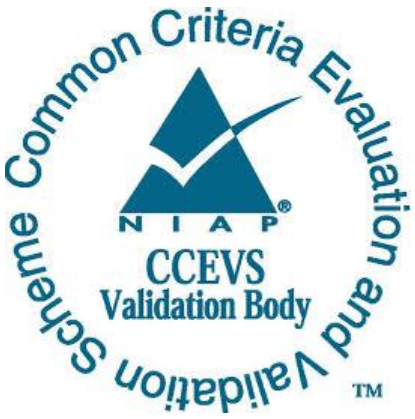
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report
IBM Inc.

IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2

Report Number: CCEVS-VR-10682-2016
Dated: February 26, 2016 Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Lead Validator: Patrick Mallett, PhD
The MITRE Corporation,
McLean, VA

Senior Validator: Jerome Myers, PhD
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Trang Huynh
King Ables
Hedy Leung
Swapneela Unkule

atsec information security corporation,
Austin, TX

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Evaluated Configuration 4
3.2 Physical Scope of the TOE 4
4 Security Policy 4
4.1 Cryptographic Support 5
4.2 User Data Protection 5
4.3 Identification and Authentication 6
4.4 Security Management 6
4.5 TOE Access 6
4.6 Trusted Path/Channels 7
5 Assumptions 7
5.1 Intended Usage of the TOE 7
6 Documentation 8
6.1 Design Documentation 8
6.2 Guidance Documentation 8
7 IT Product Testing 8
7.1 Developer Testing 9
7.2 Evaluation Team Independent Testing 9
8 Evaluated Configuration 9
9 Results of the Evaluation 9
9.1 Evaluation of the Security Target (ASE) 9
9.2 Evaluation of the Development (ADV) 9
9.3 Evaluation of the Guidance Documents (AGD) 10
9.4 Evaluation of the Life Cycle Support Activities (ALC) 10
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 10
9.6 Vulnerability Assessment Activity (VAN) 11
9.7 Summary of Evaluation Results 11
10 Validator Comments/Recommendations 11
11 Annexes 11
12 Security Target 11
13 Glossary 11
14 Bibliography 12

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the IBM BigFix Endpoint Manager solution provided by IBM, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Common Criteria Testing Laboratory (CCTL) atsec information security corporation in Austin, TX, United States of America, and was completed in February, 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL atsec information security corporation. The evaluation determined that the product is both **Common Criteria (CC) Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of the assurance requirements set forth in the "Protection Profile for Network Devices version 1.1" with "Errata #3."

The TOE is the IBM BigFix Endpoint Manager 9.2 client and server software components, operating system, and hardware (IBM System x3500 M5 server along with a monitor, keyboard, and mouse).

The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL using the "Common Methodology for IT Security Evaluation (Version 3.1, Rev 4)" for conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev 4)". This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

In addition to the assurance requirements specified in the NDPP, the evaluation team performed the ASE assurance activities defined in the CEM, so that all assurance activities specified at EAL1 have been performed by the laboratory.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The CCTL atsec information security corporation evaluation team concluded that the Common Criteria requirements specified by the "Network Device Protection Profile version 1.1" (NDPP) have been met.

The technical information included in this report was obtained from the "IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2 Security Target" and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) and against Protection Profile (PP) Assurance Activities in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including the following.

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST): describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation
- The Protection Profile to which the product is conformant
- The organizations and individuals participating in the evaluation

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2 and operating system executing on the following hardware: • IBM System x3500 M5 server
PP	Protection Profile for Network Devices Version 1.1, 8 June 2012
ST	IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2 Security Target, Version 1.0
ETR	Evaluation Technical Report For IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	IBM, Inc.
Developer	IBM, Inc.
CCTL	atsec information security corp., Austin, TX
CCEVS Validators	Kenneth B. Stutterheim, Aerospace Corporation, Columbia, Md Patrick Mallet, The MITRE Corporation, McLean, VA

3 Architectural Information

Note that the following architectural description is based on the description presented in the Security Target.

