National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

BigFix Enterprise Suite (BES), Version 7.1.1.315

Report Number: CCEVS-VR-VID10214-2009
Dated: 16 January 2009
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 6757
Fort George G. Meade, MD 20755-6757

1. EXECUTIVE SUMMARY 3
2. IDENTIFICATION 4
3. SECURITY POLICY 5
4. ASSUMPTIONS AND CLARIFICATION OF SCOPE 5
4.1 THE FOLLOWING ARE ASSUMPTIONS MADE FOR THE ENVIRONMENT OF THE TOE: 5
4.2 CLARIFICATION OF SCOPE 6
5. ARCHITECTURAL INFORMATION 6
6. DOCUMENTATION 9
7. IT PRODUCT TESTING 10
8. EVALUATED CONFIGURATION 11
9. RESULTS OF THE EVALUATION 12
9.1 EVALUATION OF THE SECURITY TARGET (ST) (ASE) 12
9.2 EVALUATION OF THE CM CAPABILITIES (ACM) 12
9.3 EVALUATION OF THE DELIVERY AND OPERATION DOCUMENTS (ADO) 12
9.4 EVALUATION OF THE DEVELOPMENT (ADV) 12
9.5 EVALUATION OF THE GUIDANCE DOCUMENTS (AGD) 12
9.6 EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC) 12
9.7 EVALUATION OF THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE) 12
9.8 VULNERABILITY ASSESSMENT ACTIVITY (AVA) 13
10. VALIDATOR COMMENTS / RECOMMENDATIONS 13
11. ANNEXES 13
12. SECURITY TARGET 13
13. GLOSSARY 13
14. LIST OF ACRONYMS 14
15. BIBLIOGRAPHY 15

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of BigFix Enterprise Suite (BES), Version 7.1.1.315. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in December 2008. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Conformant and Part 3 Conformant**, and meets the assurance requirements of EAL 3.

The Target of Evaluation (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 a number of Fixlet Sites that are maintained by the BigFix Fixlet Server which is outside the TOE evaluated configuration. Each Fixlet Site contains pre-tested, pre-packaged Fixlet messages that provide out-of-the-box management solutions.

Fixlet messages can optionally also be developed in-house by administrators to address policy, configuration and vulnerability concerns specific to an enterprise. In-house fixes are known as Actions as these are developed by an authorized administrator to address specific situations. Note that Fixlets and Fixlet Sites are not part of the TOE – 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; and,
- View, modify and audit properties and configurations of the networked client computers.

The TOE contains built-in public/private key encryption capabilities to ensure the authenticity of the Fixlet messages and remedial Actions. Each Fixlet and Action received by a BES client is authenticated by verifying a signature affixed by the applicable administrator to ensure that it was generated by an administrator authorized to perform corresponding operations. These authorized operations instruct BES 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.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). 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 and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, reviewed 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 SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level 3 (EAL 3) have been met.

The technical information included in this report was obtained from the BigFix Enterprise Suite Version 7.1.1.315 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) for Evaluation Assurance Level (EAL) 1 through 4 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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	BigFix Enterprise Suite Version 7.1.1.315 (software only TOE)
Protection Profile	Not applicable
Security Target	BigFix Enterprise Suite Security Target, version 1.0, December 16, 2008
Evaluation Technical Report	BigFix Enterprise Suite Version 7.1.1.315 Final Non-Proprietary ETR – Part I, version 1.1, December 26, 2008 BigFix Enterprise Suite Version 7.1.1.315 Final Proprietary ETR – Part II, version 1.1, December 26, 2008
CC Version	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	BigFix, Inc.
Developer	BigFix, Inc.

