BigFix Enterprise Suite
Security Target

Version 1.0

16 December 2008

Prepared by:
BigFix, Inc.
1480 64th Street
Suite 200
Emeryville, CA 94608

LIST OF TABLES

LIST OF FIGURES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The TOE is the BigFix Enterprise Suite (BES) 7.1.1.315 provided by BigFix. BES provides the means to authorize operators and allow those operators to monitor the configurations of authorized targeted systems on a network in the IT environment and also enables operators to take any necessary corrective actions, all from a centralized location.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment and the threats that are mitigated by the TOE.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL3.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – BigFix Enterprise Suite Security Target

ST Version – 1.0

ST Date – 16 December 2008

TOE Identification – BigFix Enterprise Suite (BES), Version 7.1.1.315

TOE Developer – BigFix, Inc.

Evaluation Sponsor – BigFix, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.

- Part 3 Conformant
- Assurance Level: EAL 3
- Strength of Function (SOF) Claim: SOF-Basic

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the ST.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology

The following acronyms and specific terminology pertain to BES. Note that CC-specific and other commonly used terms and acronyms are not defined here.

Action An Action is a change applied to a system in order to remediate issues identified by Fixlets. They are typically scripts written in the BigFix Action Language. A Fixlet that detects an issue may offer several different remediation Actions that authorized operators may choose from and deploy. For example, a Fixlet may detect a missing Windows Service Pack and offer an Action to download and install it on the relevant systems.

Administered Computers that an operator has authority to manage.

All Visible All Fixlets, Computers, and Actions visible (or authorized to) to a given operator.

BES BigFix Enterprise Suite

CGI Common Gateway Interface

Console Operator(s) Authorized Site Administrator, Master Operator, Operator

Fixlet A message that is the mechanism for targeting and describing a problematic situation on a computer and providing an automatic fix for it. For the purposes of this ST, the term Fixlet includes all of the different types of Fixlet messages to include Fixlets, Tasks, Analyses and Baselines.

Global (as used in the permissions chart) All Fixlets that are subscribed to by the BES deployment. Custom Fixlets created by operators (so-called Custom-Content) or those that are part of a Custom Site are not Global.

Installation Computer A secure computer (separate from the TOE Server) that hosts and runs the BES Installation Generator. This computer could be used as a Proxy Server for the TOE to subscribe to a trusted Fixlet site to obtain Fixlet messages.

Masthead Created during installation of the TOE that includes URLs for the Server CGI programs and other site information in a signed MIME message. The Masthead is central to accessing and authenticating the enterprise action site. The TOE brings content into the enterprise based on subscribed Mastheads. A Masthead is required for communicating with the BigFix Fixlet Server as it contains all the site-specific information needed to deploy Fixlets.

Master Operator A TOE Console operator with administrative rights. A Master Operator can do almost everything a Site Administrator can do with the exception of creating new users.

MDAC Microsoft Data Access Components

Operator An authorized user of the TOE Console. Ordinary Operators can deploy Fixlet actions and edit certain computer settings. Management rights are assigned by either a Site Administrator or Master Operator.

Private Custom Fixlets created by operators.

Signing Password The password specified during installation of the TOE that is used by an authorized user to sign an action for deployment.

Site Administrator The only TOE Console user with the right to create new users (i.e., Master Operator, Operator).

2. TOE Description

The Target of Evaluation (TOE) is BigFix Enterprise Suite (BES), Version 7.1.1.315. Note that there is no distinction between the BES product and the TOE since the TOE includes all parts of the product delivered to users and there are no specific restrictions imposed on the use of the product.

BES enables operators to monitor the configurations of targeted systems on a network in the IT environment from a centralized location. BES provides operators the ability to define corrective actions on individual targeted systems to be applied at the direction of the operator. Corrective actions can include, for example, installing an application or an application/operating-system update.

2.1 TOE Overview

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 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.

2.2 TOE Architecture

The TOE is comprised of four software components, BES Server, BES Console, BES Client (i.e. Agent) and BES 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 public key (signed by BigFix) specific to the site that is used, directly or indirectly, to authenticate any instructions from the BES 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 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 figures below depict a typical application of the TOE and an overview of the TOE architecture.

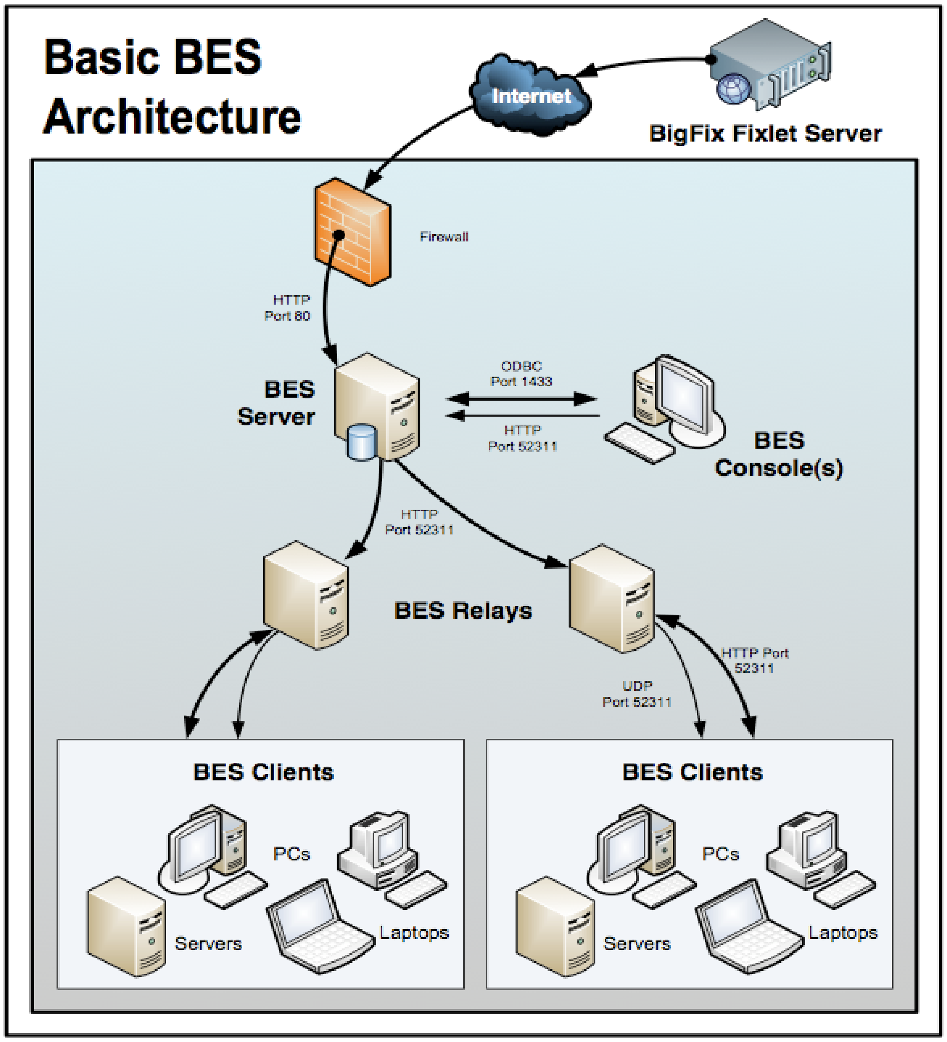

Figure 1 Typical Architecture

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.

