HCL BigFix Version 10.0.1
Common Criteria Configuration Guide

Version: 2.0

Status: Final

Last Update: 12/01/2020

Document History

Version	Date	Author	Description
2.0	2020-12-01	HCL Technologies limited	Public Version

1 Contents

2 Preface

This document is a guidance document for administrators who wish to use HCL BigFix in a certified, Common Criteria (CC) compliant, secure configuration.

2.1 Audience

This document is written for administrators installing and configuring the HCL BigFix. This document assumes that you are familiar with the BigFix basic concepts and terminologies.

This guide includes the following sections:

1. Introduction and *Common Criteria (CC) Orientation and Roadmap* – General introduction and explanation of Common Criteria and the Protection Profile.
2. Specifications and References for the *HCL BigFix CC-Evaluated System* – Describes the TOE and evaluated components as well as how to obtain the CC-Evaluated product
3. *Installation and Environmental Configuration* – Initial install procedure for the TOE and supporting components.
4. *Enhanced Security Configuration and References* – Outlines all required steps taken after install that are necessary for bringing the TOE into compliance. Describes enhanced security features and how to use them.

3 Introduction

3.1 What is Common Criteria?

The *Common Criteria for Information Technology Security Evaluation (CC*) and the companion *Common Methodology for Information Technology Security Evaluation (CEM*) are the technical basis for *the Common Criteria Recognition Arrangement (CCRA*), which ensures:

- Commercial products are evaluated by independent licensed evaluation laboratories that determine the fulfilment of specified security properties to a specified level of assurance
- Certificate Authorizing Schemes certify the evaluation results produced by the evaluation labs and issue evaluation certificates accordingly
- Issued certificates are mutually recognized by the signatories to the CCRA.

For the documentation describing the Common Criteria evaluation process and methodology, see the documents at:

https://www.commoncriteriaportal.org/index.cfm

3.2 HCL BigFix technical documentation library

This Common Criteria evaluation is based on the English version of HCL BigFix and its documentation. The following technical documents provide standard information and procedures for installing and configuring the HCL BigFix. These documents were updated and revised for version 10.0.1:

- *BigFix Installation Guide* (BigFix_Installation_Guide.pdf)
- *BigFix Configuration Guide* (BigFix_Configuration_Guide.pdf)
- *BigFix Version 10.0.1 Action Script Guide* (BigFix_Action_Guide.pdf
- *BigFix Version 10.0.1 REST API* (BigFix_REST_API.pdf) BigFix
- *Console Operator's Guide* (BigFix_Console_Operators_Guide.pdf)

- *BigFix Version 10.0.1 Relevance Guide* (BigFix_Relevance_Guide.pdf)

The above documents are available at the following link:

https://help.hcltechsw.com/bigfix/10.0/platform/commoncriteria.html

This guide is intended to be used in conjunction with the above HCL BigFix documentation when installing and configuring a CC certified solution. This guide does not replace the above documentation, it rather supplements it by identifying specific configuration criteria that are required for a Common Criteria certified installation. Any configuration that falls outside of the evaluated configuration or security assumptions outlined in this guide should be considered an insecure state with respect to CC certification.

3.3 The evaluated Configuration

The version of HCL BigFix being certified is **version 10 patch 1** (build 10.0.1.41), to meet Common Criteria Evaluation Assurance, at version 3.1R5 level 2 (EAL2).

The evaluated configuration is the configuration in which the Common Criteria evaluation was performed. This is a specific configuration of HCL BigFix set up, which is outlined in this guide. This guide does not explain all the various features of the HCL BigFix, it rather focuses on how to configure the HCL BigFix for the CC evaluation. This configuration is often referenced as the Target of Evaluation (TOE).

This guide includes the list of features that can be used, or excluded, in an evaluated configuration, along with any needed guidelines for how to include (or exclude) these features from your configuration. Once installed and configured these features will provide the complete platform necessary to operate the HCL BigFix product in compliance with this evaluation.

The evaluated configuration assumes that the configuration is set up according to these guidelines, configurations that do not follow these guidelines are not considered evaluated configurations.

3.4 Assumptions

The TOE components are connected thru a closed local area network. The computer hosting the HCL BigFix Server, must have an internet access to connect to the license server and to gather the content from the external BigFix sites (BES sites). The internet access is secured by a firewall.

When a Domain Name System (DNS) service is used by the network, the DNS provides trustworthy services.

The hardware providing the runtime environment for the TOE is protected against unauthorized physical access and modification.

The hardware and software providing the runtime environment for the TOE Server and TOE Relays are used solely for this purpose and not to run other application software, except as required for the support of the TOE and for the management and maintenance of the underlying operating system and hardware.

The organization will ensure that administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the guidance and documentation for managing the TOE, and correctly configure and operate the TOE in accordance with those policies and procedures.

4 Specifications and References for the TOE

The TOE, and supporting environment, comprises a set of software images to be installed according to the steps contained in this guide.

The HCL BigFix is a distributed system comprising the BigFix Server, BigFix Relay, Bigfix Client, database, and BigFix Console.
Only the HCL BigFix Server, BigFix Console, BigFix Relay and BigFix Client have been assessed as the part of the evaluation, while other components are considered to provide supplementary functions in the IT environment.
In this guide the term when the “CC evaluated System” is referred to, please note this includes the TOE and supporting operational environment as described below.

4.1 Evaluated security functionality

This section describes the security functionality that was evaluated for the TOE. The list of evaluated functionality is:

- Cryptographic support
- User Data Protection
- Identification and authentication
- Security Management
- Protection of the TSF

4.1.1.1 Cryptographic support

The HCL BigFix provides uses encryption and digital signatures to guarantee the communications between all components.

4.1.1.2 User Data Protection

The TOE provides an Information Flow Control Security Function Policies (SFPs), that controls the ability to apply Actions to Clients. The Action SFP is based on the list subject of authorized subjects (operators allowed to administer machine). The TOE identifies users by user name and authenticates them by password. TOE Users can be organized by membership in BigFix Admin groups. Only hashes of the passwords are stored in the BigFix system. Password policies can be applied to enforce requirements on the quality of the password that a user chooses. Lockout mechanisms prevent password guessing attacks.

