Application Control 2.x Setup Guide

Special notice

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

Edition notice

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

Contents

Chapter 1. Architecture Overview **5**

Chapter 2. System Requirements **7**

Chapter 3. BigFix Console Site Setup **9**

Enable the BAC Site 10

Subscribe Target Computers 10

Configure Web Reports and Event Collection 11

Chapter 4. Task Execution Workflow **14**

Chapter 5. Operational Best Practices **17**

Notices xix

Index .....

Chapter 1. BigFix Application Control 2.x: Architecture and Component Overview

BigFix Application Control (BAC) 2.x centralizes Windows Defender Application Control (WDAC) policy management on a dedicated WDAC Management Node. All policy compilation, TPM 2.0-based code signing, and endpoint binary delivery are handled by this node — eliminating endpoint-side scripting and reducing the attack surface across your managed fleet.

What BAC 2.x introduces

BAC 2.x offloads all policy creation, binary compilation, validation, and code-signing to a single, isolated *WDAC Management Node*. The Management Node holds the hardware TPM 2.0-protected signing identity, so compiled `.cip` policy binaries delivered to endpoints are pre-signed and require no local scripting to apply.

This architecture replaces earlier models where policy-related scripts ran directly on managed endpoints, reducing the attack surface and simplifying compliance auditing.

Core architectural components

BAC 2.x spans three tiers of infrastructure:

BigFix Root Server

Hosts BAC deployment configurations and publishes site content to subscribed endpoints. All Fixlet and Task content originates here.

WDAC Management Node

The central authority for policy authoring, XML-to-binary compilation, TPM-based signing, and staging. Policy assets are pushed from this node to BigFix Custom Sites before distribution.

Target Client Endpoints

Production endpoints that receive pre-compiled, pre-signed `.cip` binaries and enforce them through the native Windows Code Integrity engine. No policy-generation logic runs on these endpoints.

Custom site lifecycle: Review, Deployed, and Archive

BAC 2.x organizes policy assets across three custom BigFix sites, each prefixed with a configurable site prefix:

- **<Prefix>_Review** — Holds draft XML policy files for administrative inspection and rule verification before publication.
- **<Prefix>_Deployed** — Houses compiled, TPM-signed `.cip` binaries approved for active production enforcement.
- **<Prefix>_Archive** — Preserves historical XML source and compiled binaries whenever policies are updated, maintaining a full audit trail.

Relationship to Windows Defender Application Control

BAC 2.x manages both *Base Policies* and *Supplemental Policies* in WDAC XML format. The Management Node compiles these XML definitions into binary `.cip` files, signs them, and stages them for BigFix-driven deployment. Endpoints apply the binaries through the native Windows Code Integrity engine without requiring any BAC-specific runtime components.

Setup and deployment

BAC 2.x System Requirements and Infrastructure Prerequisites *(on page 7)*

Enable the BigFix Application Control Site *(on page 10)*

BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*

Governance and operations

BAC 2.x Operational Best Practices and Governance *(on page 17)*

Chapter 2. BAC 2.x System Requirements and Infrastructure Prerequisites

Verify that every host in your BAC 2.x deployment — BigFix Root Server, WDAC Management Node, and target client endpoints — meets the minimum hardware, operating system, and security specifications before you begin installation. The WDAC Management Node requires hardware TPM 2.0; this is a hard requirement with no software alternative.

BigFix Root Server

Role: Hosts BAC deployment configurations and manages site content publication workflows.

Specification	Requirement
Supported operating systems	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
CPU	4 cores minimum; 8 cores recommended
RAM	16 GB minimum; 32 GB recommended

WDAC Management Node

Role: Centralized node for policy authoring, binary compilation, TPM-based signing, validation, and staging.

Important: Hardware TPM 2.0 is required on the WDAC Management Node. The signing identity that authorizes all compiled `.cip` binaries is bound to this TPM. A node without TPM 2.0 cannot be used as a Management Node — there is no software fallback.

Specification	Requirement
Supported operating systems	• Windows 10 (version 1903 or later) • Windows 11 • Windows Server 2022 or later
CPU	4 cores minimum; 8 cores recommended
RAM	16 GB minimum; 32 GB recommended
Disk (free space)	80 GB minimum
Hardware security module	Hardware TPM 2.0 (required — no software alternative)

Target Client Endpoints

Role: Managed production endpoints that receive pre-compiled `.cip` policy binaries and enforce them through the native Windows Code Integrity engine. No BAC runtime components are required on these endpoints.