The TOE is a single network server device comprised of hardware and all of the software components (applications and operating system) that reside on the hardware. The hardware model is the IBM System x3500 M5 server along with a monitor, keyboard, and mouse.

The TOE software is comprised of the following components.

- IBEM1 9.2.3.101 Server software component
- IBEM 9.2.3.101 Client software component
- Red Hat Enterprise Linux (RHEL) 6.6 Server (x86-64)

The TOE is a content-driven messaging and management system that distributes the work of managing IT infrastructures out to managed devices (a.k.a. endpoints). The TOE identifies vulnerable or misconfigured endpoints and allows authorized users to remediate identified issues across the network.

The TOE is connected to the following devices in the Operational Environment.

- The Audit Server (syslog) is used by the TOE to remotely store the TOE's audit records.
- The Database Server is used by the TOE to store certain TSF data.
- Endpoints are servers, PCs, laptops, etc. managed by the TOE.
- Relays are endpoint aggregators used by the TOE to offload direct communications with endpoints. Relays are also endpoints.
- Remote Consoles are remote computers used by administrators to manage the TOE and endpoints.

The TOE and its managed endpoints reside on an air gapped network. The TOE utilizes a patented Fixlet® technology to identify vulnerable or misconfigured endpoints and allows authorized users to remediate identified issues across the network.

Fixlets can be downloaded from an IBM BigFix Fixlet Server over the Internet and then imported by the TOE. Since the TOE is on an air-gapped network with no Internet access, a separate Microsoft Windows system with Internet access and with the IBEM Airgap tool installed on the system is required to perform this download. Once the Fixlets are downloaded to this Microsoft Windows system, an administrator using portable media like a USB drive transfers the Fixlets to the TOE.

3.1 TOE Evaluated Configuration

The evaluation covers IBM BigFix Endpoint Manager 9.2 client and server components and operating system on the following devices.

IBM System x3500 M5 server along with a monitor, keyboard, and mouse. The IBM System x3500 M5 server contains:

- One Intel Xeon E5-2637 v3 series processor
- Quad-port Gigabit Ethernet
- One Gigabit management port
- One IBM 1.2TB 10K 6Gbps SAS 2.5" G3HS HDD
- ServeRAID M5210 SAS/SATA Controller for IBM System x
- 8GB High-speed 2133 MHz DDR4 SDRAM Registered DIMMs
- IBM HH DVD-ROM
- Seven Peripheral Component Interconnect Express (PCIe) 3.0 slots
- Two internal USB ports
- Six external USB ports (two front, four rear)
- One DB-15 VGA port

Description of air-gapped network Operational Environment components:

- 1 or more IBEM Console software component
- 0 or more IBEM Relay software component
- 0 or more IBEM Client software component (installed on systems other than the TOE)
- 1 IBM DB2 database (the database application on the database server) 1 Syslog server (for storing audit records remotely)

3.2 Physical Scope of the TOE

The TOE is a Network Device which is composed of a hardware platform and its system software. The TOE is designed to be used inside of an organization air-gapped from the Internet (e.g., not connected to the Internet) in a non-hostile environment. The TOE must be located in a protected environment (e.g., server room) where only trusted administrators have access to the physical computers. No other software can reside on the TOE.

4 Security Policy

This section summaries the security functionality of the TOE, which is as follows.

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Secure management
6. Protection of the TOE Security Functionality (TSF)
7. TOE access
8. Trusted path/channels

4.1 Cryptographic Support

The TOE contains the RHEL OpenSSL package for cryptography and Transport Layer Security (TLS).

The TOE uses the RHEL OpenSSL package in the Federal Information Processing Standards Federal Information Processing Standard (FIPS)-enabled mode for TLS and TLS/HTTPS communications between itself and other non-TOE systems (i.e., endpoints, relays, remote consoles, the database server, the audit server), except for User Datagram Protocol (UDP) communications.

