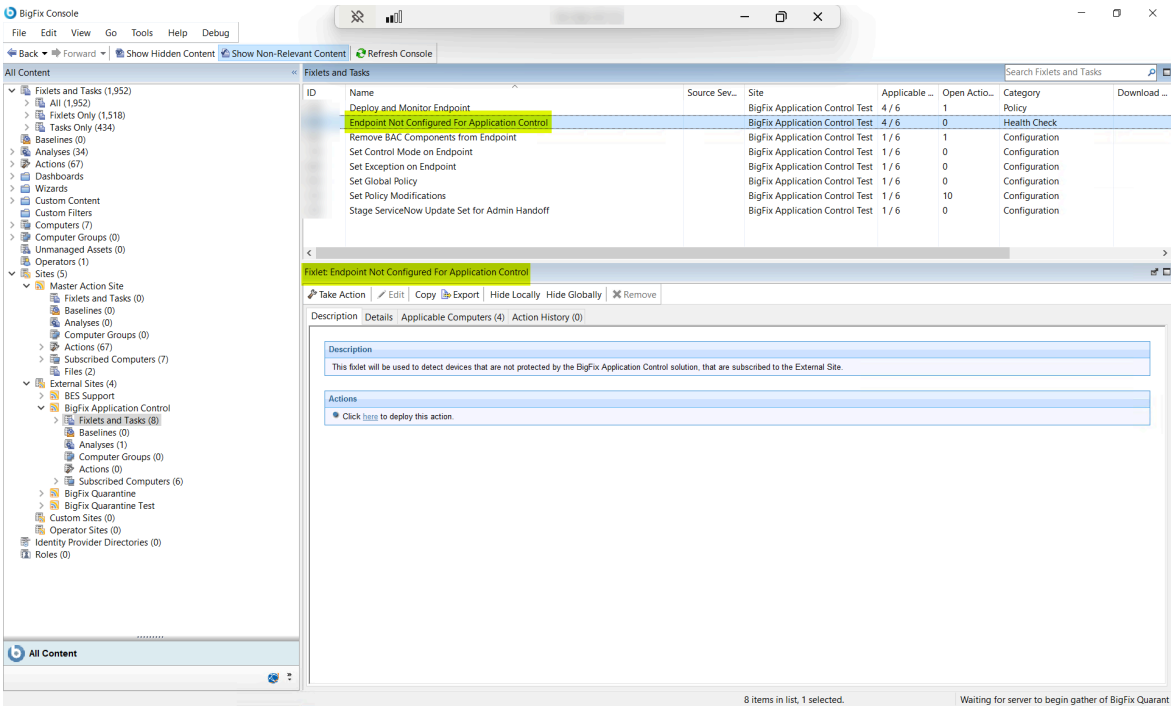
This identification step *can be* considered as a prerequisite for installing Application Control on an endpoint. You need to use **Fixlet: Endpoint Not Configured For Application Control** to identify the endpoints or devices that are not protected by BigFix Application Control but are subscribed to the external site. This Fixlet will list the devices on which you can configure Application Control.

1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.

Figure 1. Navigate to Fixlets & Tasks

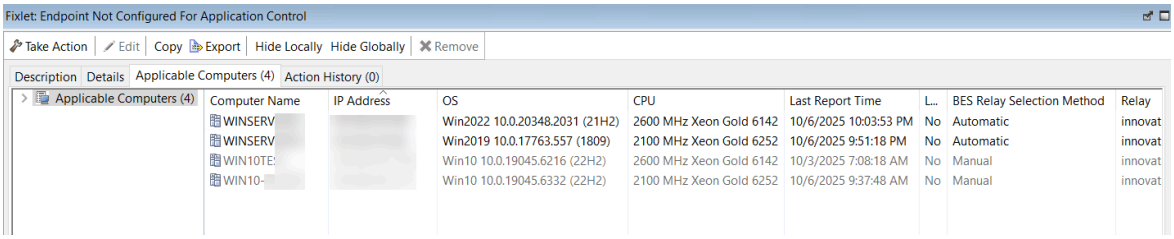


2. From the **Fixlets and Tasks** pane, select **Fixlet: Endpoint Not Configured For Application Control**.



This Fixlet does not contain any action script and the result set is based on client relevance's to get the details of devices not managed by Application Control.