Specification	Requirement
Supported operating systems	• Windows 10 (version 1903 or later) • Windows 11 • Windows Server 2022 or later
CPU	2 cores minimum; 4 cores recommended
RAM	8 GB minimum
Disk (free space)	20 GB minimum

Next steps after verifying prerequisites

Enable the BigFix Application Control Site *(on page 10)*

BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*

Related concepts

BigFix Application Control 2.x: Architecture and Component Overview *(on page 5)*

Chapter 3. BigFix Console Site Setup for BAC 2.x

Before deploying any WDAC policies, complete three sequential setup steps in the BigFix Console: enable the BAC licensed site, subscribe target computers, and activate the reporting Analyses and event collection Task. All three steps must be completed in order — no policy content reaches endpoints until they are done.

Complete the following three steps in the BigFix Console before running any BAC Task sequence or deploying WDAC policies to endpoints. Each step depends on the previous one being complete.

1. **Enable the BAC site** — Activate the BigFix Application Control licensed site from **BigFix Management** > **License Overview**. This makes all BAC Fixlets, Tasks, and Analyses available in the console. Requires a Master Operator account and a valid BAC license. See Enable the BigFix Application Control Site in the BigFix Console *(on page 10)*.
2. **Subscribe target computers** — Define which managed endpoints receive BAC content by configuring computer subscriptions on the BAC site. Subscribe all computers or apply property-based filters to target a specific OS group or UAT ring first. See Subscribe Target Computers to the BigFix Application Control Site *(on page 10)*.
3. **Configure Web Reports and event collection** — Activate Analyses 304, 305, and 306 and deploy Task 365 so that policy inventory, certificate health, and blocked execution events are visible in BigFix Web Reports. Without this step, reporting data will not appear regardless of whether policies are deployed. See Configure BAC 2.x Web Reports and Blocked Event Collection *(on page 11)*.

Important: Do not proceed to the Task execution sequence (Tasks 351–357) until all three Console setup steps are complete. Running infrastructure Tasks before the site is subscribed and Analyses are active will leave reporting in an incomplete state that requires manual remediation.

Console setup steps

Enable the BigFix Application Control Site in the BigFix Console *(on page 10)*

Subscribe Target Computers to the BigFix Application Control Site *(on page 10)*

Configure BAC 2.x Web Reports and Blocked Event Collection *(on page 11)*

Before you begin

BAC 2.x System Requirements and Infrastructure Prerequisites *(on page 7)*

After Console setup

BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*

Enable the BigFix Application Control Site in the BigFix Console

Activate the BigFix Application Control (BAC) 2.x licensed site from the BigFix Console to make all BAC Fixlet, Task, and Analysis content available to your operators and subscribed endpoints. You must have Master Operator privileges and a valid BAC license to complete this step.

- Log in to the **BigFix Console** with a **Master Operator** account. Standard operator accounts cannot enable licensed sites.
- Confirm that your BigFix license includes BigFix Application Control. If the BAC entry does not appear in License Overview, contact your HCL Software account representative.
- Allow 5–10 minutes after activation for the Root Server to synchronize site content before proceeding to computer subscription.

1. In the bottom-left domain navigation panel of the **BigFix Console**, click **BigFix Management**.
2. In the left navigation tree, click **License Overview**.
3. Locate the **BigFix Application Control (BAC)** entry in the content list.
4. If prompted, accept the license agreement, then click **Enable**.
5. Wait for site content synchronization to complete.
   A notification banner appears in the bottom-right corner of the console when synchronization finishes. This typically takes several minutes, depending on network conditions between the Root Server and its Relays.

The BigFix Application Control site is active. BAC Fixlets, Tasks, and Analyses are now visible in the console under **All Content** > **Sites** > **External Sites**. No BAC content will be deployed to endpoints until you subscribe computers to the site and run the Task sequence.

Subscribe target endpoints to the BAC site. See Subscribe Target Computers to the BAC Site *(on page 10)*.

Continue setup

Subscribe Target Computers to the BAC Site *(on page 10)*

Configure Web Reports and Event Collection for BAC 2.x *(on page 11)*

Prerequisites and reference

BAC 2.x System Requirements and Infrastructure Prerequisites *(on page 7)*

BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*

Subscribe Target Computers to the BigFix Application Control Site

Control which managed endpoints receive BigFix Application Control (BAC) content by configuring computer subscriptions on the BAC site. Subscribe all computers or apply property-based filters to target specific OS platforms or computer groups before deploying WDAC policies.

