Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 3/21

(Certification No.)

Prodotto: **HCL BigFix version 10.0.1.41**
(Product)

Sviluppato da: **HCL Technologies Limited**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 6 maggio 2021

Common Criteria

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Certification Report

HCL BigFix version 10.0.1.41

OCSI/CERT/ATS/07/2020/RC

Version 1.0

6 May 2021

Courtesy translation

Disclaimer: this translation into English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	06/05/2021

2 Table of contents

3 Acronyms

API	Application Programming Interface
BES	BigFix Enterprise Suite
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CPU	Central Processing Unit
DNS	Domain Name System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GB	GigaByte
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
HW	Hardware
IEM	IBM Endpoint Manager
ISO/OSI	International Organization for Standardization / Open Systems Interconnection
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
OS	Operating System
PC	Personal Computer
PGP	Pretty Good Privacy

PP	Protection Profile
RAM	Random Access Memory
REST	Representational State Transfer
RHEL	Red Hat Enterprise Linux
RPM	Red Hat Package Manager
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
SSH	Secure Shell
ST	Security Target
SW	Software
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
XML	eXtensible Markup Language

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[BFASG] BigFix Version 10.0.1 Action Script Guide

[BFCCCG] HCL BigFix Version 10.0.1 Common Criteria Configuration Guide, Version 1.9, 26 October 2021

[BFCG] BigFix Configuration Guide, Version 10.0

[BFCO] BigFix Console Operator’s Guide, Version 10.0

[BFIG] BigFix Installation Guide, Version 10.0

[BFRA] BigFix Version 10.0.1 REST API

[BFRG] BigFix Version 10.0.1 Relevance Guide

[ETR] Final Evaluation Technical Report “HCL BigFix version 10.0.1.41”, OCSI-CERT-ATS-07-2020_ETR_210322_v1.1, Version 1.1, atsec information security GmbH, 22 March 2021

[ST] HCL BigFix version 10.0.1 Common Criteria Security Target, Version 1.4, HCL Technologies Limited, 26 February 2021

5 Recognition of the certificate

5.1 CC Certificates recognition in Europe (SOGIS-MRA)

The European mutual recognition arrangement (SOGIS-MRA, version 3, [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) for the assurance levels up to and including EAL4 for all IT products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA up to EAL2.

5.2 International CC Certificates recognition (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of certification

The Target of Evaluation (TOE) is the software product “HCL BigFix version 10.0.1.41”, also referred to in the following as “HCL BigFix”, developed by HCL Technologies Limited.

The TOE is a centralized endpoint management system that allows authorized operators to monitor the system configurations of distributed endpoints (client computers) and enables operators to take any necessary corrective actions.

The evaluation has been conducted according to the requirements established by the Italian Scheme for the evaluation and security certification of systems and products in the information technology sector and described in the Provisional Guidelines [LGP1, LGP2, LGP3] and in the Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the TOE complies with the requirements specified in the Security Target [ST]; the potential consumers and/or users of the product should review also the Security Target, in addition to the present Certification Report. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “HCL BigFix version 10.0.1.41” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	HCL BigFix version 10.0.1.41
Security Target	HCL BigFix version 10.0.1.41 Common Criteria Security Target, Version 1.4 [ST]
Evaluation Assurance Level	EAL2
Developer	HCL Technologies Limited
Sponsor	HCL Technologies Limited
LVS	atsec information security Srl
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	4 August 2020
Evaluation ending date	22 March 2021

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE; for a detailed description, please refer to the Security Target [ST].

The TOE is a client-server application that allows monitoring and management of targeted IT systems from a central location. The TOE utilizes a patented Fixlet® technology to identify vulnerable or misconfigured computers in the enterprise and allows authorized users to remediate identified issues across the network.

Fixlet messages are available to an enterprise by subscribing to any of several Fixlet Sites that are maintained by the BigFix Fixlet Server which is not part of the TOE and is outside the evaluated configuration. Each Fixlet Site contains pre-tested, pre-packaged Fixlet messages that provide out-of-the-box management solutions. They constitute data that the TOE collects, distributes and otherwise utilizes via the Internet from the BigFix Fixlet Server to detect and remediate vulnerabilities.