4.1.1.3 Identification and authentication

All administrative interfaces require each user to be successfully identified and authenticated before allowing any other action on behalf of that user. The TOE's administrative interfaces are:

- BigFix Administration console
- BigFix Console

The HCL BigFix provides mechanisms that mitigate the risk of unattended sessions being hijacked via timeouts for locking and subsequently terminating idle sessions.

4.1.1.4 Security Management

The TOE provides security management functions that can only be accessed by authorized administrators. Functionality and data in an HCL BigFix deployment can be restricted to certain users or groups. Users and groups can be granted administrator privileges over specific data or functionality. The TOE support three classes of users each of these user roles has different responsibilities and restrictions:

- Site Administrator
- Master Operators
- Non-Master Operators

4.1.1.5 Protection of the TSF

The TOE protects itself from attempts to bypass its security mechanisms. Data transfer is protected by the use of cryptographic signature verification to ensure authenticity and integrity of Fixlet and Action messages. The TOE uses TLS and TLS/HTTPS to protect the security and integrity of all sensitive data sent between the TOE components.

The HCL BigFix provides the capability to ensure that any updates to the TOE can be verified by the administrator to be unaltered and from a trusted source.

4.2 Component specifications for the CC-evaluated system

The CC-evaluated implementation of HCL BigFix is single server deployment. The list of CC-evaluated HCL BigFix components is:

- HCL BigFix Server software component (on Windows Server 2016)
- HCL BigFix Console software components (on Windows Server 2016)
- HCL BigFix Client software components (on Windows 10, Windows Server 2016, RHEL7)
- HCL BigFix Relay software components (on Windows 10)

4.3 Description of the Target of Evaluation (TOE)

This chapter describes the Target of Evaluation (TOE) configuration for HCL BigFix version 10.0.1 The evaluated configuration consists of the software, hardware, and guidance documentation specified in the above section 3.2 HCL BigFix technical documentation library. The evaluated configuration also imposes some security settings on the configuration of the product, those settings are described in section 7.3 Hardening the HCL BigFix

4.3.1 TOE Hardware

The customer can purchase the hardware components matching those used in the TOE evaluation that host the software components.

The TOE is deployed on the 3 physical machines, The BigFix Server, the Relay and the client.

4.3.1.1 BigFix Server hardware requirements

The BigFix Sever is deployed on a single server physical machine. The hardware resources of the physical computer strictly depends on the number of managed computers (clients), and affects the

TOE performance, which is however out of the scope in the Common Criteria evaluation. For this evaluation, a low-medium set of system resources have been selected:

- Processor architecture X86-64
- CPU 4 (2.0 GHz or better)
- Memory 16 GB
- Storage 250 GB
- At least 1 NIC
- Monitor
- Keyboard
- Mouse

4.3.1.2 BigFix Relay hardware requirements

The BigFix Relays are used to increase the efficiency of the TOE by distributing the work load of data passing between Servers and Clients. The hardware resources of the physical computer hosting a Relay strictly depends on the number of managed computers (clients) connected to the Relay. The following list shows the set of system resources for the BigFix Relay:

- Processor architecture X86-64
- CPU 2 (2.0 GHz or better)
- Memory 4 GB (or higher)
- Storage 25 GB (or higher)
- At least 1 NIC
- Monitor
- Keyboard
- Mouse

4.3.1.3 BigFix Client hardware requirements

The BigFix Client is the component installed on the managed computer. The hardware requirements for the client are not critical, the client alone can consume up to 2% of the processing power and < 20MB of memory. The following list shows the set of system resources for the BigFix client:

- Processor architecture X86-64
- CPU 1 or 2 (2.0 GHz or better)
- Memory 4 GB (or higher)
- Storage 20 GB (or higher)
- At least 1 NIC
- Monitor
- Keyboard
- Mouse

4.3.2 TOE Software

The TOE software consists of

- BigFix Server
- BigFix Console
- BigFix Relay
- BigFix Client

- BigFix Administration Tool (fixed version)

4.3.2.1 Software Entity Names

Note that the HCL BigFix 10.0.1 server is a collection of processes consisting of BESGatherDB, BESFillDB, BESRootServer . The HCL BigFix Relay is running as the BESRelay process. The HCL BigFix client is running as the BESClient process.

5 How to obtain the CC-evaluated product

All BigFix license requests will be fulfilled through the HCL Federal Sales Operations team. Some the common tasks that will now be handled for you by the HCL Federal Sales Operations team include, but not limited to the following:

- Request current serial numbers/allocations
- Request current entitlements
- Create new serial numbers
    - Assigning Bigfix entitlements to a new serial number.
- Modify existing serial numbers
    - Changing the allocation of entitlements to an existing serial number

Please call 866-750-1799 or send an email to HCLSupport@vertosoft.com for all HCL Federal License Key management support including: Requesting, returning, repairing, or re-hosting a license key.

5.1 Download the BigFix Installation Generator

The CC-evaluated HCL BigFix version 10.0.1 is available as self-extracting (.exe) file and it can be downloaded from the from the ***BigFix Enterprise Suite Download Center***

https://support.bigfix.com/bes/install/downloadbes.html

Download the following BigFix Windows server image:

Installation Generator - Windows (BigFix 10.0.1.41.exe)

The BigFix Installation Generator contains the HCL BigFix server, HCL BigFix client, HCL BigFix Console and the BigFix Administration Tool.

5.2 Download the BigFix Administration tool

The TOE requires a fixed version of the BigFix Administration tool. This version includes the fix to a problem found during the internal HCL tests. The executable is available at the following link:

http://software.bigfix.com/download/bes/100/10.0.1.45/BESAdmin.exe

Size: 16MB
SHA1: 2BC692070880C2DE359267570B9EDD315624F91C
SHA256: 2FA0E5E3F684360959D4A7E2A76071D0539C004C1DEBF2A78165F190D519EC75

5.3 Download the BigFix Clients

The TOE also includes two BigFix Clients, one Windows 10, and one RHEL7. The image of the Windows BigFix client is available on the BigFix Server installation folder, while the image of the RHEL BigFix Client can be download from the download center at the following link:

https://support.bigfix.com/bes/release/10.0/patch1/

Download the following BigFix Red Hat client image:

Agent

- *Red Hat Enterprise Linux 6, 7, 8 (x86_64)*

5.3.1 Verifying the Packages

5.3.1.1 Windows packages

HCL Customer Portal is a secure site. To guarantee authenticity of the downloaded software, the Windows files are digitally signed by "HCL America Inc." The following integrity information is available for each package:

- Size
- SHA-1 signature
- SHA-256 signature

Verify the integrity of the downloaded packages opening the file properties on Windows.