- Complete site activation before subscribing computers. See Enable the BigFix Application Control Site *(on page 10)*.
- Log in to the **BigFix Console** with a **Master Operator** account. Standard operators cannot modify site subscriptions.
- Decide your subscription scope before proceeding: subscribe all computers for broad fleet coverage, or define property-based filters to limit the initial rollout to a controlled set (for example, a UAT ring or a specific OS group).

1. In the BigFix Console navigation panel, expand **All Content > Sites > External Sites**.
   The BAC site may also appear under **Systems Lifecycle** or **BigFix Management**, depending on your console configuration.
2. Click the **BigFix Application Control** site entry.
3. In the right-hand properties panel, select the **Computer Subscriptions** tab.
4. Choose a subscription scope:
   - Select **All Computers** to subscribe your entire managed fleet.
   - Select **Computers with properties matching** and define property-based filtering rules to limit subscription to specific OS platforms, computer groups, or other criteria.
5. Click **Save Changes**.

Subscribed endpoints now receive BAC site content. BAC Fixlets and Tasks are visible and evaluated for applicability against the subscribed computers. No policy is applied to endpoints until you run the Task execution sequence (Tasks 356 and 357). To verify subscription, navigate to the **Computers** tab on the BAC site and confirm that the expected endpoints appear in the list.

Activate the BAC reporting Analyses and deploy the event collection Task. See Configure Web Reports and Event Collection for BAC 2.x *(on page 11)*.

Continue setup

Configure Web Reports and Event Collection for BAC 2.x *(on page 11)*

BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*

Previous step

Enable the BigFix Application Control Site in the BigFix Console *(on page 10)*

Configure BAC 2.x Web Reports and Blocked Event Collection

Activate the three BAC 2.x reporting Analyses (304, 305, 306) and deploy Task 365 to your target endpoints so that policy inventory, certificate health, and blocked execution events are visible in BigFix Web Reports. Without these Analyses active, policy and block event data will not appear in Web Reports regardless of whether policies are deployed.

- Complete computer subscription before activating Analyses. See Subscribe Target Computers to the BAC Site *(on page 10)*.
- Confirm that BigFix Web Reports is accessible and configured for your environment. Analysis data is only surfaced in Web Reports — it does not appear in the BigFix Console content panels.
- You must have sufficient operator permissions in the **BigFix Console** to activate Analyses and deploy Tasks to target computers.

Part 1: Activate reporting Analyses

1. In the BigFix Console, navigate to the **BigFix Application Control** site content and select **Analyses**.
2. Activate each of the following three Analyses:
    a. Activate **Analysis 304 – Policy and Rule Inventory v2.x** to track deployed policy definitions, versions, and statuses.
    b. Activate **Analysis 305 – Certificate Monitor v2.x** to monitor signing certificate expiration and thumbprint validity.
    c. Activate **Analysis 306 – Blocked Events v2.x** to parse and report Code Integrity and AppLocker block events from subscribed endpoints.

    These Analyses collect policy versions, certificate validity, and block event data from subscribed endpoints and surface the results in BigFix Web Reports. Activate all three — each covers a distinct reporting dimension.

Part 2: Deploy the blocked event collection Task

3. Locate **Task 365 – Generate WDAC Code Integrity and AppLocker Blocked Events** in the BAC site content.
4. Deploy Task 365 to the target endpoints on a recurring schedule aligned to your reporting cadence.
    Task 365 triggers client-side log processing that collects local Code Integrity and AppLocker block events and publishes them into BigFix Web Reports for Analysis 306 to surface. Without Task 365 running periodically, Analysis 306 data will not be current. Schedule Task 365 based on how frequently your security team reviews block event reports.

Analyses 304, 305, and 306 are active and will begin collecting data from subscribed endpoints on their next evaluation cycle. Task 365 is deployed and will generate block event data on its configured schedule. To confirm, open BigFix Web Reports and verify that policy inventory and certificate entries appear under the BAC reporting views. Block event data will appear after Task 365 runs for the first time on target endpoints.

Proceed to the end-to-end Task execution workflow to install and configure BAC infrastructure, author policies, and deploy compiled binaries to endpoints. See BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*.