Common Criteria Test Lab	SAIC, Columbia, MD
CCEVS Validators	Dianne Hale, NIAP/CCEVS Jerome Myers, Aerospace Corporation

3. Security Policy

BES provides the following security functions:

- Audit - Audit records are generated by the TOE and are stored in the BES database in the IT Environment.
- Cryptographic Support – The TOE authenticates and ensures the integrity of Fixlet messages and remedial Actions as they are collected, distributed and deployed by various components of the TOE across the network by generating encryption key pairs.User Data Protection - The TOE provides a Fixlet Information Flow Control Security Function Policy (SFP) and Action Information Flow Control SFP to control the application of Fixlets and Actions.
- Identification and Authentication (I&A) - The TOE requires users (i.e., administrators) to be identified and authenticated before completing any security management related actions.
- Security Management - The TOE provides security management functions that can only be accessed by authorized administrators.
- Protection of the TSF - Data transfer is protected by enforcing the information flow SFPs largely via the use of cryptographic signature verification to ensure authenticity and integrity of Fixlet and Action messages carrying the instructions of authorized administrators. The TOE protects the security of audit data and operation results data gathered on networked client computers by encrypting this data before it is transmitted over the network.

4. Assumptions and Clarification of Scope

4.1 The following are assumptions made for the Environment of the TOE:

- The users of the computers hosting the BES components are willing participants that benefit from the security functions of the BES and will not willfully attempt to circumvent any BES security functions. This primarily applies to the target machines where the Client component is installed, though it applies to all hosting computers in the enterprise. Basically, since the BES is an application within its host, a malicious user could potentially cause the BES on that computer to malfunction.
- Fixlets and Actions defined by authorized administrators and other publishers (e.g., BigFix) will be suitable to perform the task they were defined to perform. While the BES serves to facilitate the distribution of Fixlets and Actions in a secure manner, the BES cannot control specifically what individual Fixlets or Actions might actually do nor ensure they will be effective in doing that. Hence, it is up to the Fixlet and Action developers to ensure they are effective (e.g., through testing).
- Authorized administrators are non-hostile and adhere to all applicable administrator guidance.
- The computers hosting the BES components and the database are physically secure to a degree appropriate to protect the BES as well as themselves. Each hosting computer needs to protect the hosted BES components as well as any other content that the user may value.
- The Web Reports component the BES product is an optional installation and was not tested as part of the evaluated configuration. The Web Reports feature is a web server that provides read-only data from the BES Database via any standard web browser. A BigFix Administrator can optionally choose to install Web Reports. When installed it functions as a Windows service and stopped and started via the Windows Service control panel.
- The BES components will be installed within operating systems that are configured so that the BES components will be protected from potential tampering by untrusted users. This includes both appropriate levels of physical protection for the host machine and logical protection stemming from a well-configured (e.g., ‘hardened’) operating system where, for example,

unnecessary services are disabled and only necessary and authorized users can log in.

- The BES database will be configured so that any communication between the TOE and the database application will be secure. By placing it on the same host as the BES Server, the communication issue is partially resolved. Communication with the applicable BES Consoles also needs to be secured using available mechanisms provided by the chosen database application and underlying operating system (e.g., IPSEC). In addition, the BES Database is expected to be configured so that it is appropriately protected by the database application. The BES must be configured to authenticate itself to the database application so that access can be limited based on access controls implemented within the database application.

