HCL BigFix Server Version 11.0.3 Common Criteria Configuration Guide

Version 1.0

2025-02-07

NIAP VID 11481

Prepared for:
HCL Technologies Limited
Via Pio Emanuelli, 1
Rome, Italy

Prepared by:
atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759

© 2025 HCL Technologies Ltd. All rights reserved.

Revision History

Version	Date	Author	Description
1.0	2025-02-07	atsec	First version

Trademarks

BigFix and its logo are registered trademarks of HCL Technologies Limited.

Windows and SQL server are registered trademarks of Microsoft Corporation.

OpenSSL is a registered trademark of OpenSSL Software Foundation.

© 2025 HCL Technologies Ltd. All rights reserved.

Table of Contents

© 2025 HCL Technologies Ltd. All rights reserved.

List of Figures

List of Tables

© 2025 HCL Technologies Ltd. All rights reserved.

1 Introduction

1.1 Document Purpose and Scope

This document serves as the administrative guidance for HCL BigFix Server version 11.0.3 under Common Criteria evaluation, conforming to the following Protection Profiles and Functional Packages:

- Protection Profile for Application Software v1.4 (pp_app_v1.4).
- Functional Package for Transport Layer Security v1.1 (pkg_tls_v1.1).

This document provides the preparative procedure and operational user guidance that are required for the Common Criteria evaluated configuration. This document describes how to install, configure, and operate HCL BigFix Server in the Common Criteria compliant manner.

This document supplements BigFix platform documentation available at https://help.hcltechsw.com/bigfix/11.0/platform/Platform_pdfguides.html

In case of inconsistency between this document and other guides, this document takes precedence.

1.2 Target of Evaluation

The Target of Evaluation (TOE) is HCL BigFix Server version 11.0.3.82, where 11.0.3 is the version number and 82 is the build number. The TOE is referred to as HCL BigFix Server version 11.0.3 in this document. The TOE is an application software that is part of HCL BigFix endpoint management platform, which automates the discovery, management, and remediation of endpoint systems.

HCL BigFix endpoint management platform is comprised of the following main components:

- BigFix Server (a.k.a. Server), the TOE.
- BigFix Administration Tool (a.k.a. Admin Tool).
- BigFix Console (a.k.a. Console).
- BigFix IEM Command-Line Interface (a.k.a. IEM CLI).
- BigFix Client (a.k.a. Client or Agent).
- BigFix Relay (a.k.a. Relay).

The TOE is the backbone of the platform, acting as a centralized source of endpoint management. The TOE collects contents from external Internet sites (i.e., HCL Fixlet servers and software vendor sites) and then redistributes the contents to the BigFix Clients directly (or through BigFix Relays). In the evaluated configuration, the TOE is administered through the Console over the network and the Administration Tool on the same computer hosting the TOE.

The content is delivered in messages that are called Fixlets. The BigFix Client runs on each endpoint system. The BigFix platform maintains real-time visibility and control over all the endpoint systems from the BigFix Console.

1.3 Operational Environment

The TOE is deployed on a single server physical machine. The required hardware platform resources depend on the number of endpoint computers that are to be managed by the TOE. The hardware platform used during the evaluation is a Dell PowerEdge R430 with Intel Broadwell Xeon E5-2620 v4 processor.

The TOE runs as a service on Microsoft Windows operating system. The TOE uses Microsoft SQL Server database to store and retrieve applicable data. In the evaluated configuration, the TOE runs on Microsoft Windows Server 2019 Standard version 1809; and Microsoft SQL Server 2019 database system is installed on the same machine as the TOE.

Besides the ordinary hardware resources used by applications (e.g., CPUs, memory, etc.), the TOE restricts its access to the network connectivity of hardware platform. The TOE uses network connectivity to communicate with other BigFix platform components (e.g., BigFix Clients) and certain Internet servers (e.g., Fixlet Servers).

The TOE restricts its access to the following sensitive information repositories:

- Windows Registry: for storing configuration options that are related to the security functionality.
- MSSQL Database: for storing Console Operator user account information, including the username and the password conditioned with the PBKDF2 function.

1.4 Evaluated Configuration

In the evaluated configuration, the BigFix platform includes the TOE and the following BigFix platform components:

- BigFix Administration Tool 11.0.3 (in the same machine where the TOE runs).
- BigFix Console 11.0.3.
- BigFix IEM CLI 11.0.3.
- BigFix Client 11.0.3.

The following restrictions apply to the Common Criteria evaluated configuration:

- BigFix Relays cannot be used as part of the BigFix platform.
- Disaster Server Architecture (DSA) cannot be used as part of the BigFix platform.
- The MSSQL database cannot run in a separate machine; it must be installed in the same machine where the TOE is installed.
- Authentication using the following mechanisms is not allowed:
  - External LDAP Server
  - Active Directory
  - SAML v2.0
- The following BigFix features are not allowed:
  - BigFix Web Reports
  - BigFix WebUI
  - BigFix Explorer Guide
  - BigFix Asset Discovery

Additionally, the TOE must be configured with the following constraints to work in the Common Criteria evaluated configuration:

- The TOE must be configured to use HTTPS to gather and download information from external sites (i.e., Fixlet servers and vendor sites).

- The TOE must be configured to use HTTPS to communicate with BigFix Clients.
- The TOE must be configured to use “FIPS mode”.
- The TOE must be configured to use OCSP Stapling and OCSP to check the revocation status of external sites' certificates.
- The Microsoft Control Flow Guard (CFG) security feature must be enabled on the Windows platform hosting the TOE.
- The network port for the WebUI interface must be disabled.
- FTP must be disabled.
- SSH must be disabled.

1.5 Assumptions

The administrators and users will ensure the security of the hardware and software platforms providing the runtime environment for the TOE. The underlying platforms are assumed to be trustworthy, to be supplied with a reliable time clock, and to be protected against unauthorized physical access and modification.

The administrators will ensure that users are aware of the security policies and procedures of their organization, and are trained and competent to operate the TOE in accordance with those policies and procedures.

The organization will ensure that administrators are aware of the security policies and procedures of their organization, and are trained and competent to administer the TOE in accordance with those policies and procedures.

2 Installation

2.1 Downloading

The TOE installation package can be downloaded from BigFix Enterprise Suite Download Center website via the HTTPS protocol: https://support.bigfix.com/bes/release/11.0/patch3/

The TOE installation package is distributed as an InstallShield installation package in EXE format. The installation package, as well as the binaries of the TOE, are signed by HCL America Inc. using Microsoft Authenticode, with RSA and SHA2-256 as the algorithms that are part of the digital signature generation.

From the same website, you can download the installation packages of other BigFix platform components, such as BigFix Console, and a set of utility software for maintaining the BigFix platform.

The HTTPS connection guarantees the authenticity of the download website. The website provides SHA-1 and SHA2-256 hash values of files for users to verify correct downloads.

2.2 Installation Preparations

Before starting the TOE installation, make sure that you read the following subsections and perform the preparation steps if needed.

2.2.1 License

HCL BigFix products require a license key to function. Your license is composed of two files:

- Public key file: license.crt.
- Private key file: license.pvk, which is protected by a password.

Below is a summary of the steps to generate and manage your license files:

1. Get license authorization file.
2. Generate license files.
3. Back up license files.

The following subsections describe the details of each step.

2.2.1.1 Get license authorization file

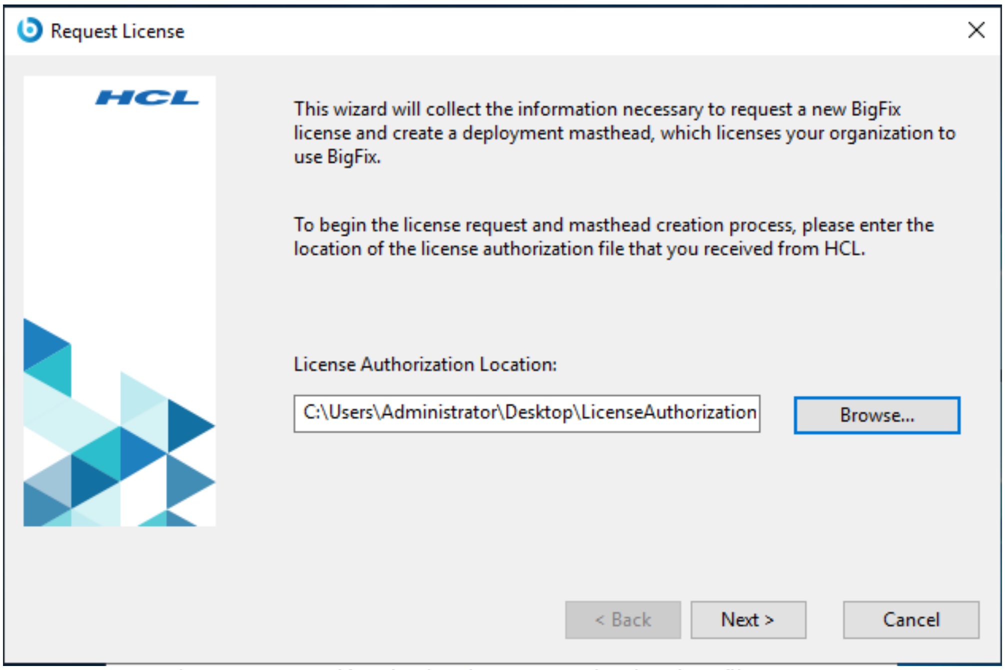
Contact HCL Software Customer Support at https://support.hcltechsw.com/csm to purchase a license. Within a few hours of your purchase, you will receive an email containing the instructions about how to access the BigFix License and Download portal.