3. Select the **Applicable Computers** tab and view the list of devices not managed by Application Control.



This Fixlet is more of a health-check Fixlet that can be used by administrators before installing the solution on any BigFix® managed endpoint.

Deploying & Monitoring Endpoints Using Application Control

This topic outlines the process for deploying and monitoring endpoints using Application Control through a specific installer task. It details the steps for installation, service configuration, and policy enforcement to ensure application allowlisting and unauthorized process blocking on managed endpoints.

It is recommended to first run the **Fixlet: Endpoint Not Configured For Application Control** to identify non-managed endpoints before running the installer task.

Use this task to deploy and monitor Application Control to endpoints that are not yet managed by the solution.

You can install BigFix Application Control using **Task: Deploy And Monitor Endpoint**. By running this task on an endpoint, you will deploy and activate a custom BigFix® Application Control (BAC) service on a Windows™ endpoint and a user pop-up service. This service enforces an application allowlisting policy and blocks unauthorized processes from running on the endpoint.

This task performs a multi-step process to install, configure, and enable the BAC service to monitor and control application software. The steps are as follows:

1. **Installation & setup**

   In this step, the task first downloads the three pre-requisite files - `.NET 8 SDK`, `ProcessMonitorService.zip`, and `NotificationUtility.zip`. Post downloading, the task installs the .NET 8 SDK, creates a dedicated folder at `\Program Files (x86)\ BigFix Enterprise\ BES Client\BAC`, and unzips the `ProcessMonitorService.zip` and `NotificationUtility.zip` files in the folder.

2. **Service & policy configuration**

   In this step, the task creates a Windows™ service called `BESBAC`. This service is configured to:
   - run the ProcessMonitorService.exe,
   - start automatically with the system, and
   - automatically attempt to restart if it fails.

   Next, the task deploys a security policy by generating a JSON policy file `effective_policy.json`. This policy works in a default-deny mode, which means that all applications are blocked for running except those explicitly allowed. The initial policy is a allowlist for:
   - essential Windows™ system processes
   - BigFix agent processes
   - any other processes running from `C:\Windows directory`

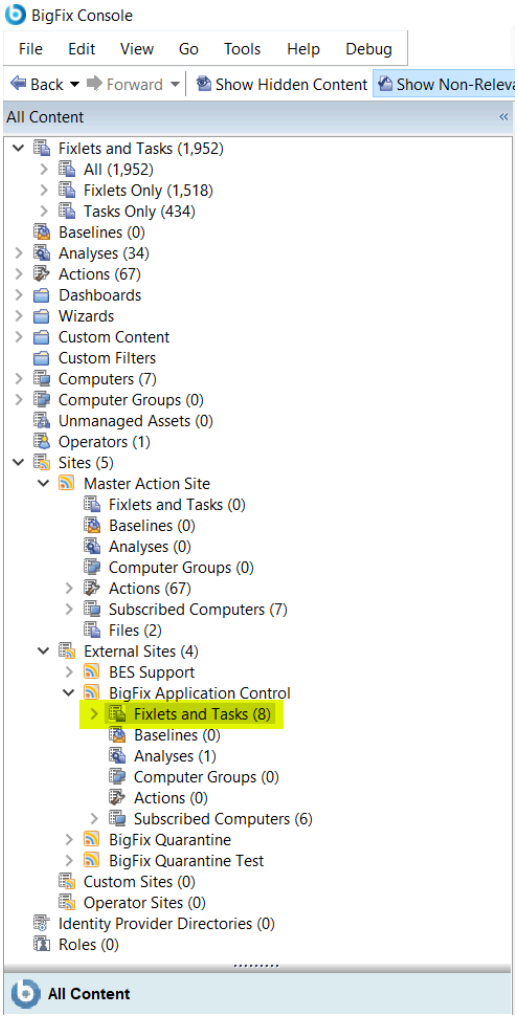
3. **Activation & Monitoring**

   In this step, the task starts the `BESBAC` service and immediately begins enforcing the security policy. Next, it creates a monitoring task named `BAC Monitoring Service` that runs every 5 minutes to check if the `BESClient` and `BESBAC` are running. If either of the services are stopped, the monitoring service restarts it ensuring that the solution is always active.