4.2 Clarification of Scope

- The BES database, which is often collocated on the computer hosting the Server, is accessible via ODBC. The Server and the Console are the TOE components that use the BES database to store and retrieve applicable data. Note that BigFix has published guidance so that users could potentially develop their own applications to access TOE-related data, provided they have applicable BES database authorizations. However, the development and use of other applications to access TOE data, while not forbidden, is outside the scope of this evaluation.
- Relays are considered an optional TOE component – they are not required for the operation of the TOE but are available as part of the product and so can be installed and enabled for use in the evaluated configuration.
- The BES database is either MSDE 2000 (which supports only a limited configuration) or SQL Server 2000 or 2005 both of which are commercial applications outside the TOE (i.e., in the IT environment); though they can reside on the same physical computer. The database is used by the TOE in order to store and retrieve applicable Fixlets and Actions as well as TOE configuration data. The BES database is expected to be configured so that only authorized users can access any contents associated with the TOE. The BES database is also expected to be configured so that its ODBC interface and communications are protected in a manner appropriate to the environment in which it is being used. Note that the BES Server can be configured to periodically collect pre-defined Fixlets from BigFix via a BigFix Fixlet Server. Those, like any locally developed Fixlets, are stored in the BES database and are available for use by administrators in monitoring Clients.
- The TOE includes the capability to run an API, which allows programmatic access to TOE functions. This is an optional capability that was not tested as part of the evaluated configuration.
- The TOE also includes the capability for customers to write their own Fixlets using the BES Relevance language. Again, this is an optional capability that was not tested as part of the evaluation.
- Although the TOE can be also be configured to access the BigFix Fixlet Server to mirror its contents, the BigFix Fixlet Server is outside the TOE.
- Fixlets or Actions that modify the TOE will invalidate the evaluation. BigFix Fixlets identify the changes that are being made and changes to the evaluated product can be prevented. However, the customer is responsible for any Actions that are locally developed and implemented.

5. Architectural Information

The TOE is comprised of four software components, BES Server, BES Console, BES Client (i.e. Agent) and BES Relay. The TOE provides an authorized user the ability to assess the current 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) in order to obtain the most current Fixlets and/or Actions.

The TOE architecture includes the following subsystems:

- *Server Subsystem*: BES server application
- *Console Subsystem*: BES console application
- *Client Subsystem*: BES client application
- *Relay Subsystem*: BES relay application

Note that of the four subsystems in the TOE, only the Relay subsystem is not security relevant.

The figures below depict a typical application of the TOE and an overview of the TOE architecture.