Follow the instructions to visit the BigFix License and Download portal at https://id.hcltechsw.com/. Download and save the BigFix License Authorization file, which has a filename like CompanyName.BESLicenseAuthorization.

2.2.1.2 Generate license files

Download and run BigFix Installation Generator software to obtain your license files based on the BigFix License Authorization file.

1. Download BigFix Installation Generator software from BigFix Enterprise Suite Download Center website via the HTTPS protocol: https://support.bigfix.com/bes/release/11.0/patch3/
2. Run BigFix Installation Generator software as OS Administrator on the Windows computer where the TOE will be installed. When prompted, choose **Production** installation.
3. After reading and accepting the License Agreement, select the first option **Setup Type**: **I want to install with a BigFix license authorization file**.
4. Specify the location of the BigFix License Authorization file that you have received from HCL. See Figure 1.



This wizard will collect the information necessary to request a new BigFix license and create a deployment masthead, which licenses your organization to use BigFix.

To begin the license request and masthead creation process, please enter the location of the license authorization file that you received from HCL.

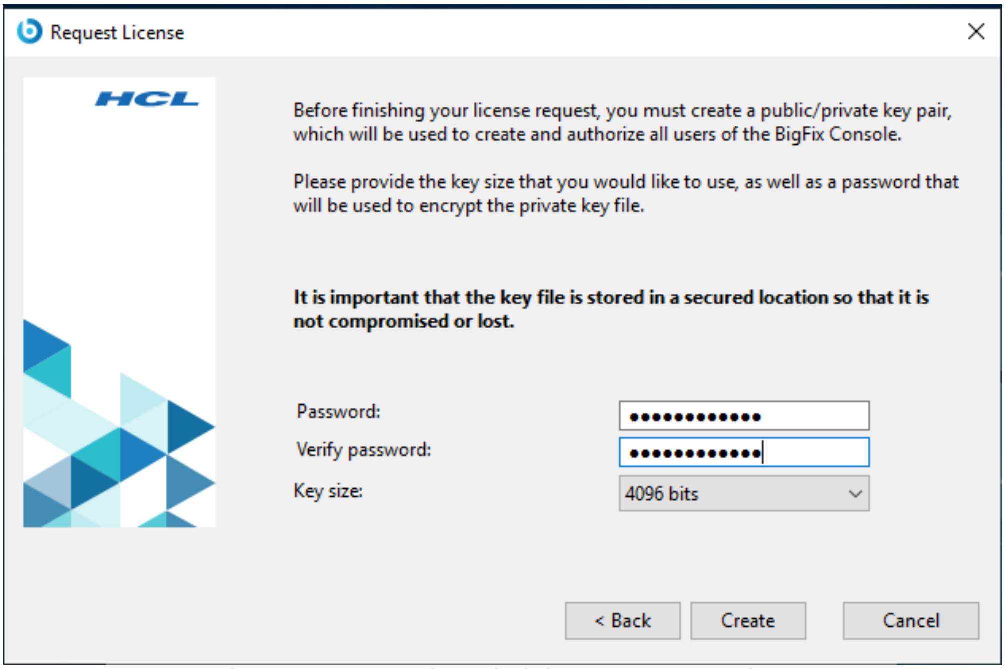
License Authorization Location: C:\Users\Administrator\Desktop\LicenseAuthorization

Figure 1: Specify BigFix License Authorization file

5. Specify the **DNS name** or **IP address** of the computer hosting the BigFix Server. The name or IP address that you enter in this field will be recorded in the license and used by Clients to identify the BigFix Server.
6. Create a private/public key pair. During this step, you are requested to set up the password for the **Site Administrator**. This password is used to protect the private key file.

   Type in the Site Administrator password twice and specify the key size of 4096 bits for encrypting the private key file. See Figure 2.

© 2025 HCL Technologies Ltd. All rights reserved.



Request License

Before finishing your license request, you must create a public/private key pair, which will be used to create and authorize all users of the BigFix Console.

Please provide the key size that you would like to use, as well as a password that will be used to encrypt the private key file.

It is important that the key file is stored in a secured location so that it is not compromised or lost.

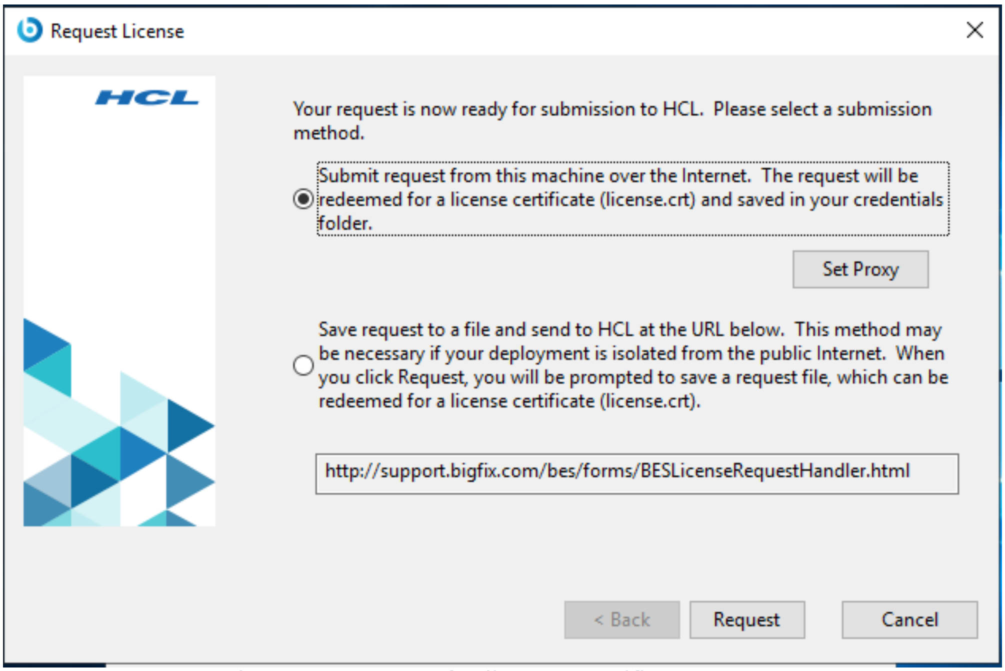
Password: ••••••••••••

Verify password: ••••••••••••

Key size: 4096 bits

Figure 2: Set up Site Administrator password

7. In the **Browse for Folder** dialog, choose a folder for storing your private key file (license.pvk), public key file (license.crt), and masthead file (masthead.afxm).
8. Submit a request to HCL over the Internet for a license certificate. This request consists of your original authorization file, BigFix Server DNS name, and your public key, all packaged into a single file. The request will be redeemed for your public key file (license.crt) from the BigFix License server. See Figure 3.



Request License

Your request is now ready for submission to HCL. Please select a submission method.

● Submit request from this machine over the Internet. The request will be redeemed for a license certificate (license.crt) and saved in your credentials folder.

○ Save request to a file and send to HCL at the URL below. This method may be necessary if your deployment is isolated from the public Internet. When you click Request, you will be prompted to save a request file, which can be redeemed for a license certificate (license.crt).

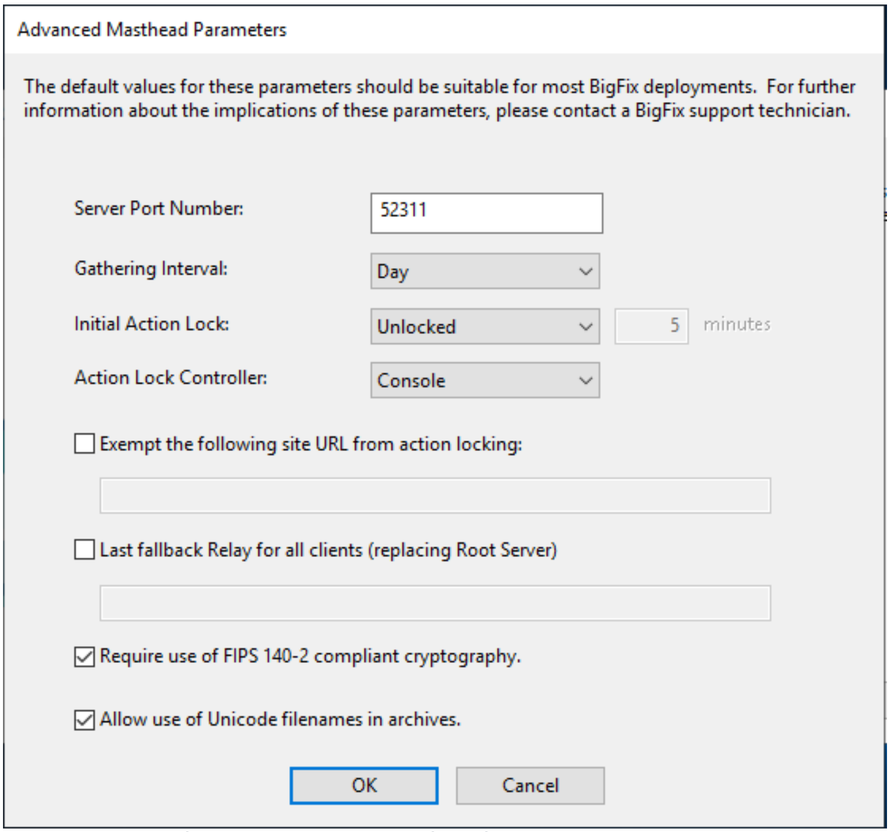
http://support.bigfix.com/bes/forms/BESLicenseRequestHandler.html

Figure 3: Request for license certificate

9. Create the masthead file. The masthead file contains configuration and license information together with a public key that is used to verify digital signatures.