Fixlets enable authorized users to perform the following functions within the enterprise:

- analyze the vulnerability status (i.e., patched or insecure configurations);
- distribute patches to vulnerable computers to maintain endpoint security;
- establish and enforce configuration security policies across the network;
- distribute and update software;
- manage the network from a central Console;
- view, modify and audit properties and configurations of the networked client computers.

The TOE contains built-in public/private key cryptographic capabilities to ensure the authenticity of the Fixlet messages and remedial Actions. Each Fixlet and Action received by a BigFix Client is authenticated by verifying a digital signature affixed by the applicable administrator to ensure that it was generated by an administrator authorized to perform corresponding operations. These authorized operations instruct BigFix Clients to view, modify and audit properties and configurations of the networked client computers. The results from those operations — or simply the gathered data — is encrypted and delivered back to the BES server.

7.3.1 TOE architecture

The TOE consists of four software components:

- BigFix Server
- BigFix Console
- BigFix Client (i.e., Agent)
- BigFix Relay

During installation of the TOE, the authorized Site Administrator creates a Masthead that ties the TOE together. Among other things, this Masthead includes a key (signed by the Site Administrator) to authenticate any instructions from the BigFix Server. Following is an overview of each of the components, hereinafter referred to as Server, Console, Client and Relay.

The TOE provides an authorized user the ability to assess the status of client machines Operating System (OS), applications, anti-virus signatures, etc. (using Fixlets) and provides the ability to update these machines as necessary (using Actions). The TOE relies on the ability of client machines to periodically check with the server (or designated relay) the most current Fixlets and/or Actions that can be obtained.

Figure 1 depicts an overview of the basic TOE architecture. There is at least one server that gathers Fixlets from the BigFix Fixlet Server on Internet where they can be viewed by the console operator and distributed to the relays. Each client inspects its local computer environment and reports any relevant Fixlets back to the relay, which compresses the data and passes it back up to the servers.

The solid arrows in Figure 1 reflect the required TOE components as well as the optional Fixlet service in the IT Environment provided by BigFix via the Internet. Note that while Figure 1 depicts the TOE as computers of various types, the TOE consists only of software running in the context of the computers and their installed operating systems.