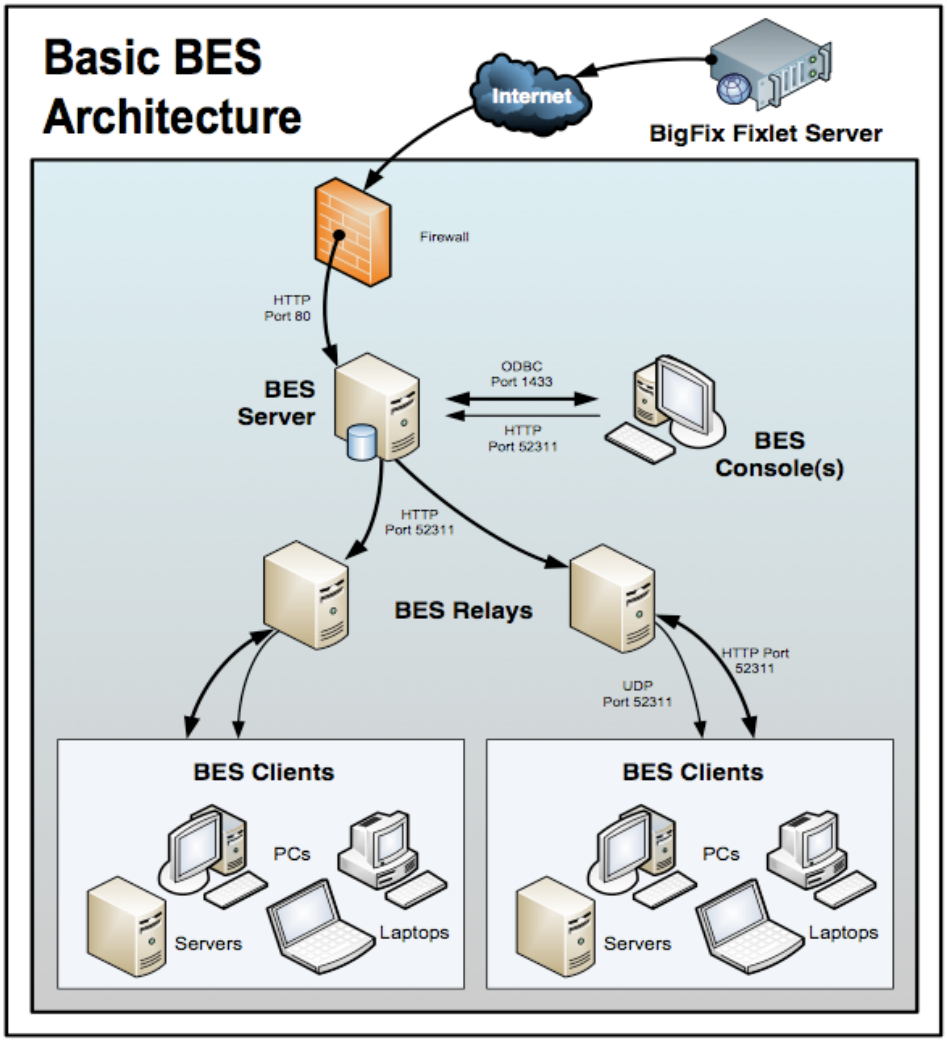

Figure 1 Typical Architecture

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 the figure 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 2, below, presents a more logical view of the primary TOE components in the context of their host computers. Note that, while not depicted below, 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.

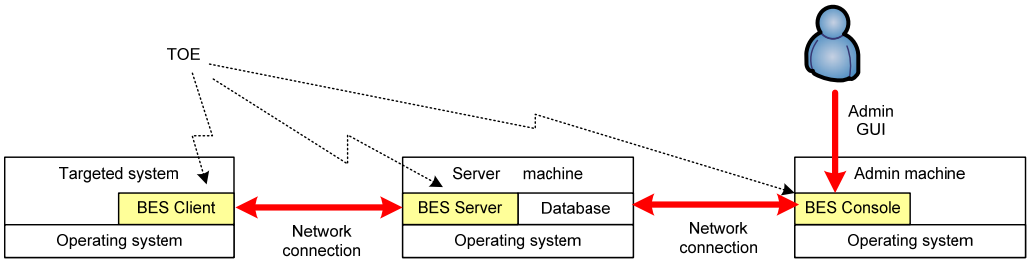

Figure 2 TOE Architecture

Server — the Server is a collection of interacting services, including application services, and a web server. The Server manages and coordinates the flow of information to and from individual computers (i.e., clients) and stores the results in the BES database. The Server offers the following features:

- The Server gathers content from the Internet (i.e., Fixlets offered by the BigFix Fixlet Server) and then redistributes the content to the BES Clients directly (or through BES Relays). When a Client detects that a Fixlet has become relevant, it reports to the Server.
- The Server monitors for changes in Fixlet content for all the Fixlet sites (e.g., BigFix Fixlet Server) to which the TOE is subscribed and it downloads these changes to the Server and makes them available to the rest of the components.
- The Server offers a GUI interface (local to the hosting operating system) for the administrators to use to create user accounts, manage the refresh rates, and Masthead management.

Console — the Console provides the ability for an authorized administrator to view and manage their entire network of computers by enabling automated distribution of fixes, software deployment, vulnerability analysis (i.e., systems requiring patches, updated Service Packs (SPs), configuration violations and/or enterprise security policy violations), and remediation from a central location.

Clients — Clients are installed on every computer (personal computer, server, workstation, desktop, laptop, etc.) within the enterprise that will be managed by the TOE. Clients are also referred to as Agents and these terms are interchangeable. Clients access a collection of Fixlet messages that detect security holes, vulnerabilities, and other configuration issues and Action messages capable of implementing corrective actions received from the Server via the Console. In most cases, the Client operates silently in the background so that users are not aware of what actions are taking place on their system; however, when an action requires user input, the Operator is able to provide friendly screen prompts for the user.