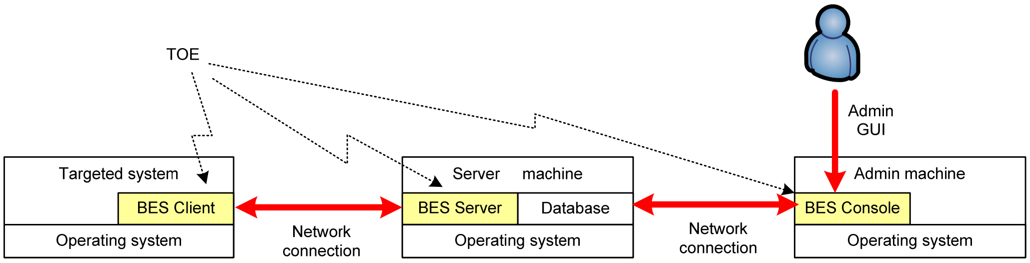

Figure 2 TOE Architecture

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. Note that 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 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). This component provides bandwidth advantages, as well as removing the need to configure individual BES Clients to connect to the Internet directly. Although it is possible to have BES Clients communicate directly over the Internet to fetch Fixlet messages and downloads, that configuration can cause additional network traffic and will not work in many enterprise environments with proxy servers.
- When the Client is installed on a new computer, it registers itself with the client registration component of the Server and the Client is given a unique Identifier (ID) based on its Internet Protocol (IP) address.
- When a Client detects that a Fixlet has become relevant, it reports to the Server using Hyper-text Transfer Protocol (HTTP) “POST” operation. It identifies the relevant Fixlet along with the registered ID of the Client computer. This information is passed on to the BES database and then becomes viewable in the Console. Also, other state changes are periodically reported by the Clients to the server directly or through Relays.
- 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.

The Server listens on a TCP port (52311 by default) for HTTP messages from Clients, Relays, and Consoles. Data files containing Fixlets, Actions, responses to actions performed on Clients, etc. are retrieved from and sent to the Server using HTTP messages. For the most part the Server just responds to HTTP requests. The exception is that the Server can issue UDP messages to Relays and Clients when new content (e.g., Fixlets) become available. Relays and Clients are configured to periodically poll the Server for new content, but if they receive such a message they will retrieve the updated content out of their normal cycle.

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.

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.

Console users, also known as Operators, can be in charge of flexibly defined groups of computers (e.g., client/agents) with varying degrees of freedom. The Site Administrator or a Master Operator has overall control of each Operator’s domain and the specific rights they have over that domain. The TOE supports three classes of Console users: Site Administrators, Master Operators, and (ordinary) Operators. See section 6.1.4 for details about their respective responsibilities.

The Console is invoked as an interactive application. It utilizes ODBC to access the BES database and HTTP to access the Server. Note that any data sent to the Server would be signed by the Operator using the console to ensure the authenticity and integrity of the applicable data and that property is transitive since any Clients ultimately receiving such data would be able to verify the signature of the issuer. The communications with the BES database via ODBC would be protected in the manner configured in the IT environment (per the database and hosting computers).

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.

The Clients listen on a UDP port (default 52311) for messages from the Server indicating that updated data is available for retrieval. The Clients use HTTP to connect to Relays and/or Servers in order to retrieve Fixlets and Actions and to send results of applying Fixlets and Actions back to a Server. Administrators can specify that the Clients encrypt these results before they are transmitted over the network.

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:

- Relieving Downstream Traffic: The Server distributes files such as patches or software packages and Fixlet messages to Clients. Relays can be set up to ease this burden so that the Server does not need to distribute the same file to every Client. Instead the file is sent once to the Relay, which in turn distributes it to the Clients. In this model, the Client connects directly to the Relay and does not need to connect to the Server.
- Reducing Upstream Traffic: In the upstream direction, Relays can compress and package data (including Fixlet relevance, action status and retrieved properties) from the Clients for greater efficiencies. During this process Relays may optionally decrypt and re-encrypt data sent from clients to ensure compression efficiencies. Administrators must designate which Relays are able to re-encrypt data.
- Reducing Congestion on Low-Bandwidth Connections: If the Server is communicating with computers in a remote office over a slow connection, designation of one of those computers as a Relay can help. Then, instead of sending patches over the slow connection to every Client independently, the Server only sends a single copy to the Relay(s) as needed and then the Relay distributes the file to the other computers in the remote office over its own fast LAN to effectively remove the slow connection bottleneck for remote groups on the network.
- Reducing Load on the Server: The Server has many duties including handling connections from Clients and Relays. At any given instant, the Server is limited in how many connections it can effectively service; however, Relays can buffer multiple Clients and upload the compressed results to the Server. Relays also distribute downloads to individual Clients, further reducing the workload of the Server and allowing the TOE to operate faster and more efficiently.

Note that 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.

Relays service a TCP port (default 52311) just like Servers so that they can establish connections to Clients and they in turn connect to a TCP port on a Server or another Relay in a chain in order to forward HTTP messages appropriately. Similarly, Relays proxy a UDP port (default 52311) so that messages from Servers regarding updated content can be forwarded and also acted upon by the Relay so that it can store and forward the updates to minimize network traffic to the extent it can.

The UDP messages serve only to get updates out to Clients earlier than their individual schedules might allow. The unreliable nature of UDP is not considered to be especially important given that it will take time to distribute updates in a large enterprise regardless. TOE users can mitigate any perceived issue by configuring the Client polling interval to be as short as necessary.

The content of essentially all HTTP messages going to Clients is signed by the applicable Operator or publisher of the content. The Client will verify the signature and act on the content only when the signature indicates the content is authentic and authorized. As such, the integrity of data going to Clients is ensured. Data gathered on clients and sent back to the Server is encrypted if the Administrator has previously designated that the Client should do so.

2.2.1 Physical Boundaries

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.

Note that 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.

2.2.2 Logical Boundaries

This section identifies the security functions that BES provides as apparent at the logical boundary of the TOE and includes:

- Audit,
- Cryptographic Support,
- User Data Protection,
- Identification and Authentication (I&A),
- Security Management, and
- Protection of the TSF.

2.2.2.1 Audit

The TOE generates audit records for an unspecified level of audit. It records date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event for the following events: Create User, Set Minimum Refresh Interval, Set Default Visibility & Client UI Icon, Edit Masthead, Initialize Action Site, Actions performed to manage sites, Change BES Client heartbeats, Create, edit, delete Fixlets, Groups, Activate/Deactivate Analyses, Take Fixlet Action, Take Custom Action, Modify Actions, Manage Administrative Rights, Create/Modify Retrieved Properties, View Fixlets, Computers, View Groups, View Unmanaged Assets, View Actions, View/Make Comments, Globally Hide/Unhide, Locally Hide/Unhide, Remove computer from database, Create/Delete Computer Groups, Modify Computer Groups, Create Custom Site, Modify Custom Site Owners, Modify Custom Site Readers/Writers. Audit records are generated by the TOE and are stored in the BES database in the IT Environment.

2.2.2.2 Cryptographic support

The TOE performs cryptographic operations by providing public/private key pairs for the purpose of digitally signing Fixlet messages and Actions within the infrastructure. These signatures enable the TOE to authenticate and ensure the integrity of Fixlet messages and remedial Actions as they are collected, distributed and deployed by various components of the TOE across the network.

The TOE generates public/private key pairs used for encryption that are distributed from the Sever to Clients and Relays. These encryption key pairs are distributed in the Masthead: a container that is digitally signed using the separate signing key pairs described above. The data gathered on Clients is encrypted using the encryption key pair, delivered over the network, and decrypted on the Server.

2.2.2.3 User data protection

The TOE provides a Fixlet Information Flow Control Security Function Policy (SFP) and Action Information Flow Control SFP that control the application of Fixlets and Actions via Clients. In general, Fixlets are provided by Operators or publishers (such as the BigFix Fixlet server) and Actions are provided by Operators. The TOE Server facilitates the distribution of applicable Fixlets and Actions to Clients and those Clients will only accept and apply Fixlets and Actions when it can be validated that they have come from an authorized source (e.g., an Operator assigned to manage that Client).