   During this step, you need to set up the parameters for creating the masthead file. The default values for these parameters are suitable for the Common

Criteria evaluated configuration. Ensure to check the option **Require use of FIPS 140-2 compliant cryptography**. See Figure 4.



Advanced Masthead Parameters

The default values for these parameters should be suitable for most BigFix deployments. For further information about the implications of these parameters, please contact a BigFix support technician.

Server Port Number: 52311

Gathering Interval: Day

Initial Action Lock: Unlocked 5 minutes

Action Lock Controller: Console

□ Exempt the following site URL from action locking:

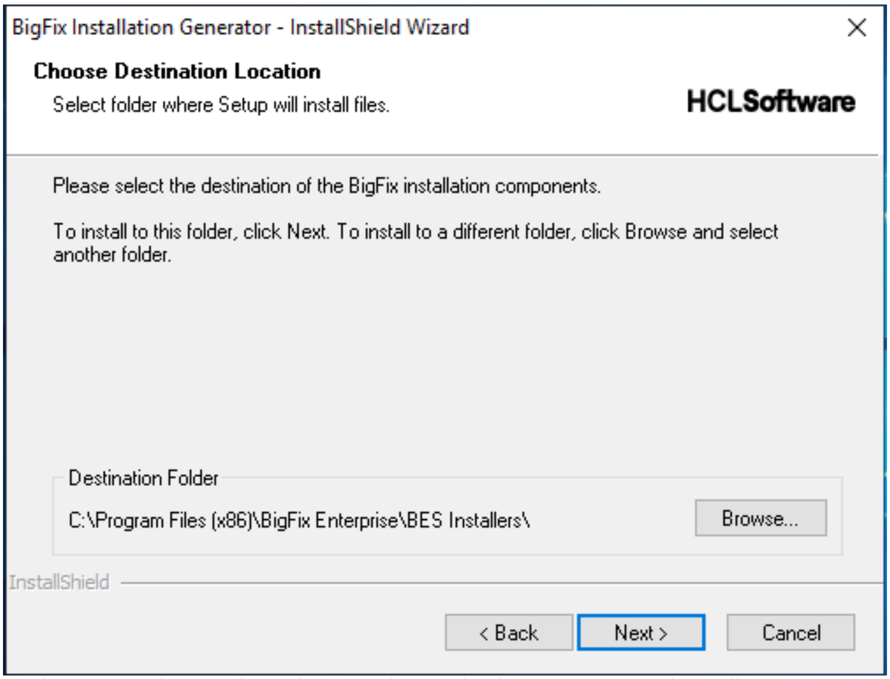
□ Last fallback Relay for all clients (replacing Root Server)

☑ Require use of FIPS 140-2 compliant cryptography.

☑ Allow use of Unicode filenames in archives.

Figure 4: Set up masthead parameters

10. Choose the folder in which to place the BigFix component installers. This step creates the installers for BigFix Server, BigFix Client, BigFix Console, but does not install the components. See Figure 5.



BigFix Installation Generator - InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

HCLSoftware

Please select the destination of the BigFix installation components.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

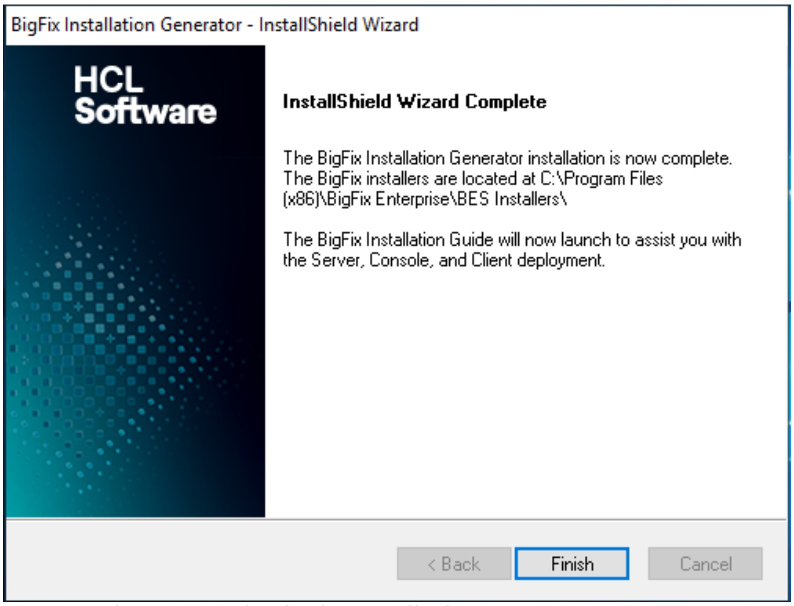
Destination Folder

C:\Program Files (x86)\BigFix Enterprise\BES Installers\

Figure 5: Choose location to place BigFix component installers

11. Click **Finish** to exit the BigFix Installation Generator - InstallShield Wizard. See Figure 6.

© 2025 HCL Technologies Ltd. All rights reserved.



BigFix Installation Generator - InstallShield Wizard

InstallShield Wizard Complete

The BigFix Installation Generator installation is now complete. The BigFix installers are located at C:\Program Files (x86)\BigFix Enterprise\BES Installers\

The BigFix Installation Guide will now launch to assist you with the Server, Console, and Client deployment.

Figure 6: Exit BigFix Installation Generator

Notes:

- It is important to keep the private key file and Site Administrator password secured. If you lose the private key file or password, a new license certificate needs to be created which entails a completely new installation.
- The masthead file created during the above process is later required to install other BigFix components. The file is placed, by default, in the following path: C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client\masthead.afxm
- It is recommended to specify the DNS name rather than IP address of the BigFix Server, because of its flexibility when changing server computers and doing advanced network configurations. The DNS name or IP address cannot be changed after a license is created.

2.2.1.3 Back up license files

Store your public key file (license.crt) with your private key file (license.pvk). Keep these two files together and create a backup copy on an external drive. Store the external drive in a secure location.

The private key file is protected by the Site Administrator password. It’s important to protect the Site Administrator password.

2.2.2 Firewall

By default, BigFix Server (the TOE) listens on TCP port 52311 for incoming connection requests from other BigFix platform components such as Consoles and Clients. For example, the Clients periodically check with the Server in order to obtain the most current updates.

The port number 52311 is the recommended port number, but you can choose a different port if that is more convenient for your particular network. Typically, you choose a port from the IANA range of private ports (49152 - 65535). You can use a reserved port number (1 - 1024), but this might reduce the ability to monitor or restrict traffic correctly and it prevents you from using port numbers for specific applications.

© 2025 HCL Technologies Ltd. All rights reserved.

Your choice of the server port number is done during the process of creating the masthead file, as described in Section 2.2.1. As a consequence, you must finalize the server port number before installation.

In addition, the TOE sends UDP packets to Clients to quickly inform them that there are new contents to be distributed. The Clients listen on a UDP port (default 52311) for messages from the Server indicating that new data is available for retrieval.

If you have defined an active firewall on the computer hosting the TOE, make sure to open the following two ports:

- TCP port 52311: inbound and outbound.
- UDP port 52311: outbound only.