5.3.1.2 RPM Packages

To guarantee the authenticity of the RPM packages, the Red Hat RPM packages are signed with a PGP key. The files are digitally signed by "IBM Corp. and HCL Technologies Limited"

Download and import the public key for that signature by running the BES Support Fixlet named Import BigFix version 9.5 public GPG key for RedHat RPMs.

For more information, how to import the PGP key and verify the package, see chapter "Signed Client Red Hat RPM packages" of PDF documentation "*HCL BigFix V10 Installation Guide"*

5.4 License Key for TOE

The TOE requires the HCL BigFix version 10 which is enabled by a license key. Contact your HCL Federal Sales Operations team, or if you have an active maintenance contract, you can contact The HCL Federal Support Center for information about obtaining a license key.

6 Installation and Environmental Configuration

The CC Evaluated HCL BigFix component placement is as follows following computers that make up the TOE and supporting Operational Environment. The machines contain:

- **Win2016 machine** (Windows Server 2016 machine)
  - HCL BigFix Server
  - HCL BigFix Client
  - HCL BigFix Console
  - HCL BigFix Administration Tool
- None or more **Win 10 machine** (Windows 10 machine)
  - HCL BigFix Relay
  - HCL BigFix Client
- None or more **RHEL 7 machine** (RHEL 7 machine)
  - HCL BigFix Client

- None or more **Win2016 machine**
  - HCL BigFix Console
  - HCL BigFix Client

Following are the software items that make up the installation package for the TOE:

- 1 HCL BigFix Installation package (BigFix-BES-10.0.1.41.exe)
- 1 HCL BigFix Red Hat Client package (BESAgent-10.0.1.41.rhe6.x86_64.rpm)
- 1 file from which license is generated (LicenseAuthorization.BESLicenseAuthorization)

The ***HCL BigFix Installation package*** contains the Windows version of the BigFix Server, Client and Console. It is required to install those components on the Win2016 box, and to install the Window client on the Win10 box

The ***HCL BigFix Red Hat Client package*** contains the RHEL version of the BigFix Client and it is required to installed the BigFix Client on the RHEL 7 box.

The file ***LicenseAuthorization.BESLicenseAuthorization*** provides a way to create the actual BigFix license for the specific server installation. The file is processed by the BigFix installer.

6.1 Installing the TOE

This section describes the steps required to install the TOE and any required prerequisites.

6.1.1 Installing the MSSQL 20016 database

The MSSQL 2016 database is a Microsoft product, it is a supporting component required by the TOE. The database will be installed locally to the Win2016 box.

The Installation and the setup of MSSQL 2016 is a prerequisite for the TOE server component. To install the MSSQL 2016 in your production environment, refer to the MSSQL installation guide. The following list is only a reference to the common steps required to install it:

1. The MSSQL 2016 is available as ISO image from Microsoft: en_sql_server_2016_enterprise_x64_dvd_41.iso.
2. Copy the MSSQL 2016 ISO image to the Win2016 box manually. The file can be copied to any location.
3. Login as Administrator, mount the ISO image and start the MSSQL 2016 installation. Follow the Installation instructions, to install the MSSQL using the “Windows authentication “.

6.1.2 Installing the HCL BigFix Server, Console and Client

This section lists the main steps required to install the HCL BigFix Server, Console and Client in your production environment. For the detailed instruction about the installation of each BigFix component, please see the PDF guide *“HCL BigFix V10 Installation Guide “*

Before you perform the steps below, you must have downloaded the BigFix installable image, purchased a license and obtained a BigFix license authorization file. The process to do it is described in the above section 5 How to obtain the CC-evaluated product

1. Copy the authorization token file to the Win2016 machine manually. They need to be saved to any location in a place that will be referenced later in the installation steps.

2. Copy the BigFix installer file *BigFix-BES-10.0.1.41.exe* to any location on the Win2016 box.
3. Login as Administrator and start the BigFix installer (double click *BigFix-BES-10.0.1.41.exe*)
5. Follow the *"HCL BigFix V10 Installation Guide "*document to generate the license files and to perform the BigFix Server installation. Select the following BigFix security settings at installation time:
   a) In the "Request License" panel select the most secure **key size (4096)** to generate the public/private key pair later used to sign the BigFix objects (server signing key).
   b) In the "Advanced Masthead Parameters" panel, used to create the masthead file, select the option **Require use of FIPS 140-2 compliant cryptography**
   c) During the Server installation process select the option "Use Windows authentication" for the MSSQL database access.
4. Install the BigFix Server, Console and Client components on the same Win2016 machine. For more details, how to install BigFix components see the PDF guide "*HCL BigFix V10 Installation Guide***"**

Installation Notes:

I. During the installation process, you are requested to provide a password for the BigFix **Site Administrator,** the installer uses this password to create the private key **license.pvk**. It is important to store and protect the Site Administrator license.pvk and password. Store your license.crt (public key) file with your existing license.pvk (private key) file. Keep these two keys together and create a backup copy on an external drive, such as a pen drive, and store it in a secure location.

II. During the Server installation process, you are requested to provide an account for the BigFix **Master Operator.** It is important to store and protect the Master Operator credentials.

III. During the installation process a **server signing key** is created and stored as a file on the server machine. Whenever operators issue an action, it is digitally signed by the server signing key, and the client will only trust actions that are signed by that key. Since clients will trust any action signed by the server signing key, it is important to protect the server signing key file. To protect the server signing key file, the physical administrator access to the server machine must be restricted.

IV. Note that the HCL BigFix installation creates a **masthead** file (masthead.afxm) which is later required to install the BigFix clients. The file is placed, by default, in the following path:

C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client\ masthead.afxm

6.1.3 Logging in and Logging Out the Console

The BigFix console is installed on the same Server machine (Win2016 machine), and, or optionally on a separate Win2016 machine. Using the BigFix console you can monitor and fix problems on all managed computers across the network.