Note that the controlled distribution and application of Fixlets and Actions is really the primary security function of the TOE. It is not within the scope of the TOE to determine anything about what those Fixlets or Actions actually do or to ensure that it was effective. That is entirely up to those creating the Fixlets and Actions for deployment.

2.2.2.4 Identification and authentication

The TOE requires users (i.e., administrators) to be identified and authenticated before completing any security management related actions. Passwords must be a minimum of six characters long. Once the administrator is authenticated, the TOE enforces role-based rules and only a Site Administrator or Master Operator can change the rules and attributes on behalf of users.

2.2.2.5 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. All authorized administrators (i.e., Site Administrators, Master Operators, and Operators) must login to the console with unique name and password. Access to management functions is based on assigned roles.

2.2.2.6 Protection of the TSF

The TOE protects itself from attempts to bypass its security mechanisms. 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.

2.3 TOE Documentation

BigFix offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of the system security features. Refer to Section 6.2 for information about these and other evidence assurance documents associated with the BES.

3. Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 3) also serves as an indicator of whether the TOE would be suitable for a given environment.

Note that the focus of the threats is on the security problem addressed by the TOE. Any threats against the TOE itself are indirect and only implied insofar as the TOE must ensure its own protection in order to address the threats identified below.

3.1 Threats

T.MANAGE An enterprise network might be mismanaged due to a lack of centralized security management control.

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions provided by the TOE, which may go undetected.

T.SECURE An enterprise network might be subject to an undetected attack by attackers attempting to issue unauthorized security management instructions.

3.2 Assumptions

A.BENIGN The users of the computers hosting the TOE components are willing participants that benefit from the security functions of the TOE and will not willfully attempt to circumvent any TOE security functions.

Application note: This primarily applies to the target machines where the TOE Client component is installed, though it applies to all hosting computers in the enterprise. Basically, since the TOE is an application within its host, a malicious user could potentially cause the TOE on that computer to malfunction.

A.FIXES The 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.

Application note: While the TOE serves to facilitate the distribution of Fixlets and Actions in a secure manner, the TOE 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).

A.NOEVIL Authorized administrators are non-hostile and adhere to all applicable administrator guidance.

Application note: This is related to A.BENIGN, but adds that administrators will also adhere to the applicable guidance, particularly the evaluated guidance.

A.PHYSEC The computers hosting the TOE components and the TOE’s database are physically secure to a degree appropriate to protect the TOE as well as themselves.

Application note: Each hosting computer needs to protect the hosted TOE components as well as any other content that the TOE user may value.

4. Security Objectives

The following subsections describe objectives for the TOE and its environment that are consistent with the environment described in the previous section.

4.1 Security Objectives for the TOE

O.AUDIT The TOE must generate audit records for the security management functions of the TOE.

O.DIGSIG The TOE must provide digital signing and verification of signature for administrators and other publishers to authenticate Fixlets or Actions on behalf of that issuer.

O.I&A The TOE must successfully identify and authenticate users before granting access to protected TOE security functions.

O.MANAGE The TOE must provide the means to effectively manage the TOE security functions as well as target machines in the IT environment and ensure those functions are available only to authorized administrators.

O.MEDIATE The TOE must ensure that only authorized instructions are applied to target machines in the IT environment.

4.2 Security Objectives for the IT Environment

OE.DOMSEP The IT environment must provide domain separation that protects the TOE from interference and tampering by untrusted subjects.

4.3 Security Objectives for the non-IT Environment

OE.FIXES The issuers of Fixlets and Actions will ensure that they are correctly designed and tested to perform their expected functions.

OE.GUIDAN The TOE will be delivered, installed, administered, and operated in a manner that maintains security.

OE.NOEVIL Only administrators that are non-hostile and will follow applicable administrator guidance will be assigned to manage the TOE and IT environment targets.

OE.PHYSEC The computers hosting the TOE and its database will be physically secure to an appropriate degree.

OE.USERS Each enterprise user will be expected to not willfully take any action to subvert the security functions of the TOE.

5. IT Security Requirements

This section includes statements of security requirements that are included in the BES for which operations have been completed or modified to conform to international interpretations. This section describes the Security Functional Requirements (SFRs) for the TOE and the IT environment, as well as the Security Assurance Requirements (SARs) for the TOE at EAL3.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are being satisfied by BigFix Enterprise Suite (BES). All SFRs are drawn from Part 2 of the CC.

Use of United States English has been used instead of United Kingdom English as an authorized CC refinement that does not require the use of the refinement convention to identify.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1(a-e): Cryptographic Operation
FDP: User Data Protection	FDP_IFC.1(a-b): Subset Information Flow Control
	FDP_IFF.1(a-b): Simple Security Attributes
FIA: Identification and Authentication	FIA_ATD.1: User Attribute Definition
	FIA_UAU.1: Timing of authentication
	FIA_UID.2: User Identification before any Action
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behaviour
	FMT_MSA.1(a-c): Management of Security Attributes
	FMT_MSA.2: Secure Security Attributes
	FMT_MSA.3(a-b): Static Attribute Initialization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1: Non-bypassability of the TSP

Table 1 TOE Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**the following events: Create User, Set Minimum Refresh Interval, Set Default Visibility & Client UI Icon, Edit Masthead, Initialize Action Site, Actions performed to manage sites, Change BES Client heartbeats, Create, edit, delete Fixlets, Groups, Activate/Deactivate Analyses, Take Fixlet Action, Take Custom Action, Modify Actions, Manage Administrative Rights, Create/Modify Retrieved Properties, View Fixlets, Computers, View Groups, View**

Unmanaged Assets, View Actions, View/Make Comments, Globally Hide/Unhide, Locally Hide/Unhide, Remove computer from database, Create/Delete Computer Groups, Modify Computer Groups, Create Custom Site, Modify Custom Site Owners, Modify Custom Site Readers/Writers].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no other information**].

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified key generation algorithm [**RSA key generation; DSA key generation**] and specified cryptographic key sizes [**1024, 2048, 4096-bit**] that meet the following: [**ANSI X9.44; FIPS 186-1**].

5.1.2.2 Cryptographic key generation (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**FIPS 140-2, Level 1 cryptographic key destruction requirements**].

5.1.2.3 Cryptographic operation (FCS_COP.1a)

FCS_COP.1a.1 The TSF shall perform [**digital signing and verification of signatures**] in accordance with a specified cryptographic algorithm [**RSA digital signature; DSA digital signature**] and cryptographic key sizes [**1024, 2048, 4096-bit**] that meet the following: [**ANSI X9.44 (RSA) (NIST certificate #388); FIPS 186-1 (DSA) (NIST certificate #298)**].

5.1.2.4 Cryptographic operation (FCS_COP.1b)

FCS_COP.1b.1 The TSF shall perform [**message hashing**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**not applicable**] that meet the following: [**FIPS 180-2 (NIST certificate #804)**].

5.1.2.5 Cryptographic operation (FCS_COP.1c)

FCS_COP.1c.1 The TSF shall perform [**hashed message authentication**] in accordance with a specified cryptographic algorithm [**HMAC**] and cryptographic key sizes [**not applicable**] that meet the following: [**FIPS 198 (NIST certificate # 446)**].

5.1.2.6 Cryptographic operation (FCS_COP.1c)

FCS_COP.1d.1 The TSF shall perform [**random number generation**] in accordance with a specified cryptographic algorithm [**FIPS 140-2 approved random number generator**] and cryptographic key sizes [**not applicable**] that meet the following: [**ANSI X9.31 (NIST certificate #464**].

5.1.2.7 Cryptographic operation (FCS_COP.1e)

FCS_COP.1e.1 The TSF shall perform [**encrypt and decrypt**] in accordance with a specified cryptographic algorithm [**AES CBC mode**] and cryptographic key sizes [**256 bits**] that meet the following: [**FIPS 197 (NIST certificate #806)**].