2.2.3 MSSQL Database

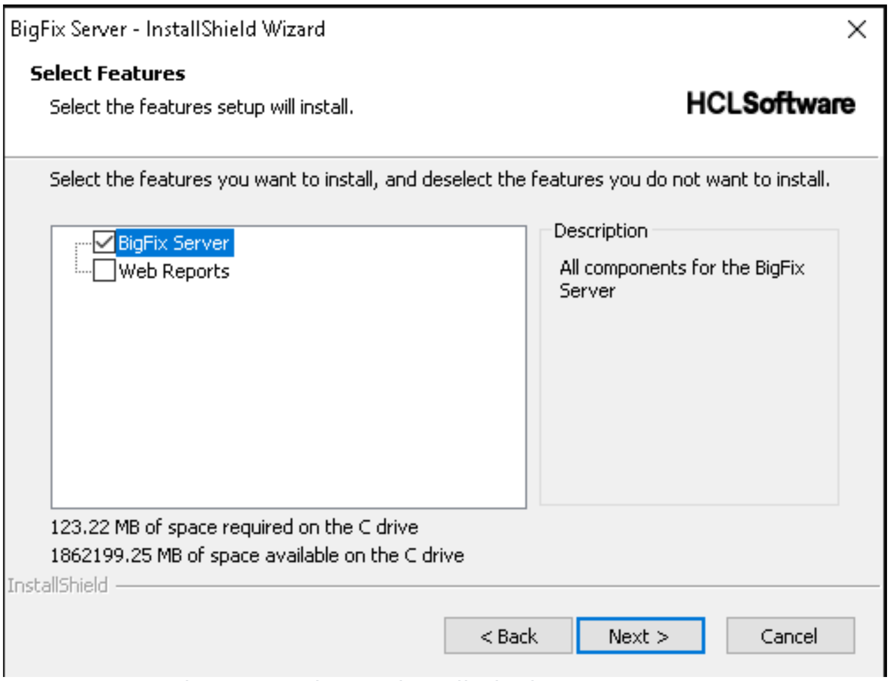
The Microsoft SQL Server 2019 database system must be installed on the same machine as the TOE, as a supporting component required by the TOE. Installation and setup of Microsoft SQL Server is available at Microsoft website. The following is a summary of steps to install Microsoft SQL Server 2019:

1. Obtain Microsoft SQL Server 2019 ISO image from Microsoft.
2. Copy the ISO image to the server computer. The file can be copied to any location.
3. Login as OS Administrator, mount the ISO image and start the installation. Follow the Installation instructions to install Microsoft SQL Server 2019 using the “Windows authentication”.

2.3 TOE Installation

To install the BigFix Server with a production license, perform the following steps:

1. On the computer where you want to install the BigFix Server, run the InstallShield Wizard for BigFix Server.
2. Select the features that you want to install: **BigFix Server**. See Figure 7.



BigFix Server - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☑ BigFix Server
□ Web Reports

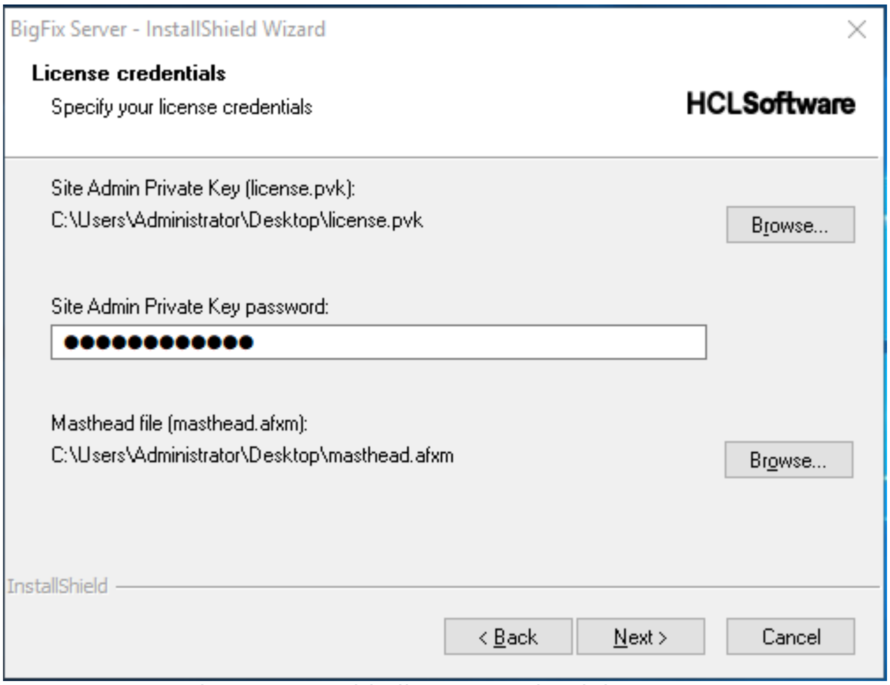
Description

All components for the BigFix Server

123.22 MB of space required on the C drive
1862199.25 MB of space available on the C drive

Figure 7: Select to install BigFix Server

3. Provide the password of the **Site Administrator** and confirm the locations of private key file (license.pvk) and masthead file (masthead.afxm). See Figure 8.



BigFix Server - InstallShield Wizard

License credentials

Specify your license credentials

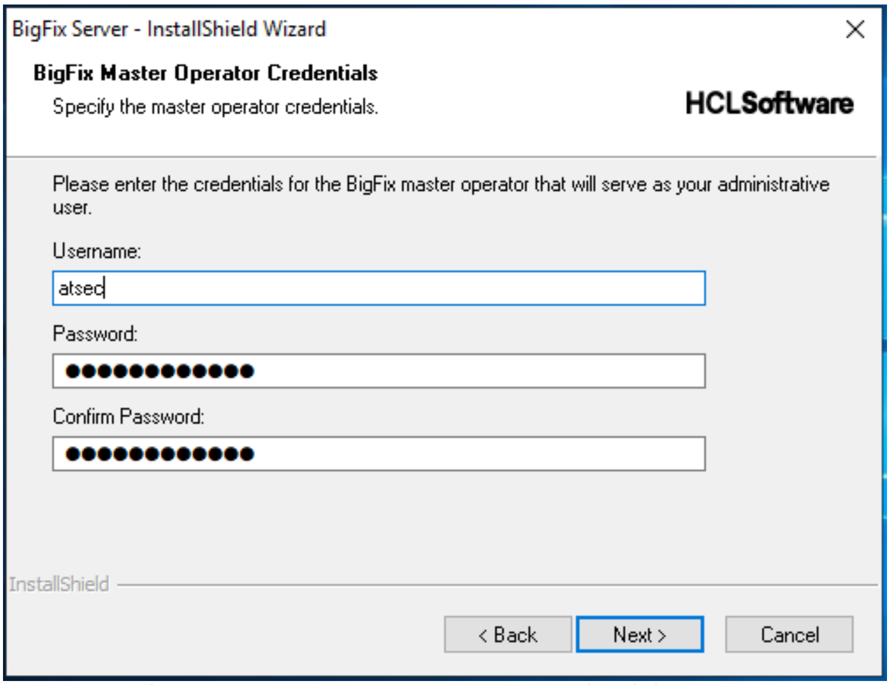
Site Admin Private Key (license.pvk):
C:\Users\Administrator\Desktop\license.pvk

Site Admin Private Key password:
●●●●●●●●●●●●

Masthead file (masthead.afxm):
C:\Users\Administrator\Desktop\masthead.afxm

Figure 8: Provide license credentials

4. Select **Single or Master Database** as database replication, to indicate there is only one database in the deployment.
5. Set up the username and password of the BigFix **Master Operator**. See Figure 9.



BigFix Server - InstallShield Wizard

BigFix Master Operator Credentials

Specify the master operator credentials.

Please enter the credentials for the BigFix master operator that will serve as your administrative user.

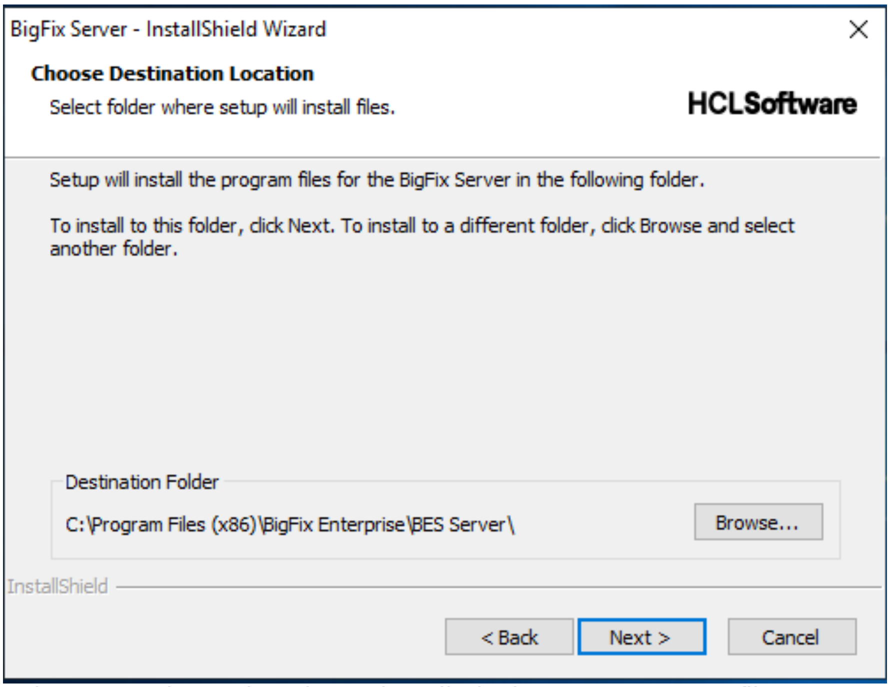
Username:
atsec

Password:
●●●●●●●●●●●●

Confirm Password:
●●●●●●●●●●●●

Figure 9: Set up Master Operator credentials

6. Select **Use Local Database** as the type of database, to indicate that the database is installed on the same computer as the BigFix Server.
7. Confirm the destination folder where the BigFix Server program files will be installed. See Figure 10.