1. Start the console by double-clicking its desktop icon or select it from the Programs menu: Start/Programs/ BigFix/BigFix Console.
2. Log in to the BigFix console using the **Master Operator** credentials that you created at the installation time.
3. For further details on using the BigFix Console see the PDF guide "*HCL BigFix V10 Console Operator's Guide"*

6.2 Replacing the BESAdmin tool

Use the following instructions to replace the executable of the BigFix Administration tool

1. On the BigFix Server locate the file C:\Program Files (x86)\BigFix Enterprise\BES Server\besadmin.exe
2. Rename the file into “besadmin.save”
3. Locate the new besadmin.exe file that you have downloaded at chapter 5 “How to obtain the CC-evaluated product“
4. Copy the new besadmin.exe into the path C:\Program Files (x86)\BigFix Enterprise\BES Server

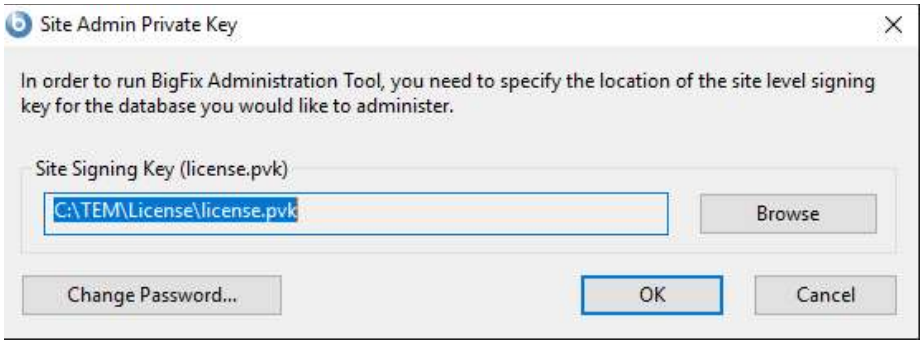
6.2.1 Testing the new BigFix Administration tool

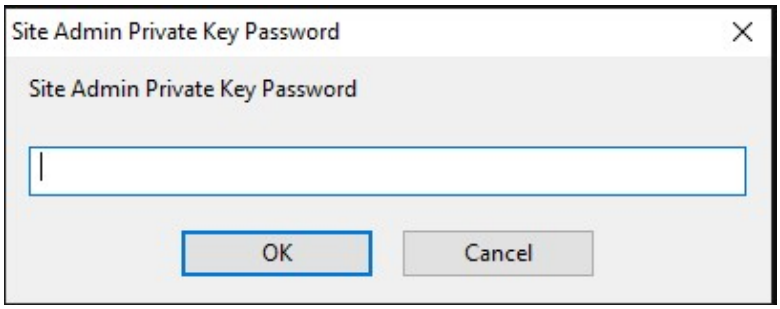
Open the BigFix Administration tool to verify it works correctly:

1. Start a windows command prompt and run the following program:

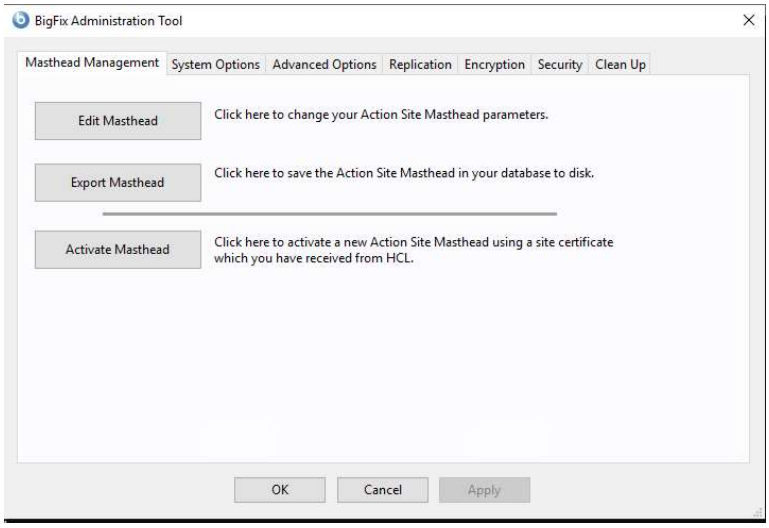
C:\Program Files (x86)\BigFix Enterprise\BES Server> besadmin.exe

2. Provide the path of the site signing key and password





3. Verify that the BigFix Administration toll is successfully started



4. Select Cancel to close it.

6.3 Installing the HCL BigFix Clients

You can now proceed to install the HCL Client on the Win10 and RHEL box

6.3.1 Installing the HCL BigFix Clients on Windows

To install the HCL BigFix Client component on the Win10 box perform the following steps:

1. The BigFix Windows Client and the masthead file is found in the BigFix Server at: C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client
2. Copy the following two files from the Win2016 box the Win10 box. The file can be copied to any location:
    a. masthead.afxm
    b. setup.exe
3. On the Win10 box, login as Administrator and start the BigFix Client installation (double click setup.exe)

6.3.2 Installing the HCL BigFix Client on RHEL7

To install the HCL BigFix Client component on the RHEL7 box perform the following steps:

1. The BigFix RHEL Client is found in the HCL BigFix Red Hat Client package (BESAgent-10.0.1.41-rhe6.x86_64.rpm). The file can be copied to any location.
2. On the RHEL7 box create the following folder:
    a. /etc/opt/BESClient
3. Copy the masthead file from the Win2016 BigFix Server to the RHEL7 box and rename it:
    a. From C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client\masthead.afxm
    b. To /etc/opt/BESClient/**actionsite.afxm**
4. CD to the directory where the BigFix Client installation has been copied and start the installation using the command

    rpm -ivh ./BESAgent-10.0.1.41-rhe6.x86_64.rpm

5. Start the BigFix Client using the command

    service besclient start

6.3.3 Installing the HCL BigFix Relay on Win10

To install the BigFix Relay component on the Win10 use the Fixlet 4555 "*Install BigFix Relay (Version 10.0.1.x)*" found in the BES Support Site.