5.1.3 User data protection (FDP)

5.1.3.1 Simple information flow control (FDP_IFC.1a)

FDP_IFC.1a.1 The TSF shall enforce the [**Fixlet Information Flow SFP**] on [**subjects: user and managed machine (client); information: Fixlets; operations: apply Fixlet**].

5.1.3.2 Simple information flow control (FDP_IFC.1b)

FDP_IFC.1b.1 The TSF shall enforce the [**Action Information Flow SFP**] on [**subjects: user and managed machine (client); information: Actions; operations: apply Action].**

5.1.3.3 Simple security attributes (FDP_IFF.1a)

FDP_IFF.1a.1 The TSF shall enforce the [**Fixlet Information Flow SFP**] based on the following types of subject and information security attributes: [

subjects:

user (authorized operator or subscribed publisher)

certificate

managed machines (clients)

operators allowed to administer machine

external content sites machine is subscribed to

custom sites machine is subscribed to

information:

Fixlet definition].

FDP_IFF.1a.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) if the Fixlet digital signature can be verified and identifies an authorized operator or subscribed publisher AND

b) if the Fixlet originates from an operator authorized to administer the machine, or from the designated publisher of an external content site that the machine is subscribed to, or from an authorized publisher of a custom site that the machine is subscribed to, then the managed machine (client) applies the Fixlet].

FDP_IFF.1a.3 The TSF shall enforce the [**no additional information flow control SFP rules**].

FDP_IFF.1a.4 The TSF shall provide the following [**no additional capabilities**].

FDP_IFF.1a.5 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional access rules**].

FDP_IFF.1a.6 The TSF shall explicitly deny an information flow based on the following rules: [**no additional deny rules**].

5.1.3.4 Simple security attributes (FDP_IFF.1b)

FDP_IFF.1b.1 The TSF shall enforce the [**Action Information Flow SFP**] based on the following types of subject and information security attributes: [

subjects:

user (authorized operator)

certificate

managed machines (clients)

operators allowed to administer machine

computer identity

inspectable properties of machine

information:

Action definition].

FDP_IFF.1b.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) if the Action digital signature can be verified and identifies an authorized operator AND

b) if the action originates from an operator authorized to administer the machine, and the operator specified the machine as 'targeted' either by its computer identity or by its inspectable properties, then the managed machine (client) applies the Action].

FDP_IFF.1b.3 The TSF shall enforce the [**no additional information flow control SFP rules**].

FDP_IFF.1b.4 The TSF shall provide the following [**no additional capabilities**].

FDP_IFF.1b.5 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional access rules**].

FDP_IFF.1b.6 The TSF shall explicitly deny an information flow based on the following rules: [**no additional deny rules**].

5.1.4 Identification and authentication (FIA)

5.1.4.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user name, password, certificate, and role**].

5.1.4.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**available actions, except security management of the TOE and its target IT systems**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.3 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security management (FMT)

5.1.5.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behaviour of, disable, enable, modify the behaviour of***] the functions [**the functions indicated in the following table:**

User Privileges	Site Administrator	Master Operator	Operator
Create User	Yes	No	No
Set Minimum Refresh Interval	Yes	No	No
Set Default Visibility & Client UI Icon	Yes	No	No
Edit Masthead	Yes	No	No
Initialize Action Site	Yes	Yes	No
Manage Sites	Yes	Yes	No
Change BES Client heartbeats	Yes	Yes	No
Create, edit, delete Fixlets, Groups	Yes	Yes	Yes
Activate/Deactivate Analyses	Yes	Yes	Yes
Take Fixlet Action	Yes	Yes	Yes
Take Custom Action	Yes	Yes	Yes
Modify Actions	Yes	Yes	Yes
Manage Administrative Rights	Yes	Yes	No
Create/Modify Retrieved Properties	Yes	Yes	No
View Fixlets, Computers	Yes	Yes	Yes
View Groups	Yes	Yes	Yes
View Unmanaged Assets	Yes	Yes	Yes
View Actions	Yes	Yes	Yes
View/Make Comments	Yes	Yes	Yes
Globally Hide/Unhide	Yes	Yes	No
Locally Hide/Unhide	Yes	Yes	Yes
Use Wizards	Yes	Yes	Yes
Remove computer from database	Yes	Yes	Yes
Create/Delete Computer Groups	Yes	Yes	Yes
Modify Computer Groups	Yes	Yes	Yes
Create Custom Site	Yes	Yes	No
Modify Custom Site Owners	Yes	Yes	No
Modify Custom Site Readers/Writers	Yes	Yes	Yes

5.1.5.2 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1a.1 The TSF shall enforce the [**Action and Fixlet Information Flow Control SFPs**] to restrict the ability to [***modify, delete,* create**] the security attributes [**role, certificate**] to [**authorized Site Administrator**].

5.1.5.3 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1b.1 The TSF shall enforce the [**Fixlet Information Flow Control SFP**] to restrict the ability to [***modify, delete***] the security attributes [**allowed operators, external content subscription, custom site subscription**] to [**authorized Site Administrator and Master Operator**].

5.1.5.4 Management of security attributes (FMT_MSA.1c)

FMT_MSA.1c.1 The TSF shall enforce the [**Action Information Flow Control SFP**] to restrict the ability to [***modify, delete***] the security attributes [**allowed operator, machine (client) properties**] to [**authorized Site Administrator and Master Operator**].

5.1.5.5 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.5.6 Static attribute initialization (FMT_MSA.3a)

FMT_MSA.3a.1 The TSF shall enforce the [**Fixlet Information Flow Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3a.2 The TSF shall allow the [**authorized Site Administrator, Master Operator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.7 Static attribute initialization (FMT_MSA.3b)

FMT_MSA.3b.1 The TSF shall enforce the [**Action Information Flow Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3b.2 The TSF shall allow the [**authorized Site Administrator, Master Operator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.8 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[manage the information flow control SFP attributes, manage users and their attributes, and other operations indicated in the FMT_MOF.1 (above)**].

5.1.5.9 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**Site Administrator, Master Operator, Operator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure* and *modification***] when it is transmitted between separate parts of the TOE.

5.1.6.2 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are to be satisfied by the IT environment of BigFix Enterprise Suite (BES).

Requirement Class	Requirement Component
FPT: Protection of the TSF	FPT_SEP.1: TSF Domain Separation
	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Protection of the TSF (FPT)

5.2.1.1 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The ~~TSF~~ **IT environment** shall maintain a security domain for its own execution that protects it **and the TOE** from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ~~TSF~~ **IT environment** shall enforce separation between the security domains of subjects in the TSC.

5.2.1.2 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT environment** shall be able to provide reliable time stamps for its own **and TOE** use.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements (SARs) for the TOE are the EAL 3 components as specified in Part 3 of the CC. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3: Authorisation controls
	ACM_SCP.1: TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2: Security enforcing high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 3 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Authorisation controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.3.7c The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.3.8c The CM plan shall describe how the CM system is used.

ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.

ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

ACM_SCP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2d The developer shall use the delivery procedures.

ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1c The presentation of the high-level design shall be informal.

ADV_HLD.2.2c The high-level design shall be internally consistent.

ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.
ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.
ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.

AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security Audit

The TOE records the occurrence of security related events and records the details of those events including date, time, subject identity, and the outcome of the event. The audit information gathered by the TOE is accessible in the SQL database that stores all BES audit data. The TOE requires Microsoft's SQL Server or MSDE in the IT environment as the database for maintaining the information flow control policies and associated security attributes.

The TOE audits the creation of authorized subjects. The subjects ID, name, role (permission level), and creation time are recorded in the SQL database. This audit data is stored in the USERINFO table of the database.