Continue setup

BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*

Previous steps

Enable the BigFix Application Control Site in the BigFix Console *(on page 10)*

Subscribe Target Computers to the BigFix Application Control Site *(on page 10)*

Governance

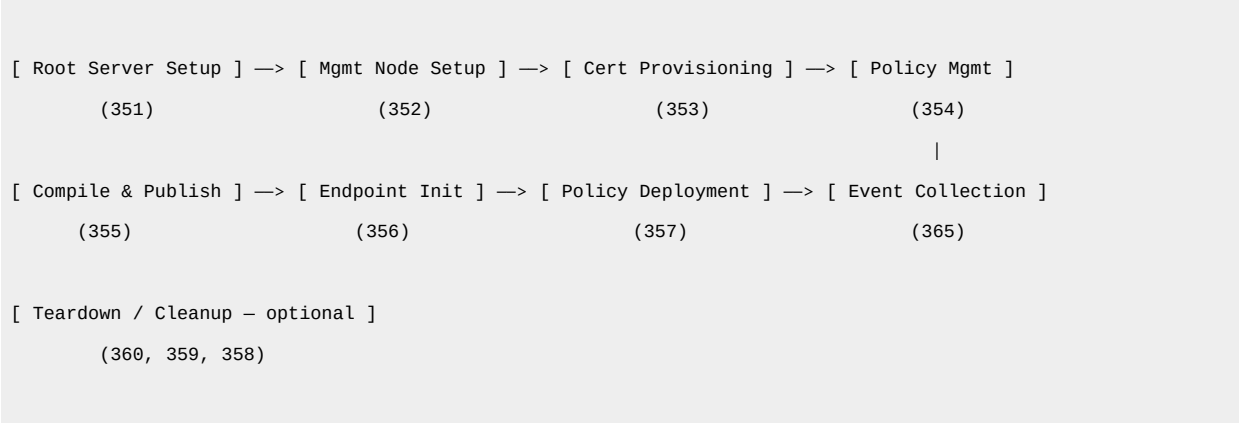
BAC 2.x Operational Best Practices and Governance *(on page 17)*

Chapter 4. BAC 2.x Task Execution Workflow and Fixlet Reference

BAC 2.x uses a fixed, ordered sequence of BigFix Fixlets and Tasks across three infrastructure tiers — Root Server, WDAC Management Node, and target client endpoints. Each phase depends on state established by the previous one; running Tasks out of sequence will produce configuration errors or leave endpoints in an incomplete policy state.

Required execution sequence

The following diagram shows the required execution order. Do not skip phases or run Tasks out of sequence — each phase depends on state established by the previous one.



BAC 2.x Fixlet and Task reference matrix

Table 1. Sequential Task and Analysis reference — BAC 2.x

Task / Analysis ID	Name	Target	Scope and action
351	BAC Configuration & Installation	BigFix Root Server	Installs and configures core BAC server modules and automated site distribution engines on the BigFix Root Server.
352	WDAC Management Node Configuration	Management Node	Prepares the isolated WDAC Management Node environment for central policy generation and staging.
353	Certificate Provisioning	Management Node	Provisions and binds the hardware TPM 2.0-protected code-signing identity used for binary policy authorization. A self-signed certificate can be generated directly on the Management Node for initial setup.

Table 1. Sequential Task and Analysis reference — BAC 2.x (continued)

Task / Analysis ID	Name	Target	Scope and action
354	Policy Management	Management Node	Authors, updates, and structures WDAC Base Policy and Supplemental Policy XML definitions.
355	Compile, Sign, and Publish	Management Node	Compiles policy XMLs into `.cip` binaries, executes TPM signing, and publishes assets to the three BAC Custom Sites (Review, Deployed, Archive).
356	WDAC Setup Initialization	Target Client Endpoints	Prepares client endpoint registry and Code Integrity file paths for incoming WDAC policy processing.
357	Policy Deployment and Refresh	Target Client Endpoints	Applies pre-compiled `.cip` policy binaries to active target paths and refreshes local Windows Code Integrity engine rules.
365	Generate WDAC Code Integrity and AppLocker Blocked Events	Target Client Endpoints	Triggers client-side log processing to collect and publish blocked execution events into BigFix Web Reports.
304 (Analysis)	Policy and Rule Inventory v2.x	BigFix Console	Collects and displays active policy definitions, versions, and deployment statuses across target devices.
305 (Analysis)	Certificate Monitor v2.x	BigFix Console	Monitors certificate expiration, validity, and thumbprint associations across managed environments.
306 (Analysis)	Blocked Events v2.x	BigFix Console	Parses and reports Code Integrity and AppLocker block events collected by Task 365.
360	WDAC Policy Cleanup	Target Client Endpoints	*Optional / Maintenance:* Purges deployed policy binaries from target paths during troubleshooting or decommissioning.
359	Management Node Teardown	Management Node	*Optional / Maintenance:* Resets Management Node configuration state during environment re-indexing or testing.
358	BAC Server Uninstall	BigFix Root Server	*Optional / Maintenance:* Removes BAC configuration components from the BigFix