Relays — Relays can increase the efficiency of the TOE. Instead of forcing each networked computer to directly access the Server, Relays can be installed on any computer within the enterprise to distribute the workload by storing and forwarding data (i.e., messages) passing between Servers and Clients. Relays query the Server (or another Relay) for Fixlet and Action messages and Client machines utilize Relays exactly as they would Servers. Relays do not need to be dedicated computers and can connect to other Relays for additional efficiency. When Relays are installed they report themselves to their corresponding Server, and subsequently the Clients are made aware of them and can access their Server via available Relays. Relays work by:

Given that the TOE is a set of software applications or components, its physical boundaries are defined by those components: Server, Console, Client and Relays. Note that each of these components has a set of requirements for its hosting computer as follows:

Server: The hardware requirements for the Server component depends on the deployment (i.e., how many Clients are attached); and, specific data can be obtained from http://support.bigfix.com/cgi-bin/redir.pl?page=serverreq. The Server can be installed on the following OS platforms: Microsoft Windows 2000 and Server 2003. A Microsoft MSDE 2000, SQL Server 2000, or SQL Server 2005 database is required to be accessible to the Server to serve as the BES database.

Console: The Console can be installed on the following OS platforms: Windows 2000, XP Home, XP Professional with MDAC 2.7.

Client: The Client can be installed on the following OS platforms: Windows 95, 98, NT 4+, Me, 2000, Server 2003, XP; Red Hat Linux 8.0, 9.0; Red Hat Linux Enterprise 3, 4, 5; Solaris 7, 8, 9, 10; HPUX 11.00, 11.11, 11.23; AIX 5.1, 5.2, 5.3; SUSE 8, 9, 10; Mac OS X 10.3, 10.4, and 10.5.

Relay: Relays are optional and can be installed on any Windows server, workstation, PC or laptop within the TOE environment running Microsoft Windows NT SP6a, 2000, XP, Server 2003, or Vista, Red Hat Linux.

The TOE can be configured to access the BigFix Fixlet Server to mirror its contents. The BigFix Fixlet Server is outside the TOE and can typically be accessed across the Internet on TCP port 80. Content from the BigFix Fixlet Server is accessed just like content on the BES Server component.

6. Documentation

The BigFix Enterprise Suite is delivered with a number of guidance documents as follows:

- BigFix Enterprise Suite Delivery, Installation, Generation and Startup Procedures, Version 1.5, 12/16/2008
- BigFix Enterprise Suite (BES) Console Operator's Guide, Version 7.1, 7/26/2008
- BigFix Enterprise Suite (BES) Administrator's Guide, Version 7.1, 7/25/2008
- BigFix Action Language Reference, v7.0, 9/08/2008
- BigFix Relevance Language Reference, v6.0, 11/03/2006
- BigFix Enterprise Suite Platform API Reference, v6.0, 3/30/2006
- Solaris Inspector Library, v6.0
- Red Hat & SUSE Linux Inspector Library, v6.0
- HP-UX Inspector Library, v6.0
- AIX Inspector Library, v6.0
- Windows Inspector Library, v6.0
- Macintosh Inspector Library, v6.0
- BigFix® Enterprise Suite (BES™) Database API Reference, 4/6/2006, v6.0
- BigFix® Enterprise Suite (BES™) Client Compliance API Reference, v5.1, 4/28/2005
- BigFix Session Library A Guide to the BigFix Session Inspectors, July 7, 2006, Compatible with BES 6.0
- BigFix Enterprise Suite Error Messages, version 1.2, 9/13/2007

Only the following documents were evaluated and should be considered as evaluator verified:

- BigFix Enterprise Suite Delivery, Installation, Generation and Startup Procedures, Version 1.5, 12/16/2008
- BigFix Enterprise Suite (BES) Console Operator's Guide, Version 7.1, 7/26/2008
- BigFix Enterprise Suite (BES) Administrator's Guide, Version 7.1, 7/25/2008

The additional documentation in the first bulleted list above provides information about developing Fixlet messages, which can optionally also be developed in-house by administrators to address policy, configuration and vulnerability concerns specific to an enterprise. This capability was not tested as part of the evaluated configuration, since the content of any user-developed Fixlet is unknown and therefore is not testable.