The TOE audits every action by authorized subjects. When an action is initiated the following information is recorded for the action: the name of the action, the date and time the action was initiated, the subject identity that created the action, the outcome of the action (success and failure), the date and time when the outcome was recorded, and the current state of the action if it is has been initiated but not yet completed. The audit data also includes non-security details such as the BES Site associated with the action. This audit data is stored in the ACTIONRESULTS table of the SQL database in the IT environment.

The TOE is operational when SQL auditing is turned on. The start-up and shutdown of the SQL Database is recorded in the Operating Systems' application Event Log.

Event	Audited
Create User	Yes
Set Minimum Refresh Interval	Yes
Set Default Visibility & Client UI Icon	Yes
Edit Masthead	Yes
Initialize Action Site	Yes
Manage Sites	Yes
Change BES Client heartbeats	Yes
Create, edit, delete Fixlets, Groups	Yes
Activate/Deactivate Analyses	Yes
Take Fixlet Action	Yes
Take Custom Action	Yes
Modify Actions	Yes
Manage Administrative Rights	Yes
Create/Modify Retrieved Properties	Yes
View Fixlets, Computers	Yes
View Groups	Yes
View Unmanaged Assets	Yes
View Actions	Yes
View/Make Comments	Yes
Globally Hide/Unhide	Yes

Locally Hide/Unhide	Yes
Remove computer from database	Yes
Create/Delete Computer Groups	Yes
Modify Computer Groups	Yes
Create Custom Site	Yes
Modify Custom Site Owners	Yes
Modify Custom Site Readers/Writers	Yes

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1

6.1.2 Cryptographic support

The TOE uses cryptography in general to ensure that it only performs corrective actions on targeted systems in the IT environment that an administrator of an instance of the TOE initiates. The TOE uses the FIPS 140-2 Level 2 certified BigFix Cryptographic Module 1.0 (based on OpenSSL) to perform all cryptographic operations. The Module has been awarded the following algorithm certificates from NIST: AES #806, SHA #804, RNG #464, RSA #388, HMAC #466. The Module itself has been awarded certificate #1080 from NIST.

During installation of the BES server, an asymmetric key pair is generated (as part of the site's Masthead). The installation application then creates a certificate request using the newly-generated keys. The administrator must then follow manual procedures that are described in the guidance to send the certificate request to BigFix. BigFix provides a CA service that it requires its customers to use according to the TOE software's license agreement. The BigFix generates a certificate using the certificate request from the new TOE installation and then it is returned to the customer using the manual procedures that are described in the guidance. The administrator must then import the certificate using the installation application for subsequent use by the TOE. This certificate is called the "site certificate". The corresponding key pair is called the "site credentials". The private key is stored encrypted on the local disk using a password that an administrator enters which is turned into a symmetric key to encrypt the site credentials' private key. Note that since this key is stored within the otherwise protected BES server where even its encrypted form should be inaccessible by untrusted users, no specific security functional requirements have been defined in this ST for the conversion of a password to a key or the use of that key encryption key. The information here is presented only for completeness.

After a site certificate is generated, copies of the certificate (along with the BixFix CA root certificate) are installed on targeted IT systems along with BES client application software. When a corrective action on a targeted system is initiated by an administrator, the request message that is sent from the BES server to the BES client is hashed using SHA-1, the hash is encrypted using an RSA digital signature algorithm, and the result is included with the message serving in effect as a signature to ensure both authenticity and integrity of the message. When a Fixlet or Action is received by the BES client, it attempts to build and verify a certificate path using the configured site certificate. If the BES client can build and validate a path, if the signature verification is successful (i.e. if the request message has not been modified based on the decrypted hash), and the signature identifies an authorized operator, the BES client accepts the request and performs the requested action.

Note that when new administrators are created by the single BES Site Administrator, the BES server as part of creating the administrator account with username and password, also generates a keypair and certificate for the new administrator. When the Master Operator or other Operators subsequently initiate corrective actions, those request messages that are sent are signed using that particular administrator's private key. The BES client then builds and verifies a path using the BigFix CA certificate, the BES server installation certificate (i.e. the site certificate), and the individual administrator's certificate.

After installation of the BES server an administrator can create key pairs that are used solely for encryption of Client data. Once the key pairs are created the administrator can specify that all Clients or a subset of Clients should encrypt data using the public key before that data is transmitted back to the Server over the network. The private key is stored on the Server or optionally on Relays that have been designated by the administrator to perform reencryption. The Server automatically distributes the public keys once they have been created and once the Clients have been instructed to encrypt audit data. The administrator can create new key pairs at any time. When a new key pair is created it is automatically distributed to all previously designated Clients. These public keys are distributed to the Clients in the digitally signed Masthead.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: The TOE provides the ability to generate site keys as well as administrator keys. The TOE does not provide the ability to destroy either site or administrator credentials. RSA key generation is performed by vendor assertion.
- FCS_CKM.4: The TOE performs key destruction in accordance with the FIPS 140-2 standard.
- FCS_COP.1a through e: The TOE can generate site keys as well as administrator keys. The TOE can also sign administrator certificates. The TOE can verify both site and administrator certificate signatures. The TOE can also sign and verify corrective action request messages. RSA digital signature is performed by vendor assertion. The TOE hashes messages using SHA-1, as specified in FIPS 180-2, in order to ensure their integrity. The TOE also performs random number generation to support key generation, and AES encryption and decryption functions, all of which are certified under FIPS 140-2.

6.1.3 User data protection

The TOE provides two Information Flow Control Security Function Policies (SFPs), Fixlet and Action (hereinafter referred to as Fixlet SFP and Action SFP), that control the ability to apply Fixlets and Actions to Clients. The TOE has the ability to control actions reflected in the applicable Information Flow Control SFP based on rule creation.

The Fixlet SFP is based on the list of authorized subjects (operators allowed to administer machine, external content sites machine is subscribed to, custom sites machine is subscribed to), their corresponding public certificates, and the (signed) Fixlet definition. The Fixlet SFP only permits a Fixlet to be accepted and applied on a targeted Client if the Fixlet originates from an operator authorized to administer the machine, or from the designated publisher of an external content site that the machine is subscribed to, or from an authorized publisher of a custom site that the machine is subscribed to. The managed machine (client) applies Fixlets if and only they are digitally signed by an authorized operator or publisher and the signature can be verified.

The Action SFP is based on the list subject of authorized subjects (operators allowed to administer machine), their corresponding public certificates, target machine attributes (computer identity and inspectable properties), and the (signed) Action definition. The Action SFP only permits an Action to be accepted and applied on a targeted Client if the Action originates from an operator authorized to administer the machine and the operator specified the machine as ‘targeted’ either by its computer identity or by its inspectable properties. The managed machine (client) applies Actions if and only if they are digitally signed by an authorized operator and the signature can be verified.

Each client is initially installed with the masthead (containing the site public key) of the associated BES server. The server provides the client the list of authorized operators and publishers, each of which is identified by a public certificate signed by the server’s certificate (verified by the site public key) so the client can be assured the list is authentic. Subsequently, the client will essentially accept instructions (Fixlets and Actions) only if they are digitally signed, the digital signature can be verified, and the signature represents an operator or publisher authorized to perform the indicated function.

The Server coordinates the flow of information to and from individual computers (Clients) and stores the results in the BES database. Server components operate quietly in the background without any direct intervention from an administrator. The TOE requires Microsoft’s SQL Server or MSDE in the IT environment as the database for maintaining the information flow control policies and associated security attributes.

The information flow control policies are applicable to all Fixlets and Actions and managed client machines in the network.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1a,b: The TOE provides Fixlet and Action information flow policy between users and managed machines by information (i.e., Fixlet or Action) definition and all operations.
- FDP_IFF.1a,b: The TOE provides a Fixlet SFP and Action SFP that have flexible rules based upon the attributes defined in the SFR.