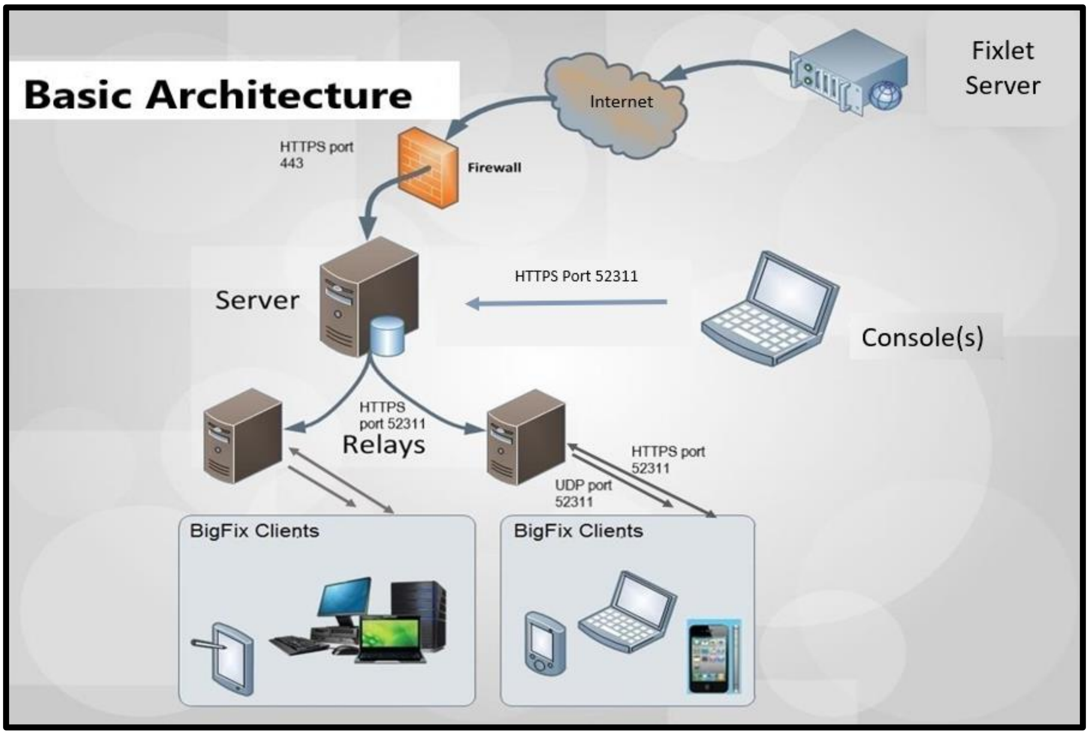

Figure 1 - TOE architecture

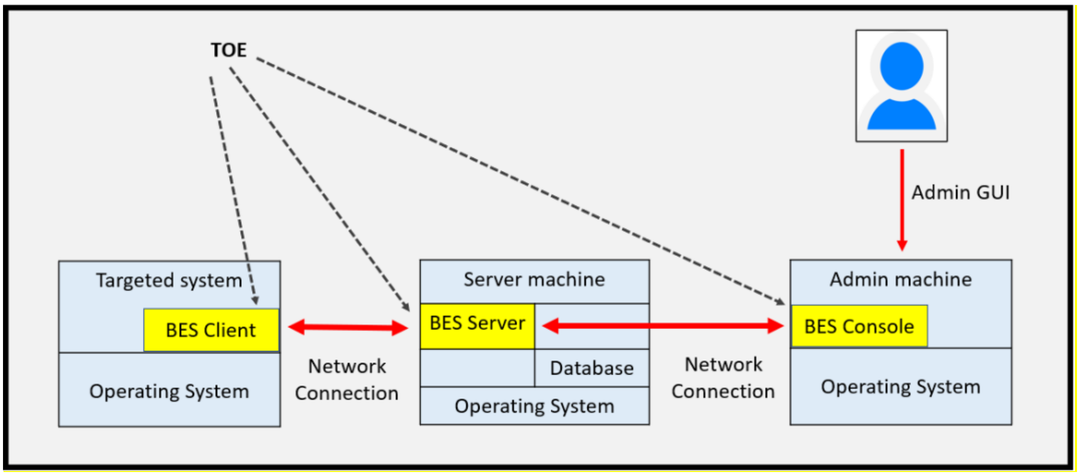

Figure 2 - TOE logical view

Figure 2 is a logical view of the primary TOE components in the context of their host computers. Note that a Relay is essentially a combination of Client and Server components acting to store and forward communications in both directions. Relays are optional components that do not affect the security functions of the TOE, but provide for network efficiency in distributing Fixlets and actions.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 1.4.3 of the Security Target [ST]. The most significant aspects are summarized below:

- **Cryptographic Support**: the TOE performs cryptographic operations by providing Rivest-Shamir-Adleman (RSA) public/private key pairs for the purpose of digitally signing Actions within the infrastructure. These signatures enable the TOE to authenticate and ensure the integrity of remedial actions as they are collected, distributed and deployed by various components of the TOE across the network. To protect the data collected from the clients, the TOE generates RSA public/private key pairs used for encryption that are distributed from the Server to Clients and Relays.

- **User Data Protection**: the TOE provides an Action Information Flow Control SFP that controls the application of Actions via Clients. Actions are provided by Operators. The TOE Server facilitates the distribution of applicable Actions to Clients and those Clients will only accept and apply Actions when it can be validated that they have come from an authorized source (e.g., an Operator assigned to manage that Client).

- **Identification and Authentication (I&A)**: the TOE requires users (i.e., administrators) to be identified and authenticated before completing any security management related actions. Once an administrator is authenticated, the TOE enforces role-based rules and only Master Operator can change the rules and attributes on behalf of users.

- **Security Management**: the TOE provides security management functions that can only be accessed by authorized administrators. The TOE restricts the ability to determine the behavior of, disable, enable, modify the behavior of the functions (i.e., security policy rules and privileges) by role and the TOE also provides the functions necessary for effective management of the TOE security functions.

- **Protection of the TOE Security Functions (TSF)**: the TOE enforces the use of TLS v1.2/HTTPS to protect the communications channel among all TOE components (Server, Console, Relay and Clients). The TOE protects the security of data and operation results data gathered on networked client computers by encrypting this data before it is transmitted over the network.