The following documentation is used as evidence for the evaluation of BES:

CC Assurance	CI Unique Identifier and description
Analysis of Correspondence (RCR)	BigFix Design Document, Version 0.6, December 18, 2008
Misuse Analysis (MSU)	BigFix Enterprise Suite Delivery, Installation, Generation and Startup Procedures, Version 1.5, 12/18/2008 BigFix Enterprise Suite (BES) Console Operator's Guide, Version 7.1, 7/26/2008 BigFix Enterprise Suite (BES) Administrator's Guide, Version 7.1, 7/25/2008
Configuration Management (ACM)	BigFix Enterprise Suite (BES) Configuration Management, version 1.2, 10/15/2007 BigFix Enterprise Suite (BES) Configuration Item List, version 1.2, 10/15/2007
Delivery and Operation (ADO)	BigFix Enterprise Suite Delivery, Installation, Generation and Startup Procedures, Version 1.5, 12/18/2008
Functional Specification (FSP)	BigFix Design Document, Version 0.6, December 18, 2008
Administration Guide (ADM)	BigFix Enterprise Suite (BES) Console Operator's Guide, Version 7.1, 7/26/2008 BigFix Enterprise Suite (BES) Administrator's Guide, Version 7.1, 7/25/2008 BigFix Enterprise Suite Error Messages, Version 1.2, 9/13/2007
Installation Guide (IGS)	BigFix Enterprise Suite Delivery, Installation, Generation and Startup Procedures, Version 1.5, 12/18/2008
High-level Design (HLD)	BigFix Design Document, Version 0.6, December 18, 2008
Identification of Security Measures (DVS)	BigFix Enterprise Suite Lifecycle, Version 1.3, October 2, 2007
Security Target (ST)	BigFix Enterprise Suite Security Target, version 1.0, December 16, 2008
Test Documentation (ATE)	BigFix Enterprise Suite CC Test Cases, Version 2.4, August 25, 2008
Vulnerability Analysis (VLA)	BigFix Enterprise Suite Vulnerability Assessment, Version 1.0, December 3, 2007

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 Plan.

The developer provided 38 manual tests that tested all TOE functionality. The evaluation team executed all developer tests. In addition, the evaluation team ran additional tests of the Identification and Authentication function and performed a port scan on the TOE environment to identify any potential vulnerability. No TOE vulnerabilities were identified. Environmental vulnerabilities were addressed through guidance documentation.

The TOE was tested on a subset of the platforms by the Evaluation Team. The following table shows which of the claimed platforms were demonstrated in evaluator team testing (highlighted in yellow) and demonstrates that although testing was performed on a subset of the possible platforms, at least one of each type of OS was tested and in many cases several versions of the same OS type was tested. There were no

differences in TOE functionality noted for the different OS versions. Since at least one of each OS type was tested the evaluation team was confident that TOE functionality was adequately tested for the claimed platforms at EAL3.