6.1.4 Identification and authentication

The TOE provides web- and application-based GUI interfaces that administrators can access using a valid username and password. In order to access any security management functions of the TOE using either type of administrator console interface, a username and password must be created for the administrator, and the administrator must be assigned to an administrative role. The TOE provides its own username/password authentication mechanism.

The Site Administrator logs into the server Administrative Tool via a GUI (on the same host as the BES server) to create user accounts for human users (Master Operators and Operators), set minimum refresh rates, set default visibility, edit and manage the Masthead, and initialize the Action site. Master Operators and Operators log into the console component to view and manage the entire network via ODBC requests to the BES database and HTTP connections to the server.

Clients and Relays are uniquely identified within the network by a unique identifier assigned by the Server during registration.

The TOE maintains the user name, password, certificate, and role security attributes to enforce I&A.

Users must be successfully identified and authenticated before access to TOE data and resources is allowed. Passwords must be a minimum of six characters long.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: For each user account, the TOE keeps at least the following information: user name, password, certificate, and role.
- FIA_UAU.1: The user is required to be successfully authenticated in order to perform any security management related function.
- FIA_UID.2: The user is required to be successfully identified before any actions are allowed. Each TOE component is also identified based on network address or unique identified assigned within the TOE.

6.1.5 Security management

The TOE provides security management functions that can only be accessed by authorized administrators. For example, only Site Administrators can create user accounts and assign Master Operator or Operator roles to users. There are certain management functions that can only be done by a Site Administrator and as day-to-day management of the enterprise (managed client machines) is accomplished by either Master Operator or Operator. The TOE ensures that only secure values are accepted for secure security attributes for digital signing and verification of secrets and these are enforced by the Fixlet and Action Information Flow Control SFPs in which only a designated Site Administrator or Master Operator have the ability to change initial values based on their role.

The Site Administrators and/or Master Operators use the Administrator Tool to create user accounts, manage the minimum refresh rates, and for Masthead management; and the Console component is used to view and manage the entire network and allows automated distribution of fixes (e.g., Fixlets), software deployment, vulnerability analysis (i.e., systems requiring patches, updated service packs, configuration violations and/or enterprise security policy violations) in order to remediate from a central location. Each Console operator (e.g., authorized user) can make ODBC requests to the BES database and HTTP connections to the Server.

Console users (i.e., operators or publishers) can be in charge of flexibly defined groups of computers with varying degrees of freedom. The authorized Site Administrator has overall control of each operator’s domain and the specific rights they have over that domain. The TOE support three classes of users: Site Administrator’s, Master Operators and ordinary Operators. Each of these user roles has different responsibilities and restrictions as follows:

- Site Administrator: This role/user creates a set of keys that grants TOE administrator privileges as well as Master Operator privileges. Although a Site Administrator can do everything a Master Operator can do, it is recommended that for day-to-day operation, the Master Operator role be used. The Site Administrator role should be reserved to perform top-level management tasks including: creating users with the TOE Administration Tool; setting the minimum refresh for the TOE through the administration tool; and, editing Mastheads.
- Master Operator: While ordinary Operators are allowed to deploy actions and edit certain properties, the Master Operator can also:
  - Edit the management rights settings for other operators, thus allowing the Master Operator to divide up the computers on the network among various operators so they each see a smaller subset of Client computers;
  - Create new computer settings that allow Clients to hold various labeled values that can be queried, sorted and filtered. Settings are also used to group computers, thus allowing the assignment of Clients to different groups for easier searching and reporting;
  - Create or edit retrieved properties, which are used to filter and sort computers and can be used to create reports and help with inventory audits;
  - Change the Client heartbeat to optimize TOE performance; and,
  - Subscribe or unsubscribe from Fixlet site.
- Operators: Operators manage the day-to-day operation of the TOE, including Fixlet management and action deployment, subject to the management rights assigned by a BES Site Administrator or Master Operator.

The following table summarizes the privileges and abilities of each type of authorized user for the TOE. Any cell not marked 'No' or 'Yes' is subject to additional restrictions and generally can be performed where they affect only the resources (e.g., a site) assigned to the Operator; 'All' indicates that the operation can be performed on all applicable targets (e.g., Analysis). This is a primary difference between the Master Operator that can perform many operations without restrictions where ordinary Operators are restricted in the scope of their functions:

User Privileges	Site Administrator	Master Operator	Operator
Create User	Yes	No	No
Set Minimum Refresh Interval	Yes	No	No
Set Default Visibility & Client UI Icon	Yes	No	No
Edit Masthead	Yes	No	No
Initialize Action Site	Yes	Yes	No
Manage Sites	Yes	Yes	No
Change BES Client heartbeats	Yes	Yes	No
Create, edit, delete Fixlets, Groups	Yes	Yes	Private/Custom Site Writer
Activate/Deactivate Analyses	Yes	All	Global and Private
Take Fixlet Action	Yes	Yes	Administered
Take Custom Action	Yes	Yes	Administered
Modify Actions	Yes	All	Private
Manage Administrative Rights	Yes	Yes	No
Create/Modify Retrieved Properties	Yes	Yes	No
View Fixlets, Computers	Yes	All	Global / Custom Site Reader
View Groups	Yes	All	Administered
View Unmanaged Assets	Yes	All	Controlled by BESAdmin
View Actions	Yes	All	Global and Private
View/Make Comments	Yes	All	All Visible
Globally Hide/Unhide	Yes	Yes	No
Locally Hide/Unhide	Yes	Yes	Yes

Use Wizards	Yes	Yes	Yes
Remove computer from database	Yes	All	Administered
Create/Delete Computer Groups	Yes	Yes	Yes
Modify Computer Groups	Yes	Yes	Yes
Create Custom Site	Yes	Yes	No
Modify Custom Site Owners	Yes	Yes	No
Modify Custom Site Readers/Writers	Yes	Yes	Site Owners

Table 4 User Privileges

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: Only authorized administrators can determine the behavior of, disable, enable or modify the behavior of the TOE as reflected in the table above.
- FMT_MSA.1a: Only the Site Administrator can modify, delete, and create roles and certificates for Fixlet and Action SFPs.
- FMT_MSA.1b: Only an authorized Site Administrator or Master Operator can modify and delete allowed operators, external content subscription and custom site subscription of the Fixlet SFP.
- FMT_MSA.1c: Only an authorized Site Administrator or Master Operator can modify, delete allowed operator, client machine properties of the Action SFP.
- FMT_MSA.2: Only secure values are accepted for security attributes.
- FMT_MSA.3a: Each user has a restrictive Fixlet SFP policy defined by default but the Site Administrator or Master Operator can override this with a more permissive policy.
- FMT_MSA.3b: Each user has a restrictive Action SFP policy defined by default but the Site Administrator or Master Operator can override this with a more permissive policy.
- FMT_SMF.1: The TOE offers a wide range of management functions including the ability to manage security attributes, audit data and security functions.
- FMT_SMR.1: The TOE supports the roles of Site Administrator, Master Operator and Operator and when a users log in the account is associated with the role.

6.1.6 Protection of the TSF

The TOE provides the capability to detect modification of Fixlets and Actions during transmission between TOE components. The Fixlet or Action must be digitally signed by an authorized operator or publisher. If the client cannot verify the signature, the Fixlet/Action is not applied. This ensures that the TOE will not apply Fixlets/Actions on behalf of unauthorized users.

The TOE also requires administrators to log in before they can access security management functions and even then the set of functions they can perform are limited based on their role.

Furthermore, all communication channels between TOE components are configured to use SSL, via OpenSSL, to ensure that all sensitive data is protected from disclosure and potential modification (or insertion).