1. Open BigFix console and select the Fixlet 4555 from the list of Fixlets and Tasks of the BES Support site.
2. Submit the Fixlet (take action) on the target client (Win10 box).

For more information, how to submit actions (take actions), see the PDF guide "*HCL BigFix V10 Console Operator's Guide".*

6.3.3.1 Installing the HCL BigFix Relay from the installation image

The Windows BigFix Relay can be alternatively installed from the image available in the download center at the following link:

https://support.bigfix.com/bes/release/10.0/patch1/

Download the following BigFix Windows relay image:

BigFix-BES-Relay-10.0.1.41.exe

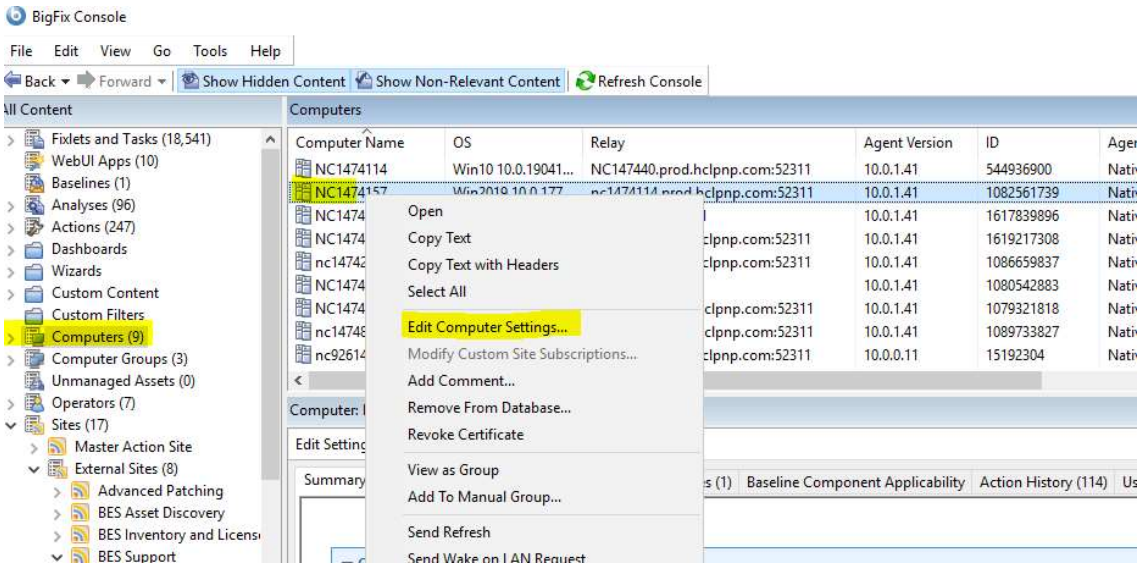
Run the executable to start the installation. During installation select the option "Install Relay as non-authenticating"

6.3.4 Assign clients to a Relay

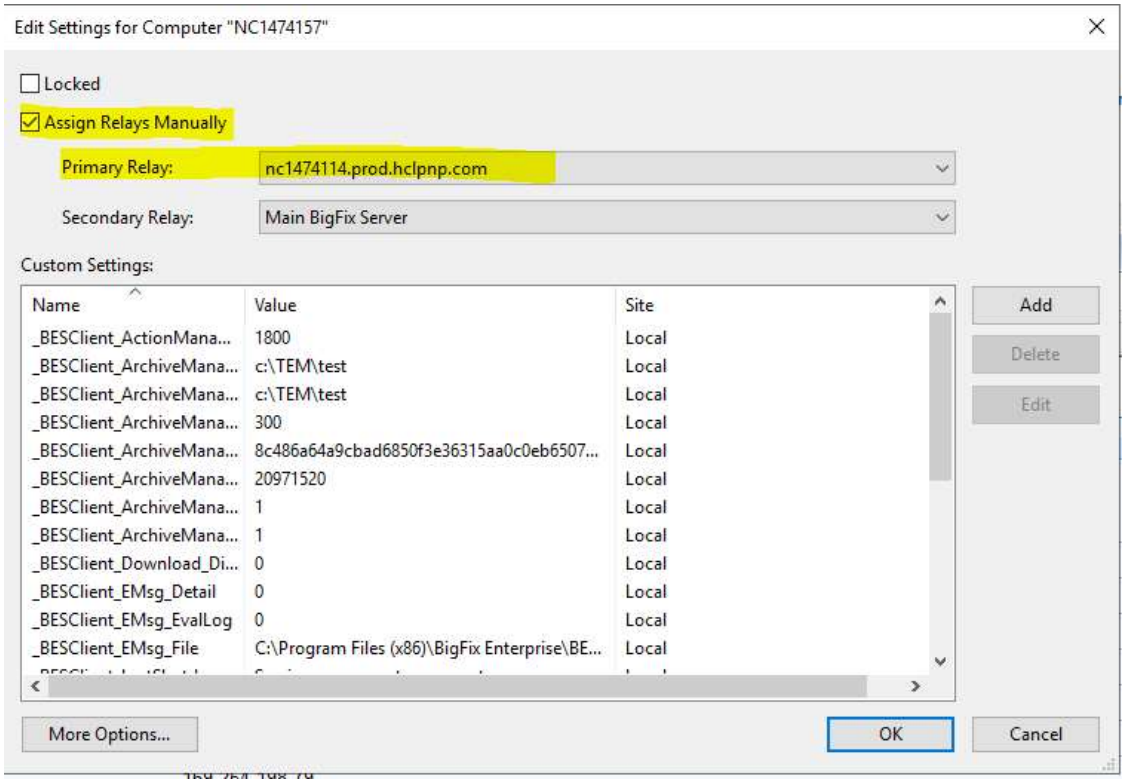
Once all clients have been installed, they can be assigned to a relay. Consider the following exceptions:

1. The client installed on the BigFix server must be connected directly to the server (no actions needed)
2. The client installed on the BigFix Relay must be connected directly to the Relay (no actions needed)

To assign a computer (client) to a relay select the computer and use the option "Edit Computer settings" available on each computer as shown in the image below:



In the “Edit Computer Settings” dialogue select option “Assign computer manually” and the wanted relay as the “Primary Relay” leave the Main Bigfix Server as Secondary relay. See the example below



6.4 Checking the software versions

The version of the HCL BigFix Server components installed on Win2016 machine can be determined by looking at the details tab of the properties of the *BESRootServer.exe* file locate at:

C:\Program Files (x86)\BigFix Enterprise\BES Server\BESRootServer.exe

The version of the HCL BigFix Relay components installed on Win10 machine can be determined by looking the at the details tab of the properties of the *BESRelay.exe* file locate at:

C:\Program Files (x86)\BigFix Enterprise\BES Relay\BESRelay.exe

The version of the HCL BigFix Client components installed on Win10 or Win2016 machine can be determined by looking the at the details tab of the properties of the *BESClient.exe* file locate at:

C:\Program Files (x86)\BigFix Enterprise\BES Client\BESClient.exe

The version of the HCL BigFix Console components installed on Win2016 machine can be determined by looking the at the details tab of the properties of the *BESConsole.exe* file locate at:

C:\Program Files (x86)\BigFix Enterprise\BES Client\BESConsole.exe

The version of the HCL BigFix Client installed on RHEL7 machine can be determined by issuing the following command:

rpm -q --queryformat '%{VERSION}\n' BESAgent

The version of the Windows OS installed on the Win2016 machine can be determined by opening the “about your PC dialogue” (Settings -> about)

The version of the Windows OS installed on the Win10 machine can be determined by opening the “about your PC dialogue” (Settings -> about)

The version of Red Hat Enterprise Linux server that is installed on RHEL7 machine can be determined by issuing from the RHEL console the command:

rpm -q --queryformat '%{RELEASE}\n' redhat-release-server

7 Enhanced Security Configuration and References

This chapter describes the steps needed to configure the TOE in an evaluated configuration

7.1 TOE Administration and operations

7.1.1 Site Administrator

The BigFix *Site Administrator operator* is responsible for installing and maintaining the HCL BigFix components, as well as advanced deployment-wide configurations. This role is used primarily during initial installation and configuration of the TOE. The security functionality available to this user are:

- Setting advanced security policies
- Setting advanced configuration options
- Configuring lockout settings

The BigFix Site Administrator uses the BigFix administrator console to perform the security management functions, by providing a password and private key.

7.1.2 Master Operator

The BigFix Master Operator (MO) will be used for all run time operations. It corresponds to the “Authorized Administrator” described in the ST document.

The BigFix Master Operator uses the BigFix console and REST API, to perform the security management functions; identification and authentication is performed with his/her user name and password.

7.1.3 Non-Master Operator

The BigFix Non-Master Operators (NMO) manage the day-to-day BigFix operations. They correspond to the “Operators” described in the ST document.

A NMO uses the BigFix console and REST API, to perform the security management functions; identification and authentication is performed with his/her user name and password.

7.2 Guidance for networking

Nothing manual needs to be done in the case of an unintentional network disconnect/reconnect. The BigFix components will automatically recover most of network interruption and database connection problems. The connection to internet must be secured by a firewall. The Server uses the HTTPS protocol and port 443 to connect with the license server and with the BigFix sites.

7.3 Hardening the HCL BigFix

This section describes the steps required set up the HCL BigFix evaluated configuration. Those steps must be performed right after the BigFix server installation. This section covers the following security setting tasks:

- Enabling authentication on Relay
- Enabling Enhanced security
- Configuring HCL BigFix session termination
- Setting the TLS cipher-suite
- Customizing HTTPS for Gathering
- Enabling encryption on Clients
- Creating roles and User accounts
- Disabling WebUI port
- Disabling FTP and SSH

7.3.1 Enabling authentication on Server and relay

In order to enable the TLS/HTTPS communication across all HCL BigFix components, some configuration settings are required to enable the authentication on Server and Relay. Following settings enable authentication, as well as the use of HTTPS.

7.3.1.1 Enabling authentication on Relay

To set the authentication on the Relay use the fixlet 1297 "BES Client Setting: Enable Relay Authentication" found in BES Support Site.

1. Login to the BigFix console using the Master Operator account
2. On the BigFix console select: External Sites > BES Support Site > Fixlet 1297
3. Submit the Fixlet (take action) on the target client (Win10 box).

7.3.2 Enabling Enhanced security

Enable the Enhanced security and TLS 1.2 from the BigFix Administration tool.

1. Open the BigFix Administration Tool (Start > All Programs > BigFix > BigFix Administration Tool).
2. Login using the *Site Administrator* credentials (key and password)
3. Open the Security tab dialog and Click the Enable Enhanced Security button to adopt the SHA-256 cryptographic digest algorithm for all digital signatures as well as for content verification and to use the TLS 1.2 protocol for communications among the BigFix components.

Please refer to the *HCL BigFix V10 Configuration Guide* for further details on how to enable Enhanced security thru the BigFix Administration Tool:

7.3.3 Configuring HCL BigFix session termination

The Console will close itself after an administrator-specified time interval. This time interval is set by the BESAdmin advanced option timeoutLogoutMinutes from the BigFix Administration tool.

1. Open the BigFix Administration Tool (Start > All Programs > BigFix > BigFix Administration Tool).
2. Login using the *Site Administrator* credentials (key and password)

3. Open the Advanced Options tab dialog and Click Add to add the option "*timeoutLogoutMinutes*"
4. Set the desired value and press OK to save it.

This option is analogous to the "timeoutLockMinutes" advanced options used to set the Console lock time.

Please refer to the following PDF guide "*HCL BigFix V10 Configuration Guide"* for further details on how to set the BigFix console session timeout from the BigFix Administration Tool.

7.3.4 Setting the TLS cipher-suite

All network communications between the BigFix components and the internet are encrypted by using the TLS protocol standard. Administrator Operators can control which TLS ciphers should be used for encryption. Set the TLS cipher-suite use the from the BigFix Administration command line (besadmin CLI). To run this task, you need the Site Administrator private key (license.pvk) and password created during the installation process. To run the besadmin CLI open a Windows command prompt and cd to the following path:

C:\Program Files (x86)\BigFix Enterprise\BES Server\BESAdmin.exe

7.3.4.1 setTLSCipherList

Use the following command to set the ephemeral Diffie-Hellman (DHE) and ephemeral elliptic curve Diffie-Hellman (ECDHE) for key exchange:

1. BESAdmin.exe /securitysettings /setTLSCipherList="TLSv1.2:!ADH:!AECDH:!kDH:!kECDH:!PSK:!SRP:!NULL:!SHA:!kRSA"
2. When prompted provide the Site Admin private key (license.pvk) location, and password.

