

HCL BigFix Compliance v10

Course Summary

Description

BigFix Compliance enforces continuous compliance with security policies throughout an organization for every endpoint both on and off the corporate network. It includes out-of-the-box support for most popular security benchmarks published by CIS, DISA STIG, USGCB and PCI-DSS. An intelligent agent on every endpoint monitors, enforces and reports on the security configuration status of the endpoints in real-time regardless of OS type or location. In this course, students will learn to interact and operate the BigFix Compliance solution. They will gain a solid understanding of the various components of the solution and will be able to configure, operate, develop reports, perform maintenance tasks, and troubleshoot BigFix Compliance.

Objectives

After taking this course, students will be able to:

- Understand Key BigFix Compliance Concepts
- Understand the Features and Functions of BigFix Compliance
- Learn to Configure and Operate BigFix Compliance
- Create custom reports including creating groups; checklist targeting and exception
- Understand how to maintain BigFix Compliance
- Be able to perform basic troubleshooting techniques

Topics

- Overview including key concepts, features and functions of BigFix Compliance
- Design and install BigFix Compliance (architecture, infrastructure, and implementation)
- Configure and Operate BigFix Compliance including Navigation and Checklists
- Create a wide variety of reports for different stakeholders in the organization
- Deployment tasks and technologies
- Maintain BigFix Compliance
- Troubleshoot BigFix Compliance including Disaster Recovery planning

Prerequisites

Students should have: basic Microsoft Windows skills and have previously taken AIS BigFix Operator Fundamentals course, or equivalent experience.

Duration

One day

HCL BigFix Compliance v10

Course Outline

I. Overview

- A. Introduction, covering: benefits and advantages; the BigFix portfolio and adjacent products; roles and responsibilities; compliance motivators (Business Needs, IT Needs)
- B. Key Concepts, including: security vs. compliance; checklists and parameters; reporting; and enforcement
- C. Features and Functions, such as: enforcing compliance rules; reporting on compliance; and automation of process

II. Plan and Install

- A. Architecture of Compliance, including: Scalability (BigFix architecture, checklists, data import); network design; firewalls, proxy servers, and ports; network planning; and reporting groups
- B. BigFix Platform and Compliance Infrastructure, covering: server and database requirements; disk space; permissions; licensing & masthead; installing BigFix Server, relays, and clients; security and access
- C. Implementation of Compliance, including: installing the Compliance analytics server; subscribing systems to checklists; configuring data source connection; mail server settings; roles; server settings; session settings; and user provisioning

III. Configure and Operate

- A. Navigation, such as: interface navigation and customization, setting default views, creating custom views
- B. Using checks and checklists, including: check Fixlets; modifying check parameters; activating Measured Value Analyses; creating and managing Custom Checklists; using the Synchronize Custom Checks wizard; taking a remediation action; importing SCAP content; using OVALDI and viewing

IV. Exception Management

- A. Reporting, including: running and exporting reports; reviewing existing built-in overview and list reports; and customizing reports
- B. Computer Grouping, covering: creating computer groups for reporting; checklist targeting and exception; computer properties from BigFix

V. Maintain

- A. Compliance Application management, such as: Extract, Transform, Load monitoring and management; and database management
- B. BigFix Platform management, including: Fixlet site version; Platform updates and upgrades; process start and stop procedures; and backup & restore

VI. Troubleshoot

- A. Disaster Recovery planning, covering: backing up the Application Server; and successful recovery from a failure
- B. Support resources, including log locations; VM Manager command line options; manual catalog updates; support; Forums and self-help