The TOE uses Rivest-Shamir-Adleman (RSA) asymmetric key pairs for key establishment in the TLS and TLS/HTTPS protocols. The connections between the TOE and the database server and between the TOE and the audit server support TLS 1.0 in the evaluated configuration. All other TLS connections support TLS 1.0, TLS 1.1, and TLS 1.2 in the evaluated configuration.

The TLS and TLS/HTTPS protocols use the RSA algorithm with key sizes of 2048-bits or greater. These protocols use the Advanced Encryption Standard (AES) 128-bits and 256-bits cryptographic algorithms in cipher block chaining (CBC) mode for symmetric cryptography. These protocols also use the secure hash algorithms (SHAs) of SHA-1 and SHA-256 for cryptographic hashing and keyed-hash message authentication.

The TOE also supports several other block cipher modes of chaining for AES. A list of the modes is in section 7.1.2. In addition, the TOE supports SHA-224, SHA-256, SHA-384, and SHA-512 for cryptographic hashing and keyed-hash message authentication.

The TOE overwrites all secret keys, private cryptographic keys, and critical security parameters (as defined by NDPP v1.1) once they are no longer required.

The RHEL OpenSSL package in FIPS-enabled mode contains a deterministic random bit generator (DRBG) that uses CTR_DRBG (AES). This DRBG is used by the TOE to fulfill various cryptographic keying requirements. For entropy, the DRBG uses a software-based noise source.

4.2 User Data Protection

The TOE ensures that packets sent through the TOE are made unavailable. The TOE does not provide pass-through capabilities for network packets.

4.3 Identification and Authentication

The TOE's administrative interfaces are as follows.

- IBEM Console (remote GUI)
- Local OS console (RHEL)

All administrative interfaces require each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user. All administrative interfaces support password lengths of 15 characters or greater. For all administrative interfaces, the password composition includes upper case letters, lower case letters, numbers, and special characters. These interfaces provide obscured feedback of authentication data to the administrative user during the login process.

The authentication mechanisms for all administrative interfaces are local to the TOE. The TOE does not use remote authentication mechanisms such as Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, etc. The administrator account data used by the IBEM Server software component is stored on the database server. When an administrator logs in to the TOE from the IBEM Console interface, the IBEM Server software component retrieves the administrator's I&A data from the database server and performs the validation of the administrator's I&A data. When an administrator logs in to the TOE from the local OS console interface, the operating system identifies and authenticates the user using the operating system's local I&A files.

4.4 Security Management

The TOE allows an authorized administrator to manage the TOE locally via the local OS console and remotely via the IBEM Console. Only authorized administrators are allowed to use these interfaces and manage the TSF data of the TOE.

The TOE provides security management of its trusted update feature via the IBEM Console.

The TOE can associate a user with a single role. Note though that the IBEM Server software component uses a separate user authentication database than the RHEL operating system for defining user accounts and associating roles. The guidance documentation describes how to properly manage user accounts and roles between the IBEM Server software component and the operating system.

4.5 TOE Access

The TOE provides an administrator-specified advisory notice and consent warning message on all interactive user interfaces prior to establishing an administrative user session. The TOE also allows administrators to terminate their own interactive sessions.

The TOE enforces session locking of all local interactive sessions after an administrator-specified period of inactivity.

The TOE enforces session termination of all remote interactive sessions after an administrator-specified period of inactivity.

4.6 Trusted Path/Channels

The TOE uses trusted communication channels between itself and other trusted IT products. The TOE initiates a connection to the database server which is protected using TLS. In addition, the TOE initiates a connection to the audit server (syslog server) which is protected using TLS.

The TOE uses trusted path communications between itself and the IBEM Console. The IBEM Console initiates and uses TLS/HTTPS to communicate to the TOE.

5 Assumptions

5.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation.

As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP).