- **Trusted path/channels**: the TOE enforces the use of TLS v1.2/HTTPS to protect the communications channel between the TOE and Fixlet Servers, which are considered external IT entities. The TOE enforces the use of TLS v1.2 for the REST

API interface provided by the TOE to allow external IT entities to perform security management functions.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure use of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST], whose review is recommended to potential consumers. Initially, the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security Srl.

The evaluation was completed on 22 March 2021 with the issuance by the LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 26 March 2021. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] released by the LVS and documents required for the certification, and considering the evaluation activities carried out, on the basis of the evidence examined by the Certification group, OCSI concluded that the TOE “HCL BigFix version 10.0.1.41” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2, with respect to the security functions described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarises the final verdicts for each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security Problem Definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Tests	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass

Assurance classes and components		**Verdict**
Functional testing	ATE_FUN.1	Pass
Independent testing – sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for the assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product “HCL BigFix version 10.0.1.41” are suggested to properly understand the specific purpose of this certification reading this Report with reference to the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the assumptions and the Organizational security policies described, respectively, in sect. 3.2 and 3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure use of the product includes a number of recommendations relating to delivery, initialization and secure usage of the product, according to the guidance documentation provided together with the TOE ([BFASG], [BFCCCG], [BFCG], [BFCM], [BFCO], [BFIG], [BFRA], [BFRG]).

9 Annex A – Guidelines for the secure use of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

The TOE delivery procedure consists in downloading the following files from the BigFix Enterprise Suite Download Center and verifying them:

- BigFix Installation Generator
- Hot fix version 10.0.1.45 for BigFix Administration tool
- BigFix Clients
- BigFix Guidance

The CC-evaluated HCL BigFix version 10.0.1.41 is available as self-extracting (.exe) file. Namely, the BigFix Windows server image, called Installation Generator - Windows (BigFix 10.0.1.41.exe), contains the HCL BigFix server, HCL BigFix Client, HCL BigFix Console and the BigFix Administration Tool.

The BigFix Administration tool hot fix executable is currently available at: https://software.bigfix.com/download/bes/100/10.0.1.45/BESAdmin.exe.

The TOE also includes two BigFix Clients available for Windows 10 and for RHEL 6-8 platforms. Namely, 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.

Before using the TOE the downloaded files can be verified as follows:

- *Windows packages*: to guarantee authenticity of the downloaded software, the Windows files are digitally signed by “HCL America Inc.”. Integrity information is available for each package in terms of size, SHA-1 signature, SHA-256 signature by simply opening the file properties on Windows.
- *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”. It is possible to 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 on how to import the PGP key and verify the package refer to chapter “Signed Client Red Hat RPM packages” of PDF documentation “BigFix Installation Guide” [BFIG].
- *Guidance*: To guarantee authenticity of the downloaded files, integrity information is available for each guidance in terms of size, SHA-1 signature, SHA-256 signature.

The TOE is enabled by a license key. Information on license keys can be obtained from the HCL Federal Sales Operations team or from the HCL Federal Support Center for information.

9.2 Installation, initialization and secure usage of the TOE

For secure installation and configuration of the TOE refer to the guidance documents [BFIG], [BFCG] and [BFCCCG], where BigFix platform set-up is provided along with some sample deployment scenarios, configuration scenarios and types of installation on Windows and Linux machines. Platform management tasks are also included. In [BFCCCG] details on the application of the hot fix is provided.

For secure usage of the TOE refer to the guidance documents [BFASG], [BFCO], [BFRA] and [BFRG]. They contain information on usage of the Console, REST API, Scripts and Relevance language.

10 Annex B – Evaluated configuration

The evaluated configuration consists of the software and guidance documentation specified in section 1.4.2 of the Security Target [ST]. Namely, the TOE SW components are the following:

- BigFix Server 10.0.1.41
- BigFix Client 10.0.1.41
- BigFix Relay 10.0.1.41
- BigFix Console 10.0.1.41
- BigFix Administration Tool 10.0.1.45

The guidance documentation consists of the following documents: [BFASG], [BFCCCG], [BFCG], [BFCM], [BFCO], [BFIG], [BFRA], [BFRG].