BigFix Server - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Setup will install the program files for the BigFix Server in the following folder.

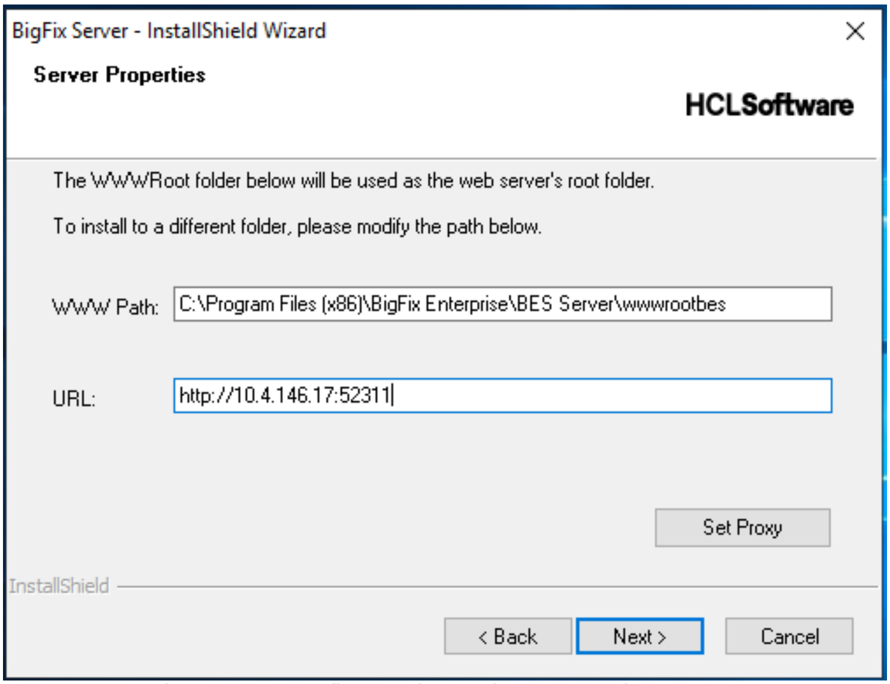
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

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

Figure 10: Choose location to install BigFix Server program files

8. Confirm the web server's root folder and URL of the BigFix Server. See Figure 11.



BigFix Server - InstallShield Wizard

Server Properties

The WWWRoot folder below will be used as the web server's root folder.

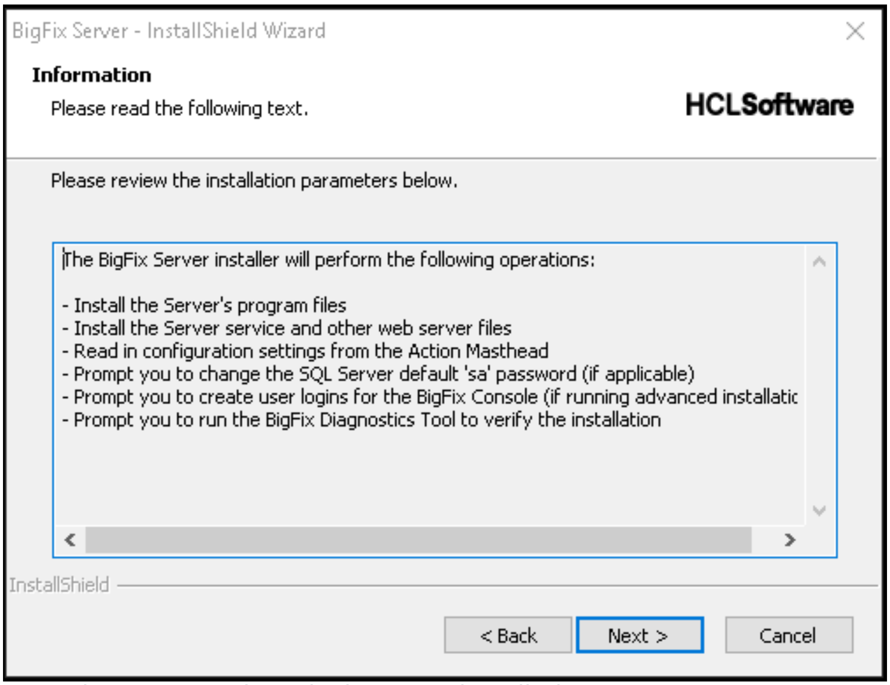
To install to a different folder, please modify the path below.

WWW Path: C:\Program Files (x86)\BigFix Enterprise\BES Server\wwwrootbes

URL: http://10.4.146.17:52311

Figure 11: Confirm web service properties

9. Review all the installation parameters and click **Next** to start installation. See Figure 12.



Information

Please read the following text.

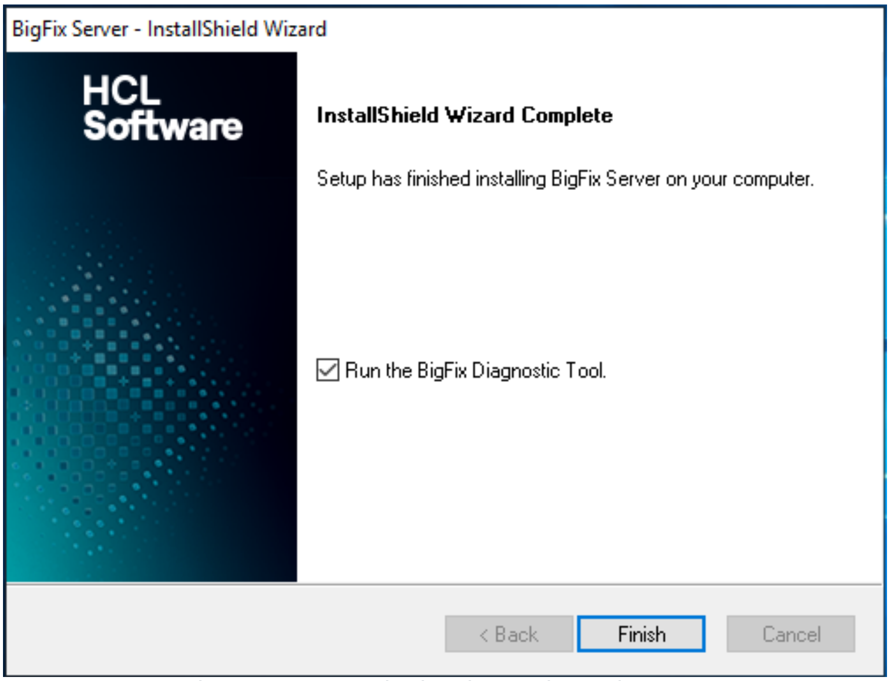
Please review the installation parameters below.

The BigFix Server installer will perform the following operations:

- Install the Server's program files
- Install the Server service and other web server files
- Read in configuration settings from the Action Masthead
- Prompt you to change the SQL Server default 'sa' password (if applicable)
- Prompt you to create user logins for the BigFix Console (if running advanced installatic
- Prompt you to run the BigFix Diagnostics Tool to verify the installation

Figure 12: Review BigFix Server installation parameters

10. When the installation has finished, select **Run the BigFix Diagnostic Tool** to verify the installation is successful. See Figure 13.



InstallShield Wizard Complete

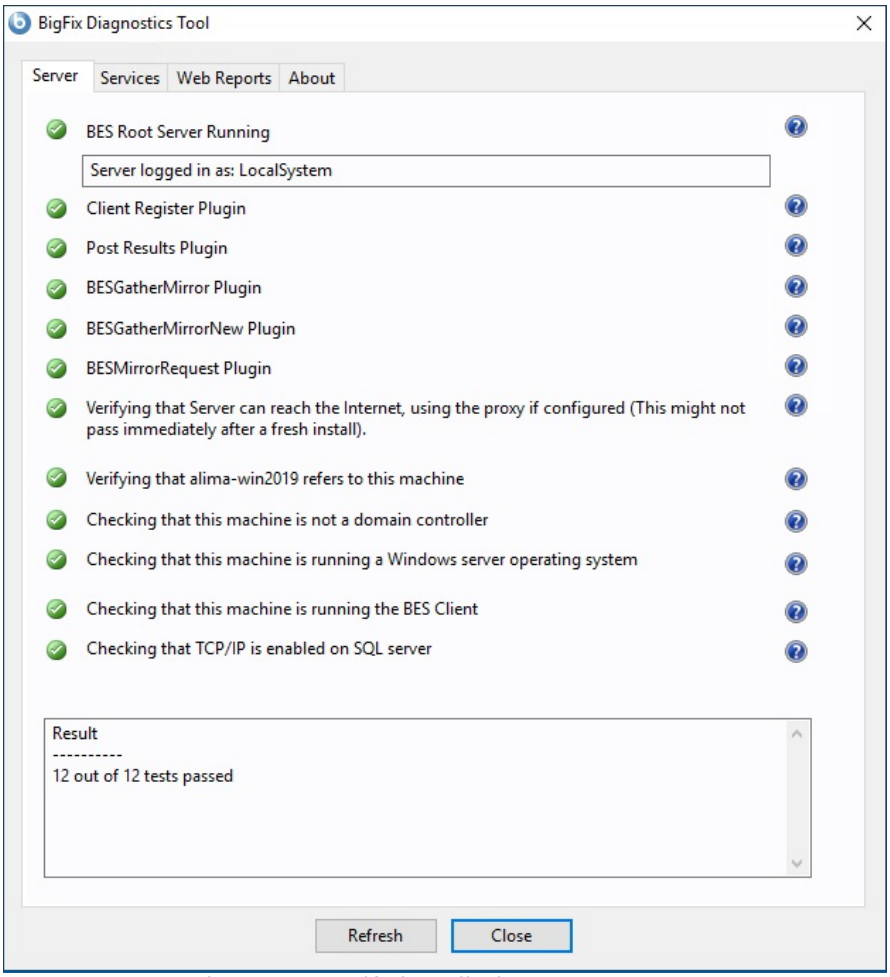
Setup has finished installing BigFix Server on your computer.