7.3.4.2 TestTLSCipherList

To test the above chiper-list use the following command

1. BESAdmin.exe /securitysettings /testTLSCipherList="TLSv1.2:!ADH:!AECDH:!kDH:!kECDH:!PSK:!SRP:!NULL:!SHA:!kRSA"
2. When prompted provide the Site Admin private key (license.pvk) location, and password.

7.3.5 Customizing HTTPS for Gathering

The BigFix Server (Win2016 machine) must be configured to gather license updates and external sites content by using the HTTPS protocol only.

Set the following client setting on BigFix server (Win2016 box).

1. Login to the BigFix console using the *Master Operator* account
2. On the BigFix console select: Computers > Server computer > Edit Settings dialogue
3. Set the client property *_BESGather_Use_Https* to 1.

Please refer to the *HCL BigFix V10 Configuration Guide* on how to configure client settings thru the BigFix Console

7.3.6 Enabling encryption on Clients

All data gathered from Clients must be encrypted before they are delivered over the network. Use the following procedure to enable the encryption on Clients.

7.3.6.1 Generate the encryption key

To enable the Client encryption, you must generate an encryption key and provide it to the clients. Use the BigFix Administration Tool to create and deploy the key:

1. Open the BigFix Administration Tool (Start > All Programs > BigFix > BigFix Administration Tool).
2. Login using the *Site Administrator* credentials (key and password)
3. Select the Encryption tab and Click the Generate key button to generate a new Key. Select the most secure key size of 4096 bits (default) to generate the key.

The report encryption is now enabled and the server can decrypt the encrypted reports gathered from the client

7.3.6.2 Enable encryption on clients

Client encryption feature can be enabled or disabled, by default the feature is disabled. To enable the encryption on the Clients, use the Fixlet 978 "*Enable Encryption for Clients*" found in BES Support Site:

1. Login to the BigFix console using the Master Operator account
2. On the BigFix console select: External Sites > BES Support Site > Fixlet 978
3. Submit the fixlet (take action) on all target clients (Win2016, Win10, RHEL7)

Please refer to the *HCL BigFix V10 Configuration Guide* for further details on how to enable the encryption on clients.

7.3.7 Disabling WebUI port

The BigFix Server (Win2016 machine) must be configured to disable listening on the WebUI port which is not installed on the TOE:

Set the following client setting on BigFix server (Win2016 box).

1. Login to the BigFix console using the *Master Operator* account
2. On the BigFix console select: Computers > Server computer > Edit Settings dialogue
3. Set the client property *_APIServer_HTTPServer_IsEnabled* to 0.

Please refer to the following PDF document "*HCL BigFix V10 Configuration Guide"* on how to configure client settings thru the BigFix Console.

7.3.8 Disabling FTP and SSH

The SSH and the FTP servers are optional components on Windows server 2016, make sure those components have not been installed, or if present, verify they have been disabled.

7.3.9 Windows 2016 security settings

Make sure that the latest version of security OS and MSSQL 2016 updates are installed on the machine.

The HCL BigFix doesn't require or prerequisite any specific OS security settings in addition to the OS Administrator access to the server machine which must be restricted to trusted administrators only.

Secure the server computers and the SQL database using company or industry-wide standards.

7.3.10 Firewall configuration

After installation of Windows (Win 2016 Server and Win 10), the firewall will be on and it have to be configured to have the BigFix ports open on the external network interfaces. Open the following ports on the BigFix Server and Relay

- TCP Port 52311
- UDP Port 52311 – outbound only

The firewall on the RHEL7 Client machine must be configured to accept the following:

- TCP Port 52311 – outbound only
- UDP Port 52311 – inbound only

Changing the firewall settings falls outside the scope of the Common Criteria evaluated configuration.

7.4 Creating roles and User accounts

The TOE support two classes of users: *Master Operators* (MO) and *Non- Master Operators* (NMO). Each of these user roles has different responsibilities. The Master Operator can create other Operators and Non-Master Operators, and can perform any BigFix operation.

The role of Master Operator should be restricted to a small set of authorized personnel only. To manage the day-to-day BigFix operations, the role of Non-Master Operator should be used instead. To enforce security, NMO must be assigned to a role in order to be able to login to the BigFix console.

The following section describes the main steps required to create Non-Master Operators. Please refer to the following PDF document "*HCL BigFix V10 Configuration Guide"* for further details on how to create and manage BigFix Operators.

7.4.1 Create roles

To create roles, use the BigFix console as follow:

1. Login to the BigFix console using the Master Operator account
2. On the BigFix console select: Tools > Create Role, or right click in the Roles work area and select Create Role.
3. The Create Role dialog appears and prompts you for a name
4. Use Permission dialogue to grant the wanted permissions.

Please refer to the following PDF document "*HCL BigFix V10 Configuration Guide"* for further details on how to manage roles.

7.4.2 Create Non-Master Operators

To create a NMO and to assign roles, use the BigFix console as follow:

1. Login to the BigFix console using the Master Operator account
2. On the BigFix console Click Tools > Create Operator, or right click in the Operators work area and select Create Local Operators.
3. The Add User dialog appears and prompts you for an Operator name and password.
4. Select the Assigned Roles tab > Assign Role button to select a role for the new operator.

7.5 Processes that receive data from the network

The firewall will only allow the following processes to process data received over an external facing network interface:

BESRootServer. This is main process providing the central server functionality for the HCL BigFix Server. This process accepts inbound connections on port 52311.

BESrelay. This is main process providing the central server functionality for the HCL BigFix Relay. This process accepts inbound connections on port 52311.

BESclient. This is main process providing the functionality for the HCL BigFix Client. This process accepts inbound UDP connections on port 52311.