The deployment scenarios for HW and SW elements include a minimal configuration where at least one component for HCL BigFix Server, HCL BigFix Client, HCL BigFix Console and HCL BigFix Administration Tool is available. Table 2 summarizes the TOE minimal configuration and the additional optional components.

SW Component	Number of deployed components	Operating system of the hosting machine
HCL BigFix Server	One	Windows Server 2016
HCL BigFix Client	One	Windows Server 2016
HCL BigFix Console	One	Windows Server 2016
HCL BigFix Administration Tool	One	Windows Server 2016
HCLBigFixRelay	none or more	Windows 10
HCL BigFix Client	none or more	Windows 10
HCL BigFix Client	none or more	RHEL 7
HCL BigFix Console	none or more	Windows Server 2016
HCL BigFix Client	none or more	Windows Server 2016

Table 2 - TOE deployment scenarios

Each TOE component requires additional hardware and software that comprise the operational environment. The software and hardware required by each TOE component is listed in the following:

- BigFix Server: Windows Server 2016, MSSQL Server 2016, Processor X86-64 (4CPU), 16 GB RAM, 250 GB Disk

- BigFix Console: Windows Server 2016, Processor X86-64 (2CPU), 4 GB RAM, 20 GB Disk
- BigFix Relay: Windows 10, Processor X86-64 (2CPU), 4 GB RAM, 25 GB Disk
- BigFix Client: Supported operating systems (Windows Server 2016, Windows 10, Red Hat Enterprise Linux 7), Processor X86-64 (2CPU), 4 GB RAM, 20 GB Disk

The MSSQL 2016 database is also required for the TOE and is part of the operational environment. The Installation and the setup of MSSQL 2016 is a prerequisite for the TOE server component.

The TOE also requires the Domain Name System (DNS) service in the operational environment.

The following restrictions apply to the evaluated configuration:

- The Server component must be configured as an authenticating server.
- The Server component must be configured to use HTTPS to gather from external sites.
- The Server component must be configured to require TLS v1.2 for all HTTPS communications.
- The Server component must be configured to use “Enhanced security”.
- The Server component must be configured to use “FIPS mode”.
- The Relay components must be configured as an authenticating relay.
- The Client components must be configured to send “encrypted reports” only.
- Each user account can have only one role assigned to it.
- FTP must be disabled.
- SSH must be disabled.
- The Web Reports interface must be disabled or not installed.
- The WebUI interface must be not installed.

11 Annex C – Test Activities

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

The following software items that make up the installation package for the TOE were used:

- 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 Windows 2016 box, and to install the Windows client on the Windows 10 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.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The test results provided by the Developer were generated for the BigFix 10.0.1.41 on a compliant hardware platform as stated in the Security Target [ST]. The Developer has performed his tests using the version of the TOE, in the evaluated configuration as defined in the CC guide [BFCCCG].

The test plan provided by the Developer lists test cases by SFR groups. The provided mapping lists the SFRs and the relevant TSFI test cases. The test plan is focused on the security functions of the TOE. The test cases are mapped to the corresponding functional specification and the subsystems. Some tests are automated. Each test case may contain several tests of the same function, stressing different parts (for example, base functionality, behavior with illegal parameters and reaction to missing privileges). Each test within a test case reports is considered PASS if the conditions indicated in the test case document are met, otherwise FAIL is reported.

11.2.2 Test coverage

The functional specification has identified the following TSFIs:

- Besadmin CLI
- BigFix Client
- Console
- REST API
- Client Register
- BigFix Site Administrator
- BigFix Relay
- OpenSSL (Server, Relay, Client)

The mapping provided by the Developer shows that the tests cover all individual TSFI identified for the TOE.

11.2.3 Test results

As described in the testing approach, the test results are written into documents, or in the form of screenshots. All test results from the tested environment show that the expected test results are identical to the actual test results, so all tests can be considered passed.

The Evaluators verified that the Developer testing was performed on HW/SW compliant to the Security target [ST]. The Evaluators were able to follow and fully understand the Developer testing approach by using the provided test documentation. The Evaluators analyzed the Developer testing coverage and the depth of the testing by reviewing all test cases. The Evaluators found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification as well as the subsystem/internal interfaces. The Evaluators reviewed the test results provided by the Developer and found them to be consistent with the expected test results according to the test plan.