Note that the IT environment is relied upon to maintain a security domain for its own (including the BES database and hosting operating systems and hardware) execution as well as protection of the TOE from interference and tampering by untrusted subjects. Both, the TOE and the underlying operating system operate in their own space.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The TOE uses SSL to protect the security and integrity of all sensitive (or TSF) data sent between the TOE components.
- FPT_RVM.1: There is no means to bypass the TOE's security policies.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by BigFix ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. BigFix ensures changes to the implementation representation are controlled. BigFix performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- BigFix BES Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 3 assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Delivery and operation

BigFix provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. BigFix's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. BigFix also provides documentation that describes the steps necessary to install BigFix Enterprise Suite (BES) in accordance with the evaluated configuration.

These activities are documented in:

- BigFix BES Delivery, Installation, Generation and Start-up Procedures

The Delivery and operation assurance measure satisfies the following EAL 3 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

BigFix has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- BigFix BES Design Document

The Development assurance measure satisfies the following EAL 3 assurance requirements:

- ADV_FSP.1
- ADV_HLD.2

- ADV_RCR.1

6.2.4 Guidance documents

BigFix provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- BigFix BES Administrator Guide
- BigFix BES Console Operator Guide

The Guidance documents assurance measure satisfies the following EAL 3 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

BigFix applies security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure development of the TOE.

These activities are documented in:

- BigFix BES Life Cycle Plan

The Life cycle support assurance measure satisfies the following EAL 3 assurance requirements:

- ALC_DVS.1

6.2.6 Tests

BigFix has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. BigFix has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- BigFix BES Test Plan
- BigFix BES Test Results

The Tests assurance measure satisfies the following EAL 3 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of BigFix Enterprise Suite (BES) and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references.

BigFix has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, Basic.

BigFix performs regular vulnerability analyses of the entire TOE (including documentation) to identify obvious weaknesses that can be exploited in the TOE.

These activities are documented in:

- BigFix BES Vulnerability Analysis
- BigFix BES Administrator Guide
- BigFix BES Console Operator Guide

The Vulnerability assessment assurance measure satisfies the following EAL 3 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

This ST does not claim conformance to any Protection Profile.

8. Rationale

This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence how threats to the TOE and intended usage assumptions are countered by the security objectives.

	T.MANAGE	T.NOAUTH	T.SECURE	A.BENIGN	A.FIXES	A.NOEVIL	A.PHYSEC
O.AUDIT			X				
O.DIGSIG			X				
O.I&A		X	X				
O.MANAGE	X	X					
O.MEDIATE		X	X				
OE.DOMSEP	X	X	X				
OE.FIXES					X		
OE.GUIDAN						X	
OE.NOEVIL				X		X	
OE.PHYSEC							X
OE.USERS				X			

Table 5 Environment to Objective Correspondence

8.1.1.1 T.MANAGE

An enterprise network might be mismanaged due to a lack of centralized security management control.

This Threat is satisfied by ensuring that:

- O.MANAGE: The TOE must provide effective means of security management for itself as well as targeted IT environment machines.
- OE.DOMSEP: The IT environment ensures that the TOE and itself are appropriately protected from tampering that might allow the TOE security functions to be subverted.

8.1.1.2 T.NOAUTH

An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions provided by the TOE, which may go undetected.

This Threat is satisfied by ensuring that:

- O.AUDIT: The TOE must generate audit records for the security management functions of the TOE.
- O.I&A: The TOE must successfully identify and authenticate users before granting a user access to protected TOE security functions to prevent potential unauthorized access to functions.
- O.MANAGE: The TOE must provide effective means of security management for itself as well as targeted IT environment machines.
- O.MEDIATE: The TOE must ensure that it applies only the instructions of authorized administrators on target IT environment machines.
- OE.DOMSEP: The IT environment ensures that the TOE and itself are appropriat4elty protected from tampering that might allow the TOE security functions to be subverted.

8.1.1.3 T.SECURE

An enterprise network might be subject to an undetected attack by attackers attempting to issue unauthorized security management instructions.

This Threat is satisfied by ensuring that:

- O.AUDIT: TOE must generate audit records for the security management functions of the TOE.
- O.DIGSIG: The TOE provides digital signing and verification for users to authenticate and ensure the integrity of Fixlets and Actions on behalf of that user.
- O.I&A: The TOE must successfully identify and authenticate users before granting a user access to protected TOE security functions to prevent potential unauthorized use of the corresponding functions.
- O.MEDIATE: The TOE must ensure that it applies only the instructions of authorized administrators on target IT environment machines.
- OE.DOMSEP: The IT environment ensures that the TOE and itself are appropriat4elty protected from tampering that might allow the TOE security functions to be subverted.

8.1.1.4 A.BENIGN

The users of the computers hosting the TOE components are willing participants that benefit from the security functions of the TOE and will not willfully attempt to circumvent any TOE security functions.

This Assumption is satisfied by ensuring that:

- OE.NOEVIL: Only administrators that are non-hostile and will follow applicable administrator guidance will be assigned to manage the TOE and IT environment targets. This reinforces that even administrators are users and will serve in a manner that would not willfully cause the TOE security functions to be subverted.
- OE.USERS: Each enterprise user will be expected to not willfully take any action to subvert the security functions of the TOE. This directly corresponds to the stated assumption.

8.1.1.5 A.FIXES

The 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.

This Assumption is satisfied by ensuring that:

- OE.FIXES: The issues of Fixlets and Actions will ensure that they are correctly designed and tested to perform their expected functions. This directly corresponds to the stated objective.

8.1.1.6 A.NOEVIL

Authorized administrators are non-hostile and adhere to all applicable administrator guidance.

This Assumption is satisfied by ensuring that:

- OE.GUIDAN: The TOE will be delivered, installed, administered, and operated in a manner that maintains security. This reinforces OE.NOEVIL in that guidance is expected to be followed during the lifecycle of the product.
- OE.NOEVIL: Only administrators that are non-hostile and will follow applicable administrator guidance will be assigned to manage the TOE and IT environment targets. This directly corresponds to the stated assumption.

8.1.1.7 A.PHYSEC

The computers hosting the TOE components and the TOE's database are physically secure to a degree appropriate to protect the TOE as well as themselves.

This Assumption is satisfied by ensuring that:

- OE.PHYSEC: The computers hosting the TOE and its database will be physically secure to an appropriate degree. While more general, the objective directly corresponds to the stated assumption.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the ST.

8.2.1 Security Functional Requirements Rationale

All SFRs identified in this ST are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy. The following table indicates the requirements that effectively satisfy the individual objectives.

	O.AUDIT	**O.DIGSIG**	**O.I&A**	**O.MANAGE**	**O.MEDIATE**	**OE.DOMSEP**
TOE						
FAU_GEN.1	X					
FCS_CKM.1		X				
FCS_CKM.4		X				
FCS_COP.1(a-e)		X				
FDP_IFC.1(a-b)		X			X	
FDP_IFF.1(a-b)		X			X	
FIA_ATD.1			X			
FIA_UAU.1			X	X		
FIA_UID.2			X			
FMT_MOF.1				X		
FMT_MSA.1(a-c)				X	X	
FMT_MSA.2				X		
FMT_MSA.3(a-b)				X	X	
FMT_SMF.1				X		
FMT_SMR.1				X		

	O.AUDIT	O.DIGSIG	O.I&A	O.MANAGE	O.MEDIATE	OE.DOMSEP
FPT_ITT.1				X	X	
FPT_RVM.1				X	X	
IT Environment						
FPT_SEP.1						X
FPT_STM.1	X					

Table 6 Objective to Requirement Correspondence

8.2.1.1 O.AUDIT

The TOE must generate audit records for the security management functions of the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE generates audit records for the security management functions of the TOE.
- FPT_STM.1: The IT Environment supports the generation of audit records by providing reliable timestamps.