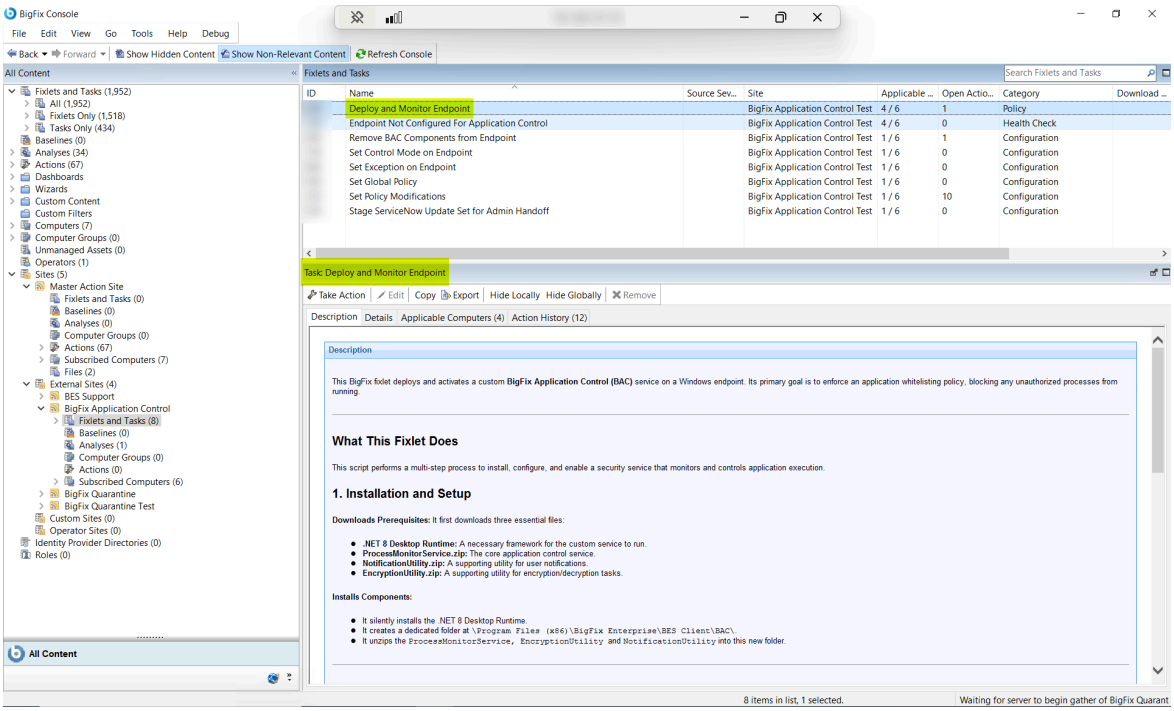
Follow the steps below to deploy the Application Control on the endpoints:

1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.

Figure 2. Navigate to Fixlets & Tasks



2. From the **Fixlets and Tasks** pane, select **Task: Deploy And Monitor Endpoint**.



This task does not contain any action script and the result set is based on client relevance to get the details of devices not managed by Application Control.

3. From the **Task: Deploy And Monitor Endpoint** pane, under **Configuration Options** enter the following information:

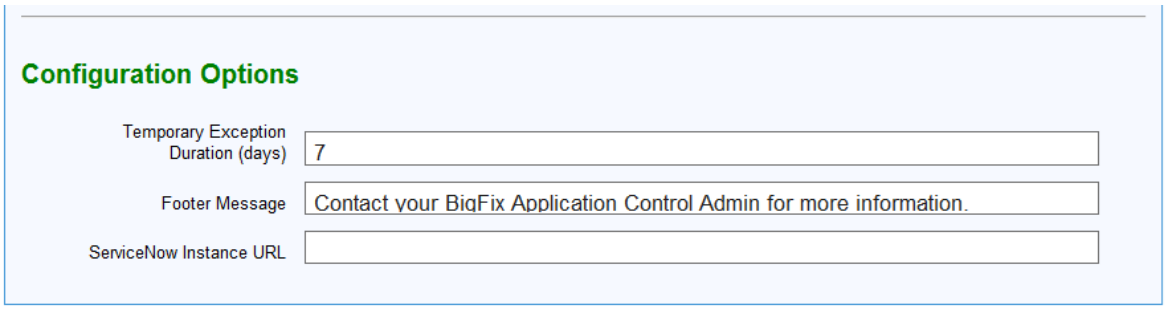


Table 2. Task: Deploy And Monitor Endpoint Configuration Options

Field Name	Description
Temporary Exception Duration (days)	Number of days for which the block listed applications are to be allowed for usage as per your organization's policies.
Footer Message	Message to be displayed to the endpoint users when they are raising exception requests.
ServiceNow Instance URL	Your organization's ServiceNow™ instance URL where the tickets are created for the exceptions raised by Application Control end-users.