The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in the product were not covered by this evaluation.

The TOE requires the following in its operational environment:

- IBEM Console software component
- IBM DB2 database (the database application on the database server)
- Syslog server (for storing audit records remotely)
- Optionally IBEM Relay software component
- Optionally IBEM Client software component (installed on systems other than the TOE)

5.2 Intended Usage of the TOE

A.NO_GENERAL_PURPOSE

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6 Documentation

The following documentation was used as evidence for the evaluation of the IBM BigFix Endpoint Manager 9.2.

6.1 Design Documentation

None

6.2 Guidance Documentation

The following documentation was used as evidence for the evaluation of the IBM BigFix Endpoint Manager 9.2.

- IBM Endpoint Manager Version 9.2 API Reference Guide
- IBM Endpoint Manager Version 9.2 Configuration Guide
- IBM Endpoint Manager Version 9.2 Console Operator's Guide
- IBM Endpoint Manager Version 9.2 Configuration Guide
- IBM Endpoint Manager Version 9.2 Getting Started Guide
- IBM Endpoint Manager Version 9.2 Installation Guide
- IBM Endpoint Manager Version 9.2 Relevance Language Guide
- IBM Endpoint Manager Version 9.2 Web Reports Guide
- IBM BigFix Endpoint Manager 9.2 Common Criteria Guide, Version 1.1

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the IBM BigFix Endpoint Manager 9.2, Version 1, 2015-12-07.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team has verified the TOE by performing the tests specified in the Protection Profile for Network Devices Version 1.1.

8 Evaluated Configuration

The guidance documentation provides specific instructions for configuring the TOE into the evaluated configuration.

9 Results of the Evaluation

The results of the assurance requirements are described in this section and are presented in detail in the proprietary ETR.

All work units defined by the NDPP received a pass verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 4 and CEM Version 3.1 Revision 4. The evaluation determined the IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2 to be (compliant to) Part 2 extended, and to meet the assurance requirements defined by the NDPP.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each of the ASE CEM work units as well as the assurance activities specified in the NDPP. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions. This is a statement of security requirements which the IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2 product meets and that are consistent with the CC, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and NDPP and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team examined the documentation and found it adequate to aid in understanding how the TSF provides the security functions. The documentation consists of a functional specification contained in the Security Target and Guidance documents.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activities specified in the NDPP. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance (Console Operators Guide and the Configuration Guide) in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and NDPP and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and assurance activities specified in the NDPP. The ALC evaluation ensured the TOE is identified so that the consumer is able to properly identify the evaluated TOE and that the TOE identification is consistent with the Security Target and the CC guidance.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and NDPP and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit and assurance activities specified in NDPP. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team performed devised an independent set of tests as mandated by the protection profile.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and NDPP and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each of the VAN CEM work units (AVA_VAN.1 and AVA_NDPP.1) and assurance activities specified in the NDPP. Based on the analysis above, the evaluator determined that no applicable potential vulnerabilities are documented in publicly available sources. The evaluation team produced and performed penetration tests and found no unexpected results.

The validation team reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and NDPP and that the conclusion reached by the evaluation team was justified.

The evaluation team did determine that there is a non-public potential vulnerability for OpenSSL that will be resolved once it is public with a patch and subsequent testing.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the testing defined by the NDPP and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM and NDPP and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

None

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as IBM BigFix Endpoint Manager Common Criteria TOE Release 9.2 Security Target, Version 1.0.

13 Glossary

The following definitions are used throughout this document:

Common Criteria Testing Laboratory (CCTL)	IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct

	Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource required from the sponsor or developer by the evaluator or by the evaluation authority to perform one or more evaluation or oversight activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	TOE is that software, firmware and/or hardware that is configured as an IT system/product and the associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the certification body leading to the issuance of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The evaluation team used the following documents to produce this Validation Report:

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
- Protection Profile for Network Devices Version 1.1, 8 June 2012.