7.6 Support

For support with your HCL BigFix Common Criteria deployment, please contact your HCL Federal Sales representative to arrange for a technician to contact you. For more general information about this product, see the HCL Federal Support Center web page:

https://hclpnpsupport.hcltech.com/csm?id=federal

8 Errors Handling and Troubleshooting

In case of error, the TOE shows error messages directly on the interface used when the error occurs. All errors are self -explanatory, and in some cases the TOE can recover from error situations.

The following sections list common group of errors and the related corrective actions

8.1 BigFix Administration Tool errors

The BigFix Administration tool shows up an error dialog whenever an error is encountered. The following table lists common groups of errors and the related corrective actions:

Errors	Corrective action	Who
Database Connection	Verify that the database is running. Verify the network connection between the server and the data base. If the problem persists, contact the BigFix support	BigFix Administrator
Invalid Action Site Masthead	Select the correct Action Site Masthead in the error dialogue	BigFix Administrator
Invalid Signing Key Location	Select a valid signing key location.	
Invalid Certificate	Select the correct private key file. If the problem persists, contact the BigFix support	BigFix Administrator
Incorrect Password	Use the correct password or the correct private key file	BigFix Administrator
Database Not Initialized	Initialize the data base. If the problem persists, contact the BigFix support	BigFix Administrator
Invalid Database Version	Upgrade the product (and DB version). If the problem persists, contact the BigFix support	BigFix Administrator
Invalid Site certificate	Use a valid site certificate. If the problem persists, contact the BigFix support	BigFix Administrator
Invalid edit masthead option	Use the correct option (error suggests the correct option or the invalid set)	BigFix Administrator
Invalid command	Use the correct command option (error shows the list of options or the invalid set)	BigFix Administrator

Invalid advanced options	Use the correct option (error suggests the corrects options or the invalid set)	BigFix Administrator
Report encryption errors	Select the correct option (error suggests the corrects options or the invalid set)	BigFix Administrator
Security settings errors	Select the correct option (error suggests the corrects options or the invalid set)	BigFix Administrator

8.2 Console Errors

The BigFix console shows up an error dialog whenever an error is encountered. The following table lists common groups of errors and the related corrective actions:

Errors	Corrective action	Who
Database connection errors	Verify that the database is running. Verify network connection between the server and the data base. If the problem persists, contact the BigFix support	OS Administrator
Server connection errors	Verify that the BigFix Server is running. Verify network connection between the server and the console. If the problem persists, contact the BigFix support	OS Administrator
Incorrect user or password	Use the correct password or the correct Operator name	MO or NMO
Unable to login	Ask the Master Operator to grant the login permission	NMO
Password is expired	Ask the Master Operator to reset the Operator password	NMO
Import objects error	The imported object has an invalid format. Use a valid BES object	MO or NMO
Objects with the same name	An object with the same name already exists. Use a different name	MO or NMO
Invalid signatures	Use the Administration tool to resign the invalid object	BigFix Administrator
Invalid SHA (prefetch download)	The downloaded file is corrupted or it has an invalid SHA. Correct the SHA or verify the file.	MO or NMO
SSL hand shaking errors	The server from which the file is downloaded, doesn't support the wanted TLS protocol. The download operation can't be completed on that server.	MO or NMO
Action syntax errors	Use the correct action syntax (error shows the invalid line)	MO or NMO
Relevance syntax errors	Use the correct relevance expression	MO or NMO

8.3 REST API and IEM CLI Errors

The REST API returns an error results whenever an error is encountered. The following table lists common groups of errors and the related corrective actions:

Error	Corrective action	who
Database connection errors	Verify that the database is running. Verify network connection between the server and the data base. If the problem persists, contact the BigFix support	DB Administrator OS or Network Administrator
Server connection errors	Verify that the BigFix Server is running. Verify network connection between the server and the REST client. If the problem persists, contact the BigFix support	OS or Network Administrator
Incorrect user or password	Use the correct password or the correct Operator name	NO or NMO
Unable to login	Ask the Master Operator to grant the login permission	NMO
Password is expired	Ask the Master Operator to reset the Operator password	NMO
Operator Permission errors	Ask the Master Operator to grant the missing permission	NMO

Import objects error	The imported object has an invalid format. Use a valid BES object	NO or NMO
Objects with the same name	An object with the same name already exists. Use a different name	NO or NMO
REST API syntax errors (xml)	Use the correct REST syntax (error shows the invalid line)	NO or NMO
Invalid REST API options	Use the correct option (error suggests the corrects options or the invalid set)	NO or NMO
Login timeout	Session is expired. Log into the server with Operator name and password	NO or NMO

8.4 Troubleshooting common connectivity problems

Connectivity problems can cause malfunctions in the TOE. The following table lists the most common connectivity problems and the related corrective actions:

Problem	Corrective action	who
Computer doesn't appear in the console	Verify the network connection between the computer and the server/relay. Verify the client has got the correct masthead	OS or Network Administrator
Computer doesn't perform actions timely	Verify the network connection between the computer and the sever/relay. Verify the firewall on the computer doesn't block incoming UDP messages.	OS or Network Administrator
Computer doesn't connect to the assigned Relay	Verify the network connection between the computer and the relay. Verify the firewall on the relay doesn't block incoming HTTPS messages	OS or Network Administrator
Computer doesn't register to an authenticating relay	Verify the network connection between the computer and the relay. Verify the firewall on the relay doesn't block incoming HTTPS messages. New computers need a certificate to connect to an authenticating relay. See "Manual key exchange procedure"	OS or Network Administrator
Fixlets don't become relevant on all computers	Verify the computer is powered on, or not frozen. Verify the network connection between the computer and the sever/relay. Verify the firewall on the computer doesn't block incoming UDP messages.	OS or Network Administrator
Computer becomes unavailable (greyed) in the console	Verify the computer is powered on, or not frozen. Verify the network connection between the computer and the sever/relay.	OS or Network Administrator

9 Notices

This information was developed for products and services offered in the U.S.A. HCL Technologies Limited 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.

10 Trademarks

HCL the HCL logo is trademarks or registered trademarks of HCL Technologies Limited, registered in many jurisdictions worldwide. Other product and service names might be trademarks of HCL or other companies.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.