4. From the **Task: Deploy And Monitor Endpoint** pane, click the **Applicable Computers(n)** tab and view the endpoints on which you want to run the task.
5. Select the **Take Actions** tab and select the endpoints on which you want to apply this installer task.
6. Click **OK**.

Chapter 3. Remove BigFix® Application Control from an Endpoint

This topic provides instructions for administrators to remove Application Control from target endpoints using the Task: Remove BAC Components from Endpoints. This process involves stopping the BAC service, deleting associated files, and cleaning user profiles.

Learn how to remove BigFix Application Control from managed endpoints.

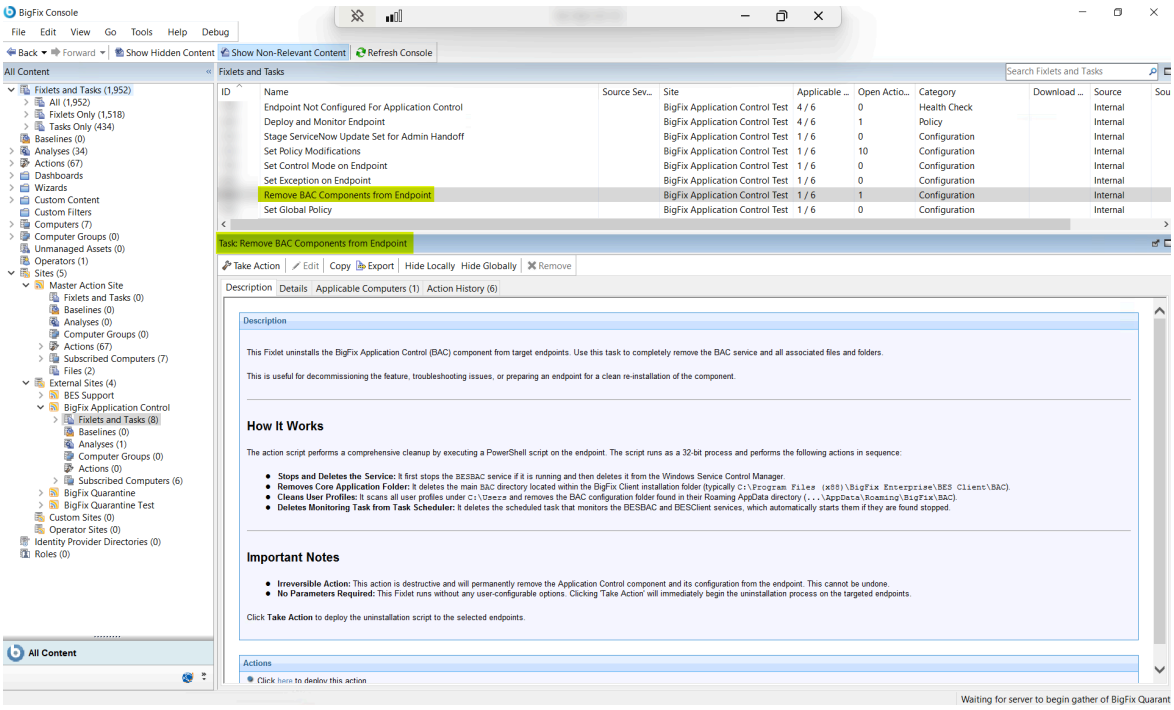
As an administrator, you can remove or uninstall BigFix Application Control from target endpoints. This task removes the BAC service and all associated files and folders from the target endpoints.

You use the **Task: Remove BAC Components from Endpoints** for uninstalling **Application Control**. This task performs the following actions:

1. Stops and deletes the BESBAC service from Windows™ Service Control Manager.
2. Removes the BAC directory located in the BigFix Client installation folder.
3. Scans and cleans user profiles by removing the BAC folder from their Roaming AppData directory.
4. Deletes the task that monitors BESBAC and `BESClient` services.

Follow the steps below to configure the watcher service refresh interval:

1. From the **Fixlets and Tasks** pane, select **Task: Remove BAC Components from Endpoint**.



2. Select the **Take Actions** tab and select the endpoints from which you want to remove BigFix Application Control.
3. Click **OK**.

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.