Component	OS Type	OS Version	Evaluator Comments
Server	Microsoft Windows	Microsoft Windows 2000	Tested with Win 2000
		Microsoft Windows Server 2003	
Console	Microsoft Windows	Microsoft Windows 2000	Tested with WinXP Professional with MDAC 2.7
		Microsoft Windows XP Home	
		Microsoft Windows XP Professional with MDAC 2.7	
Client	Microsoft Windows	Microsoft Windows 95	Tested with WinXP (two platforms). Note that Win 95, 98, NT, and Me are provided for backwards compatibility. Testing was performed with the most common of the more up to date versions of Windows and a common client OS version
		Microsoft Windows 98	
		Microsoft Windows NT 4+	
		Microsoft Windows Me	
		Microsoft Windows 2000	
		Microsoft Windows Server 2003	
		Microsoft Windows XP	
	RedHat Linux	RedHat Linux 8.0	Tested 3 of the five Linux OSversions and at least one of the two "flavors," i.e., Enterprise and non-Enterprise. No differences in functionality were noted.
		RedHat Linux 9.0	
		Red Hat Linux Enterprise 3	
		Red Hat Linux Enterprise 4	
		Red Hat Linux Enterprise 5	
	Solaris	Solaris 7	Tested 3 of the four Solaris OS versions with no differences in functionality noted. Testing included the oldest and newest versions.
		Solaris 8	
		Solaris 9	
		Solaris 10	
	HPUX	HPUX 11.00	Tested the newest of three OS versions.
		HPUX 11.11	
		HPUX 11.23	
	AIX	AIX 5.1	Tested one of the three versions of the OS
		AIX 5.2	
		AIX 5.3	
	SUSE	SUSE 8	Tested the newest of three OS versions.
		SUSE 9	
		SUSE 10	
	Mac OSX	Mac OS X 10.3	Tested the newest of three OS versions.
		Mac OS X 10.4	
		Mac OS X 10.5	

8. Evaluated Configuration

The TOE evaluated configuration consists of the BES software running in the environment described in section 2 of this report. There are no excluded components of the BES as installed from BigFix. Note that the TOE includes the capability to run an API, which allows programmatic access to TOE functions. This

is an optional capability that was not tested as part of the evaluated configuration. The TOE also includes the capability for customers to write their own Fixlets using the BES Relevance language. Again, this is an optional capability that was not tested as part of the evaluation.

9. Results of the Evaluation

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

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 3 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 3 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of one document that included a functional specification, a high-level design document, and correspondence demonstration. The evaluation team ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 3 AGD CEM work unit. 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 in describing how to securely administer the TOE.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 3 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance.

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

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 3 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

10. Validator Comments / Recommendations

In addition to the information provided in Section 6, Clarification of Scope, the Validators would like to highlight the following:

The Security Target includes the assumption that the Fixlets and Actions (i.e., update packages sent by the TOE to client systems) will be suitable to perform the task that they were defined to perform. Therefore, the TOE does not require extensive testing of Fixlets and Actions to ensure that they do not impact the TOE, i.e., the actual function of the Fixlets and Actions is outside the scope of the TOE and only the secure delivery of the Fixlets and Actions is within the scope of the TOE.

The Validators found that the evidence reviewed prior and during the Final Validation Oversight Review (VOR) supported the determination that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validators agree that the CCTL presented appropriate rationales to support the evaluation results presented in the Evaluation Technical Report for the BigFix Enterprise Suite (BES) Version 7.1.1.315. The Validators conclude that the evaluation and Pass result for the ST and TOE are complete and correct.

11. Annexes

Not applicable

12. Security Target

The security target is the BigFix Enterprise Suite Security Target, version 1.0, December 16, 2008.

13. Glossary

The following definitions are used throughout this document:

Common Criteria Testing Laboratory (CCTL). An 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 (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Feature. Part of a product that is either included with the product or can be ordered separately.

Target of Evaluation (TOE). A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

Validation. The process carried out by the CCEVS Validation Body leading to the issue 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. List of Acronyms

API	Application Programming Interface
BES	BigFix Enterprise Suite
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FW	Firewall
IT	Information Technology
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PC	Personal Computer
SFR	Security Assurance Requirement
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

15. Bibliography

1. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005.
2. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
3. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.
5. Final Evaluation Technical Report for BigFix Enterprise Suite Version 7.1.1.315, version 1.1, December 26, 2008 Final Proprietary ETR – Part II.
6. BigFix Enterprise Suite Security Target, version 1.0, December 16, 2008.
7. NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories. Version 1.0, March 20, 2001.
8. SAIC CCTL Evaluation Procedures Annex, Version .20, January 31 2004.