8.2.1.2 O.DIGSIG

The TOE must provide digital signing and verification of signature for administrators and other publishers to authenticate Fixlets or Actions on behalf of that issuer.

This TOE Security Objective is satisfied by ensuring that:

- FCS_CKM.1: The TOE is required to generate cryptographic key pairs for signature generation and verification.
- FCS_CKM.4: The TOE is capable of destroying key pairs as required by FIPS 140-2.
- FCS_COP.1(a-e): The TOE is required to use SHA-1 to hash the contents of Fixlets and Actions and then to use a RSA digital signature algorithm to asymmetrically encrypt the result in order to digitial sign Fixlets and Actions so their authenticity and integrity can be ensured.
- FDP_IFC.1(a-b): The TOE is required to provide digital signature verification of signature for information flowing through the TOE..
- FDP_IFF.1(a-b): The TOE is required to enforce digital signature verification to support information flow rules established by an authorized user.

8.2.1.3 O.I&A

The TOE must successfully identify and authenticate users before granting access to protected TOE security functions.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE is required to maintain security attributes for users.
- FIA_UAU.1: The TOE is required to authenticate users before allowing any TSF-mediated actions.
- FIA_UID.2: The TOE is required to identify users before allowing any TSF-mediated actions.

8.2.1.4 O.MANAGE

The TOE must provide the means to effectively manage the TOE security functions as well as target machines in the IT environment and ensure those functions are available only to authorized administrators.

This TOE Security Objective is satisfied by ensuring that:

- FIA_UAU.1: The TOE is required to authenticate users, particularly administrators, before allowing any TSF-mediated actions.
- FMT_MOF.1: The TOE is required to determine the behavior of, disable, enable, and modify security functions to authorized users by role and privilege.
- FMT_MSA.1(a-c): The TOE is required to restrict access to security attributes appropriately.
- FMT_MSA.2: The TOE is required ensure only secure values are accepted for security attributes.
- FMT_MSA.3(a-b): The TOE is required to enforce the information flow control SFPs to provide restrictive access to authorized users.
- FMT_SMF.1: The TOE is required to offer the functions necessary for effective management of the TOE security functions as well as the targeted IT environment machines.
- FMT_SMR.1: The TOE is required to define authorized administrators that will be able to perform the applicable security management functions.
- FPT_ITT.1: The TOE is required to protect communications between TOE components so that instructions cannot be corrupted, modified, or observed (where access to sensitive information might allow a potential attacker to identify a weakness).
- FPT_RVM.1: The TOE is required to ensure that its functions cannot be bypassed.

8.2.1.5 O.MEDIATE

The TOE must ensure that only authorized instructions are applied to target machines in the IT environment.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.1(a-b): The TOE is required to mediate information flowing through the TOE.
- FDP_IFF.1(a-b): The TOE is required to enforce information flow rules established by an authorized user.
- FMT_MSA.1(a-c): The TOE is required to restrict access to security attributes appropriately.
- FMT_MSA.3(a-b): The TOE is required to ensure appropriate default information flow settings and restrict access to change those settings appropriately.
- FPT_ITT.1: The TOE is required to protect the integrity of sensitive data sent between TOE components.
- FPT_RVM.1: The TOE is required to ensure that its functions cannot be bypassed.

8.2.1.6 OE.DOMSEP

The IT environment must provide domain separation that protects the TOE from interference and tampering by untrusted subjects.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_SEP.1: The IT environment is required to protect the TOE from tampering.

8.3 Security Assurance Requirements Rationale

EAL3 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats and assumptions defined for the environment. At EAL3, the BES will have incurred a search for obvious flaws to support its introduction into a non-hostile environment.

8.4 Strength of Functions Rationale

The TOE minimum strength of function is SOF-Basic. The evaluated TOE is intended to operate in commercial and Department of Defense low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in Section 4. Further, SOF-Basic was chosen to address the permutational mechanisms provided by the I&A mechanisms of the TOE (i.e., FIA_UAU.1).

8.5 Requirement Dependency Rationale

The following table reflects the CC-required dependencies being satisfied in this ST where the following pertains to the conventions used in column 3 (ST Dependencies):

- ***Italicized text*** – required dependency is being satisfied within the IT environment.
- Underlined text – required dependency is being satisfied by an assurance requirement.
- Normal text – the dependency is satisfied by the TOE.
- [Red text in brackets] – indicates a dependency that is not directly satisfied

ST Requirement	CC Dependencies	ST Dependencies
TOE SFRs		
FAU_GEN.1	FPT_STM.1	*FPT_STM.1*
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4 and FMT_MSA.2	FCS_COP.1a and FCS_CKM.4 and FMT_MSA.2
FCS_CKM.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FMT_MSA.2	FCS_CKM.1 and FMT_MSA.2
FCS_COP.1a	(FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	FCS_CKM.1 and FCS_CKM.4 and FMT_MSA.2
FCS_COP.1b	(FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	Note that while FCS_CKM.1 and FMT_MSA.2 are included, SHA-1, as required by FCS_COP.1b, does not use keys or any other data entered by an administrator; hence, the dependencies are irrelevant.
FCS_COP.1c		
FCS_COP.1d		
FCS_COP.1e		
FDP_IFC.1a	FDP_IFF.1	FDP_IFF.1a
FDP_IFC.1b	FDP_IFF.1	FDP_IFF.1b
FDP_IFF.1a	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1a and FMT_MSA.3
FDP_IFF.1b	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1b and FMT_MSA.3
FIA_ATD.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1(a, b)	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.1a
FMT_MSA.1(a, c)	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_IFC.1b
FMT_MSA.2	ADV_SPM.1 and FMT_MSA.1 and FMT_SMR.1 and (FDP_ACC.1 or FDP_IFC.1)	[ADV_SPM.1] and FMT_MSA.1 and FMT_SMR.1 and FDP_IFC.1(a-b)
FMT_MSA.3a	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1(a, b) and FMT_SMR.1
FMT_MSA.3b	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1(a, c, d) and FMT_SMR.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_ITT.1	none	none
FPT_RVM.1	none	none
IT ENV SFRs		
FPT_SEP.1	none	none
FPT_STM.1	none	none
TOE SARs		
ACM_CAP.3	ALC_DVS.1	ALC_DVS.1

ST Requirement	CC Dependencies	ST Dependencies
ACM_SCP.1	ACM_CAP.3	ACM_CAP.3
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_DVS.1	none	none
ATE_COV.2	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_DPT.1	ADV_HLD.1 and ATE_FUN.1	ADV_HLD.2 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_MSU.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.2
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.2 and AGD_ADM.1 and AGD_USR.1

Table 7 Security Requirement Dependencies

The TOE contains FCS_CKM.1 to address the TOE's capability to generate a public/private key pair to provide digital signing and signature verification of all authorized users completing security relevant actions on the TOE. These keys are generated by the TOE per Sections 5.1.2.1 and 6.1.2.

The required CC-dependency of ADV_SPM.1 (Informal TOE security policy model) of FMT_MSA.2 (Secure security attributes) is not required as the contents of this ST serves as an informal TOE security policy model sufficient for the purpose of this dependency.

8.6 Explicitly Stated Requirements Rationale

This ST does not contain any explicitly stated requirements.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. The following table demonstrates the relationship between security requirements and security functions.

	Security Audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF
FAU_GEN.1	X					
FCS_CKM.1		X				
FCS_CKM.4		X				
FCS_COP.1(a-e)		X				
FDP_IFC.1(a-b)			X			
FDP_IFF.1(a-b)			X			
FIA_ATD.1				X		
FIA_UAU.1				X		
FIA_UID.2				X		
FMT_MOF.1					X	
FMT_MSA.1(a-c)					X	
FMT_MSA.2					X	
FMT_MSA.3(a-b)					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_ITT.1						X
FPT_RVM.1						X

Table 8 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.