☑ Run the BigFix Diagnostic Tool.

Figure 13: Run BigFix Diagnosis Tool

11. A window pops up showing the installation status. If all the buttons are green, the installation completed successfully. Otherwise, address the problem to be sure that the server is working correctly. See Figure 14.

© 2025 HCL Technologies Ltd. All rights reserved.



✓ BES Root Server Running

Server logged in as: LocalSystem

✓ Client Register Plugin

✓ Post Results Plugin

✓ BESGatherMirror Plugin

✓ BESGatherMirrorNew Plugin

✓ BESMirrorRequest Plugin

✓ Verifying that Server can reach the Internet, using the proxy if configured (This might not pass immediately after a fresh install).

✓ Verifying that alima-win2019 refers to this machine

✓ Checking that this machine is not a domain controller

✓ Checking that this machine is running a Windows server operating system

✓ Checking that this machine is running the BES Client

✓ Checking that TCP/IP is enabled on SQL server

```
Result
----------
12 out of 12 tests passed
```

Figure 14: Verify installation status

Notes:

- During the Server installation process, you are requested to create an account for the BigFix Master Operator. It is important to protect the Master Operator credentials.
- During the installation process, a server signing key is created and stored as a file on the server machine. Whenever operators issue an action, it is digitally signed by the server signing key, and the Client will only trust actions that are signed by that key. Since Clients will trust any action signed by the server signing key, it is important to protect the server signing key file. To protect the server signing key file, the physical administrator access to the server machine must be restricted.

2.4 Client Installation

After the TOE installation, certain configuration steps are required to transform the TOE into the Common Criteria evaluated configuration (refer to Section 3). If the Administrator chooses to use the BigFix Console to manage the TOE configuration (refer to Section 3.1), it is necessary to install the BigFix Client on the same machine where the TOE is installed. Otherwise, this step is optional.

To install the BigFix Client, perform the following steps:

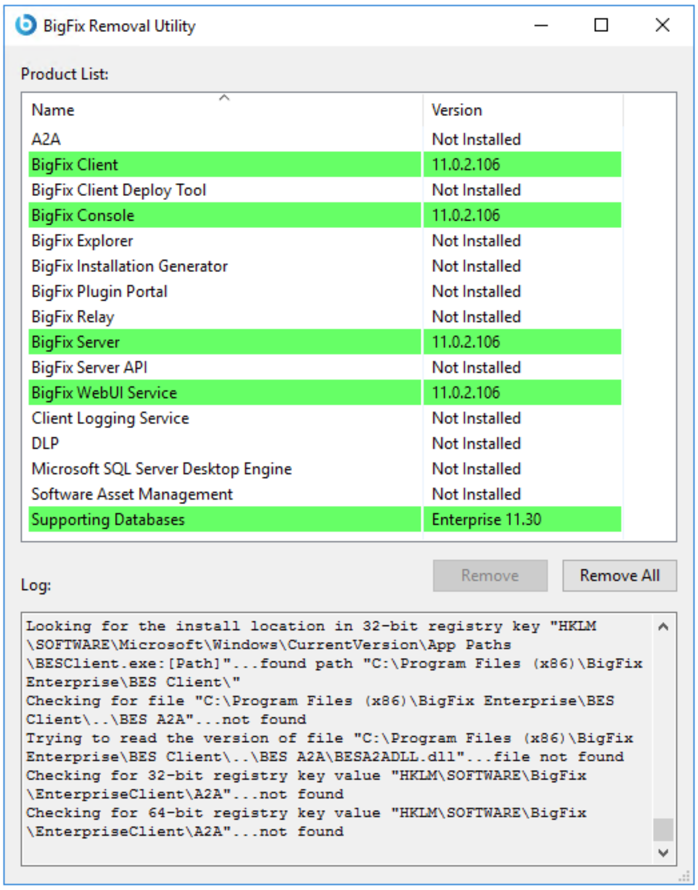
1. On the computer where the TOE is installed, run the InstallShield Wizard for BigFix Client.

2. After the welcome panel, you are prompted for a location to install the software. You can accept the default or click **Browse** to select a different location.
3. After the files have been moved, click **Done** to exit the installer. The BigFix Client program is now installed and will automatically begin working in the background.

2.5 Uninstallation

To uninstall BigFix Server or other BigFix components, run the following steps:

1. Download BESRemove utility software from BigFix Enterprise Suite Download Center website via the HTTPS protocol: https://support.bigfix.com/bes/release/11.0/patch3/
2. Run BESRemove.exe program.
3. Select the components that you want to uninstall and then click **Remove**. Or click **Remove All** to remove all the BigFix components from the system. See Figure 15.



Product List:

Name	Version
A2A	Not Installed
BigFix Client	11.0.2.106
BigFix Client Deploy Tool	Not Installed
BigFix Console	11.0.2.106
BigFix Explorer	Not Installed
BigFix Installation Generator	Not Installed
BigFix Plugin Portal	Not Installed
BigFix Relay	Not Installed
BigFix Server	11.0.2.106
BigFix Server API	Not Installed
BigFix WebUI Service	11.0.2.106
Client Logging Service	Not Installed
DLP	Not Installed
Microsoft SQL Server Desktop Engine	Not Installed
Software Asset Management	Not Installed
Supporting Databases	Enterprise 11.30

Log:

```
Looking for the install location in 32-bit registry key "HKLM
\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths
\BESClient.exe:[Path]"...found path "C:\Program Files (x86)\BigFix
Enterprise\BES Client\"
Checking for file "C:\Program Files (x86)\BigFix Enterprise\BES
Client\..\BES A2A"...not found
Trying to read the version of file "C:\Program Files (x86)\BigFix
Enterprise\BES Client\..\BES A2A\BESA2ADLL.dll"...file not found
Checking for 32-bit registry key value "HKLM\SOFTWARE\BigFix
\EnterpriseClient\A2A"...not found
Checking for 64-bit registry key value "HKLM\SOFTWARE\BigFix
\EnterpriseClient\A2A"...not found
```

Figure 15: Uninstall BigFix components

© 2025 HCL Technologies Ltd. All rights reserved.

3 Configuration

After the TOE installation, it is necessary to perform certain configuration steps to transform the TOE into the Common Criteria evaluated configuration.

Below is a summary of the configuration steps:

1. Customizing HTTPS communication.
2. Enabling Windows Control Flow Guard runtime.
3. Disabling unnecessary ports and services.
4. Restarting.

3.1 Customizing HTTPS Communication

In the evaluated configuration, the network communications between the TOE and other trusted IT products should be secured. By design, the TOE administrative traffic is protected with the HTTPS protocol. That is, the TOE uses HTTPS to accept requests from BigFix Consoles and REST API applications.

In order to transform the TOE into the evaluated configuration, the Administrator must perform certain configuration settings to enable the TOE to use HTTPS for accepting requests from the BigFix Clients and collecting contents from external sites (i.e., Fixlet servers and vendor sites).