11.3 Functional and independent tests performed by the Evaluators

The Evaluators configured the test system according to the documentation provided by the Developer and the test plan. The CC guide [BFCCCG] was preliminary assessed and verified being consistent with the Security Target [ST]. The Evaluators configured the TOE and the TOE operational environment in person, to ensure that the Evaluators' test configuration was consistent with the ST.

The Evaluators' testing effort consists of two parts. The first one is the execution of a subset of the Developer tests and the second is the execution of the tests created by the Evaluators. The chosen subset of the Developer tests included Developer automated tests. However, the Evaluators repeated automated tests of the Developer in manual mode, due to the inability of the Evaluators to gain access to the HCL network (because of internal Developer policies) where the automatic test system is contained. All the test results conformed to the expected test results from the Developer test plan.

During the Evaluators' review of the test cases provided by the Developer, the Evaluators gained confidence in the Developer testing effort both in terms of depth and of coverage in the Developer supplied test cases. The analysis has shown a very wide coverage of the TSF, therefore the Evaluators devised only a small number of test cases, compared to the amount of functionality claimed in this evaluation. The Evaluators chose the following tests in particular:

- Some additional basic user privilege operation check for REST API and Console
- Additional test on BESAdmin.exe (hotfix)
- Additional Authentication test on CLI interfaces
- An additional test on REST API Authentication using dirty strings
- Additional test on REST API and IEM CLI XML parsing of malformed XML input

All Evaluator-written tests passed successfully.

11.4 Vulnerability assessment and penetration tests

The configuration adopted for the penetration testing was the same used for the independent tests, which was consistent with the configuration under evaluation as specified in the Security Target [ST]. The operational environment of the TOE for penetration testing was verified as well.

The Evaluators started investigating into the ST and the guidance documentation to identify potential attack vectors. Based on the analysis, the Evaluators considered that, regarding physical security of the TOE, either attackers or legitimate users may potentially try to launch attacks through the Administration Tool interface. The BigFix Console interface of the TOE turned out to be not a feasible attack vector.

The Evaluators decided to consider the following logical attack vectors for a public vulnerability search with reference to the ISO/OSI protocol stack:

- Transport layer: UDP BigFix Client (which is also present on BigFix Server), TLS1.2 all TOE component communications
- Application layer: HTTP REST API, HTTPS REST API

The Evaluators used various key words in Google search engine and in various vulnerability databases, including Common Vulnerabilities and Exposures (CVE), Exploit Database (EDB), Packet Storm (PS), SecurityFocus (SF), and HCL Customer Support, to try to find potential vulnerabilities. The Evaluators found 12 potential vulnerabilities to further investigate into.

The subsequent analysis of the potential vulnerabilities lead to concluding that none of those were applicable. Namely, 2 vulnerabilities could be excluded since they affect libraries not part of the TOE, 3 vulnerabilities could not be exploited in the evaluated configuration, 4 vulnerabilities were resolved with proper patching in version 10.0.1 of BigFix, 1 vulnerability was not applicable assuming that administrators of the TOE are trained, competent and aware of organizational security policies (assumption of the operational environment) and 2 vulnerabilities of the TLS version used in the TOE could not be exploited because either part of a function never called by the TOE or managed by a proper failure handler in the BigFix code. These last two vulnerabilities were verified by examining BigFix source code.

The Evaluators continued the vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE to be further investigated with penetration testing. However, none of the documentation revealed really obvious oversights or possible flaws. The Evaluators concentrated then on complex functions of the TOE which might include possible incorrect implementation and selected the following strategies for penetration testing:

- UDP fuzzing against the Client interface
- REST API fuzzing / Path Traversal
- Sniffing between TOE components

The fuzzcat and sFuzz tools were used for REST API fuzzing/Path Traversal, while Wireshark was used to intercept the traffic between TOE components. The Evaluators chose to fuzz specific TSFI, to identify flaws within the TOE.

At the end of the penetration testing sessions, no vulnerability was discovered that is exploitable in the intended operational environment of the TOE by attackers with Basic attack potential. The Evaluators also identified no residual vulnerabilities.