Table 1. Sequential Task and Analysis reference — BAC 2.x (continued)

Task / Analysis ID	Name	Target	Scope and action
			Root Server during full teardown. Run after Tasks 360 and 359.

Setup prerequisites

BAC 2.x System Requirements and Infrastructure Prerequisites *(on page 7)*

Enable the BigFix Application Control Site in the BigFix Console *(on page 10)*

Subscribe Target Computers to the BigFix Application Control Site *(on page 10)*

Configure BAC 2.x Web Reports and Blocked Event Collection *(on page 11)*

Governance

BAC 2.x Operational Best Practices and Governance *(on page 17)*

Chapter 5. BAC 2.x Operational Best Practices and Governance

Apply these operational practices to maintain WDAC policy integrity, avoid production enforcement outages, preserve audit history in BigFix Web Reports, and manage the signing certificate lifecycle before expiration interrupts policy compilation in BAC 2.x.

Always validate in Audit Mode before promoting to Enforcement Mode

Always deploy new policies or policy changes in **Audit Mode** within a UAT ring before promoting to **Enforcement Mode** in production.

In Audit Mode, Windows Code Integrity logs blocked execution events without actually blocking them. This lets you identify legitimate applications that would be denied under the new policy — and add the appropriate rules — before enforcement affects production workloads.



CAUTION: Promoting a policy directly to Enforcement Mode without an Audit Mode validation pass risks blocking legitimate processes across all subscribed endpoints simultaneously. Review Analysis 306 block event data from your UAT ring before promoting any policy to production enforcement.

Site prefix lifecycle governance: Review, Deployed, and Archive

The BAC 2.x site engine uses a configurable *Site Prefix* to organize policy assets across three custom BigFix sites. Treat each site as a distinct stage in the policy promotion pipeline:

<Prefix>_Review

Holds draft XML policy files for administrative inspection and rule verification before publication. No policy in this site has been compiled or signed. This is the only stage where policy XML is safe to edit directly.

<Prefix>_Deployed

Houses compiled, TPM-signed `.cip` binaries approved for active production enforcement. Task 357 distributes content from this site to subscribed endpoints.

<Prefix>_Archive

Preserves historical XML source and compiled `.cip` binaries whenever policies are updated. This site provides the full audit trail of every policy version ever deployed.

Do not manually modify or delete content in the Archive site. The BAC automation manages this site as an immutable history record. Manual edits will corrupt the audit trail.

Preserve Web Reports audit history when removing rules

Assign unique names to each new policy iteration. When you need to disable an existing rule while retaining its history in BigFix Web Reports, use the **Purge Supplemental Policy Rule** Fixlet rather than overwriting the existing policy file.

Overwriting a policy file replaces the record in Web Reports and destroys the audit trail for that rule. The Purge Supplemental Policy Rule Fixlet disables the rule in a way that Analysis 306 tracks as a state change, preserving the full record of when the rule was active and when it was removed — which is essential for compliance audits and incident investigations.

Manage signing certificate expiration proactively

Use **Analysis 305 – Certificate Monitor v2.x** to track certificate expiration dates and thumbprint associations across your managed environment. A signing certificate that expires while policies are in active use will prevent Task 355 from compiling new `.cip` binaries until the certificate is renewed and re-provisioned via Task 353.

Plan certificate renewals well in advance of the expiration date. A signing outage during a critical policy update window — for example, during an incident response — has no short-term workaround other than an emergency renewal.

Reporting and monitoring

Configure BAC 2.x Web Reports and Blocked Event Collection *(on page 11)*

Task and Fixlet reference

BAC 2.x Task Execution Workflow and Fixlet Reference *(on page 14)*

Architecture

BigFix Application Control 2.x: Architecture and Component Overview *(on page 5)*

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.