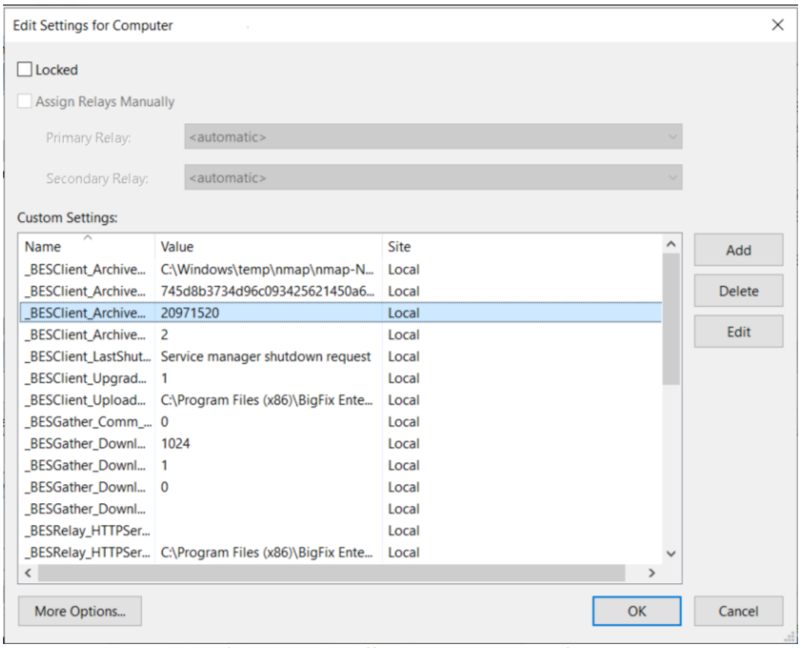
The configuration settings are maintained as Windows Registry keys at the following location:
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\EnterpriseClient\Settings\Client

The TOE configuration can be managed through the BigFix Console remotely over the network or using the Windows Registry Editor locally on the TOE.

- **Through the BigFix Console**

  This approach is more straightforward and, therefore, recommended. Log into the BigFix Console as a Master Operator (refer to Section 4.1):

  1. Navigate to the **Computer** section under the **All Content** domain, then select the computer running the BigFix Server (TOE).
  2. Right-click the computer and choose **Edit Computer Settings**. A dialog window will appear. See Figure 16.
  3. In the **Custom Setting** box, check if the entry you want to configure (e.g., _BESGather_Use_Https) has been created. If it exists, click the **Edit** button to set its value (e.g., 1).
  4. If the setting entry does not exist, click the **Add** button to create the entry and set the value.



Name	Value	Site
_BESClient_Archive...	C:\Windows\temp\nmap\nmap-N...	Local
_BESClient_Archive...	745d8b3734d96c093425621450a6...	Local
_BESClient_Archive...	20971520	Local
_BESClient_Archive...	2	Local
_BESClient_LastShut...	Service manager shutdown request	Local
_BESClient_Upgrad...	1	Local
_BESClient_Upload...	C:\Program Files (x86)\BigFix Ente...	Local
_BESGather_Comm_...	0	Local
_BESGather_Downl...	1024	Local
_BESGather_Downl...	1	Local
_BESGather_Downl...	0	Local
_BESGather_Downl...		Local
_BESRelay_HTTPSer...		Local
_BESRelay_HTTPSer...	C:\Program Files (x86)\BigFix Ente...	Local

Figure 16: Edit computer setting

- **Using the Windows Registry Editor**

  Log into the TOE computer as the Windows OS Administrator:

  1. Open **Registry Editor**. One way is to press the Windows + R keys simultaneously, type “regedit”, and press Enter.
  2. Browse to the registry path:
  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\EnterpriseClient\Settings\Client
  3. If the key you want to configure does not exist at the registry location, create the key and give it a name (e.g., _BESGather_Use_Https). Then add a string value (REG_SZ type) named “value” to the key and set the value (e.g., 1).
  4. If the key has already been created, set its value only.

The configuration settings are summarized in Table 1. The remainder of this section discusses details.

Configuration Setting	Value and Purpose
_BESGather_Use_Https	Set to 1 to enforce HTTPS for gathering from Fixlet servers.
_BESRelay_Download_UseHttps	Set to 1 to enforce HTTPS for downloading from vendor sites.
_BESServer_HTTPServer_ForceTLS	Set to 1 to enforce HTTPS for accepting requests from Clients.
_BESGather_CAVerifyStrict	Set to 1 to enable strict root CA validation when gathering.
_BESRelay_Download_CAVerifyStrict	Set to 1 to enable strict root CA validation when downloading.
_BESGather_OcspVerify	Set to 1 to enable OCSP stapling and OCSP certificate revocation checks when gathering.
_BESRelay_Download_OcspVerify	Set to 1 to enable OCSP stapling and OCSP certificate revocation checks when downloading.
_BESRelay_HTTPRequester_OCSPCacheHours	Set to 0 to turn off OCSP caching.
_RESTAPI_HTTPServer_PortNumber	In case of using a port number different from the default (BigFix port 52311), set the port for REST API. A non-default port is required when using a custom TLS server certificate for REST API.
_RESTAPI_HTTPServer_SSLCertificateFilePath	Set the full path of the TOE's custom TLS server certificate file for REST API. It is ignored if _RESTAPI_HTTPServer_PortNumber is not set or is set to the BigFix port (52311).
_RESTAPI_HTTPServer_SSLPrivateKeyFilePath	Set the full path of the TOE's custom TLS server private key file for REST API. It is ignored if _RESTAPI_HTTPServer_PortNumber is not set or is set to the BigFix port (52311).
_BESGather_CACert	In case a customized set of trusted CA certificates is required for gathering, set the full path the folder storing the trusted certificates.
_BESRelay_Download_CaCertDirectory	In case a customized set of trusted CA certificates is required for downloading, set the full path of the folder storing the trusted certificates.

Table 1: Configuration settings for customizing HTTPS communication

3.1.1 Customizing HTTPS for Gathering

The word "gathering" refers to gathering Fixlets from subscribed Fixlet servers. In the evaluated configuration, the TOE uses only the HTTPS protocol to gather Fixlets from Fixlet servers.

3.1.1.1 Enforcing HTTPS

To enforce the TOE to use only HTTPS for gathering, set the configuration setting **_BESGather_Use_Https = 1**.

The possible values of _BESGather_Use_Https are 0, 1, and 2.

- When set to 0, the TOE uses the protocol defined in the Fixlet server URL for gathering.
- When set to 1, the TOE uses HTTPS for gathering from Fixlet servers.
- When set to 2, the TOE first tries to use the HTTPS protocol. If the gathering fails, the TOE will use the HTTP protocol. The fallback from HTTPS to HTTP only applies to the Fixlet servers having URLs starting with http://. The default value for this setting is 2.

3.1.1.2 Trusted certificates

By default, the TLS certificates used for enabling the HTTPS connection are validated by using the Certification Authority (CA) certificate bundle included in the BigFix Server installation. The Windows default path is:
C:\Program Files (x86)\BigFix Enterprise\BES Server\Reference\ca-bundle.crt

In case a custom bundle of trusted certificates is required to validate the certificates, a custom directory should be specified through the configuration setting **_BESGather_CACert**:

1. Create or download a set of trusted certificates (for example, http://curl.haxx.se/ca/cacert.pem). The certificates that you can use are:
   - "VeriSign Universal Root Certification Authority" (to gather sites)
   - "thawte Primary Root CA - G3" (to check license updates)
2. Create a configuration setting called **_BESGather_CACert** (if it does not exist).
3. Set its value to the full path of the folder storing those trusted certificates (e.g., C:\TEM\certificates\custom-ca-bundle.crt).

3.1.2 Customizing HTTPS for Downloads

The word “downloads” refers to the effect triggered by the action commands in Fixlets to download software patches from the software vendor sites.

3.1.2.1 Enforcing HTTPS

To enforce the TOE to use only the HTTPS protocol for downloads, set the configuration setting **_BESRelay_Download_UseHttps = 1**.

3.1.2.2 Trusted certificates

The majority of BigFix content works without additional changes in the BigFix platform configuration. Customization is needed only in specific cases, depending on the type of certificate used:

- Certificates signed by external/public CA: no action needed.
- Certificates signed by internal/private CA: custom certificates need to be added.
- Self-signed certificates: custom certificates need to be added.

By default, the TOE uses a predefined folder, <StorageFolder>/TrustedDownloadCerts, to store custom certificates and/or bundles. All the .crt and .pem files contained in this folder are added to the default certificates when an HTTPS download is performed.

In addition to that predefined folder, a custom directory can be specified through setting the configuration setting **_BESRelay_Download_CaCertDirectory**:

1. Create a configuration setting called **_BESRelay_Download_CaCertDirectory** (if it does not exist).
2. Set its value to the full path of the folder storing the custom CA bundles. All the .crt and .pem files contained in this folder are added to the default certificates.

3.1.3 Customizing HTTPS for Communicating with Clients

To enforce the TOE to use HTTPS when accepting all the connections from Clients, set the configuration setting **_BESServer_HTTPServer_ForceTLS = 1**.

For these communications, the TOE uses a BigFix-issued certificate / private key that cannot be changed.

3.1.4 Customizing HTTPS on REST API

The TOE provides a REST application programming interface (API). It allows for using a set of standardized and operating system independent methods to perform the majority of the tasks available in the BigFix Console.

By design, the TOE enforces the HTTPS protocol to protect the communication channel of REST API applications. By default, the port number for the REST API is the BigFix port (52311); in case the Administrator wants to set a port number for the REST API different from the BigFix one, the configuration setting **_RESTAPI_HTTPServer_PortNumber** should be set.

If the Administrator wants to use a custom certificate for the REST API, ***it is mandatory to configure the port number***; in this case, the path of custom certificate and private key should be configured:

1. Create a configuration setting called **_RESTAPI_HTTPServer_PortNumber** (if it does not exist). Set its value to the chosen port number (different from the BigFix port, defaulting to 52311).

Important: If you combined the private key file with the certificate file, skip Step 2 below and go directly to Step 3.

2. Create a configuration setting called **_RESTAPI_HTTPServer_SSLPrivateKeyFilePath** (if it does not exist). Set its value to the full path name of the private key (.pem) file which contains the private key for the server.
3. Create a configuration setting called **_RESTAPI_HTTPServer_SSLCertificateFilePath** (if it does not exist). Set its value the full path name of the certificate (.pem) file.

3.1.5 Managing Certificate Verification

As a TLS client, the TOE needs to verify and check revocation status of the certificates received from external sites.

To enable strict root CA validation, set the following configuration settings:

- **_BESGather_CAVerifyStrict = 1**
  to enable strict root CA validation when gathering.
- **_BESRelay_Download_CAVerifyStrict = 1**
  to enable strict root CA validation when downloading.

To enable both OCSP Stapling and OCSP on the TOE to check the revocation status of external sites' certificates, set the following configuration settings:

- **_BESGather_OcspVerify = 1**
  to enable OCSP stapling and OCSP certificate revocation checks when gathering
- **_BESRelay_Download_OcspVerify = 1**

to enable OCSP stapling and OCSP certificate revocation checks when downloading

In addition, OCSP caching should be disabled. The Administrator must set the configuration setting **_BESRelay_HTTPRequester_OCSPCacheHours = 0**.

3.2 Enabling Windows Control Flow Guard

The Microsoft Control Flow Guard (CFG) is a Windows platform security feature to combat memory corruption vulnerabilities.

The CFG is enabled at the TOE’s build time; the runtime is disabled when installing the BigFix Server. CFG runtime can be enabled using any of the following approaches:

- As the OS Administrator, configure Windows Defender Exploit Protection to enable CFG (e.g., using the Windows Security app or PowerShell Set-ProcessMitigation cmdlet).
- As the Site Administrator (refer to Section 4.1), run the Admin Tool command with the following options:
  ```
  C:\Program Files (x86)\BigFix Enterprise\BES Server\BESAdmin /setcontrolflowguard /enable /all
  ```

3.3 Disabling Unnecessary Ports and Services

3.3.1 Disabling WebUI Port

BigFix WebUI is a BigFix platform component providing a web interface of administration. BigFix WebUI is not part of the evaluated configuration.

The TOE is designed to listen on the TCP port 52315 (the WebUI port) to accept the requests from the BigFix WebUI. In the evaluated configuration, the WebUI port must be disabled.

To disable the WebUI port, set the configuration setting **_APIServer_HTTPServer_IsEnabled = 0**.

3.3.2 Disabling FTP and SSH

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

3.4 Restarting Service

After finishing the aforementioned configuration steps, the Administrator must restart the BigFix Server service:

1. Open **Windows Services Control Manager**. One way is to press the Windows + R keys simultaneously, type “services.msc”, and press Enter.
2. Select **BES Root Server**.
3. On the **Action** menu, click **Restart**.

4 Security Management

4.1 User Roles

The TOE provides security management functions that can only be accessed by authorized users. The TOE support three types of user roles:

- **Site Administrator**.
- Console Operators:
  - **Master Operators** (MO),
  - **Non-Master Operators** (NMO), a.k.a. Operators.

Each of those user roles has different privileges and responsibilities. Often these roles overlap, and one person might be assigned multiple duties.

- The Site Administrator is responsible for installing and maintaining the BigFix software, and to run administrative tasks that globally affect the environment such as site-level signing key management. There is only one Site Administrator for a BigFix environment.
- Console Operators are the users who access the BigFix Console. They can be Master Operators or Non-Master Operators. While Master Operators can create other operators and assign management rights, Non-Master Operators cannot.
  - Master Operators are the administrative users of the Console. They have access to all the computers defined in the BigFix environment. They also have the authority to create and manage other Console Operators. Any Master Operator can create, assign, and revoke management rights that allow operators to deploy actions.
  - Non-Master Operators (a.k.a. Operators) manage the day-to-day BigFix operations, including Fixlet management and action deployment, on a subset of computers they are allowed to manage by the Master Operator. They cannot create other operators or assign management rights.

In the evaluated configuration, the BigFix Server (TOE) is administered through the Console over the network and the Administration Tool on the same computer hosting the TOE. The Site Administrator uses the Administrator Tool to perform the security management functions, by providing the password and private key. The Console Operators use the BigFix Console to perform the security management functions, by providing the username and password.

4.2 Management Functions

4.2.1 Create Console Operators

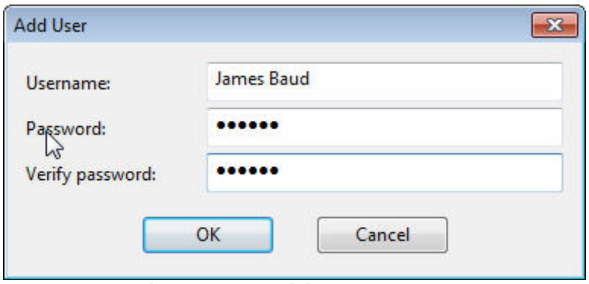
During the BigFix installation process, the first Master Operator (default name is BFAdmin) is created to log in the BigFix Console.

The Master Operator can create other Console Operators via the BigFix Console. Below is a summary of the steps for Master Operators to add a Console Operator.

As the Master Operator,

1. Start the Console by double-clicking its desktop icon or select it from the Programs menu: **Start** > **Programs** > **BigFix** > **BigFix Console**.

2. Click the **Tools** > **Create Operator** menu item or right click in the **Operators** work area and select **Create Operator**. The **Add User** dialog appears. See Figure 17.
3. Enter the **Username** of the newly created operator.
4. Enter a **Password** and retype it for confirmation.
5. Click **OK**. The **Console Operator** window opens.
6. From the **Details** tab, specify if the newly created operator is a Master Operator or not, and assign operator permissions. See Figure 18.



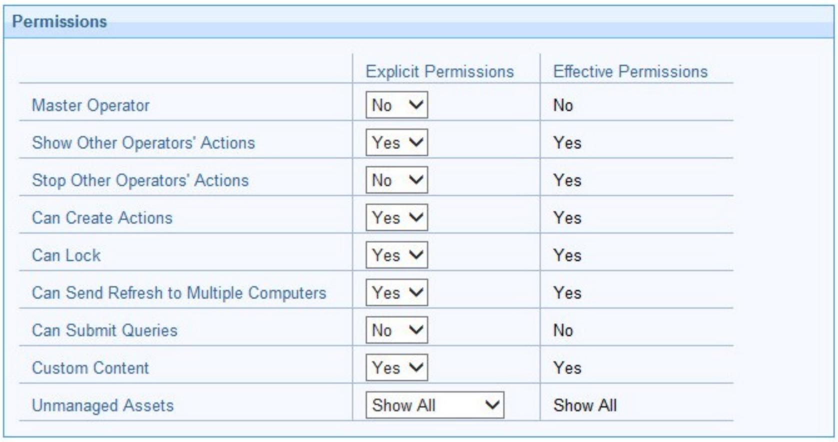
Add User

Username: James Baud

Password: ••••••

Verify password: ••••••

Figure 17: Add user



Permissions

	Explicit Permissions	Effective Permissions
Master Operator	No	No
Show Other Operators' Actions	Yes	Yes
Stop Other Operators' Actions	No	Yes
Can Create Actions	Yes	Yes
Can Lock	Yes	Yes
Can Send Refresh to Multiple Computers	Yes	Yes
Can Submit Queries	No	No
Custom Content	Yes	Yes
Unmanaged Assets	Show All	Show All

Figure 18: Set up permissions

4.2.2 Change Password

Console Operators can change their passwords via the BigFix Console.

The dialog is available by selecting **File** > **Change Password**. In the dialog, enter the current password, then enter and validate the new password.

4.2.3 Obtain TOE Name and Version

The Site Administrator can learn the TOE name and version by checking one of the following files stored on the computer hosting the TOE.

- The BigFix Server version is always written in the log file at C:\Program Files (x86)\BigFix Enterprise\BES Server\server_audit.log. Open the file and check the line starting with “BES Root Server version”.
- Looking at the details tab of the properties of the BESRootServer.exe file at C:\Program Files (x86)\BigFix Enterprise\BES Server\BESRootServer.exe.

The Console Operator can learn the TOE version by selecting the **Help** > **About** panel of BigFix Console. The Console version is the same as the Server version, since a Console to connect the Server must use the same version of BigFix DB (an “internal”

© 2025 HCL Technologies Ltd. All rights reserved.

value referencing the version of the DB tables used by BigFix) and this version changes at each release.

4.2.4 Verify TOE Updates

The Console Operator can check for the updates to the TOE via BigFix Console:

1. Open BigFix Console. Ensure “Show Non-Relevant Content” is highlighted.
2. Open “Fixlets and Tasks” > “Fixlets Only” > “By Category” > “Upgrade” > “By Source” > “HCL”.
3. Search the list of Fixlets for “BigFix Server 11.0.3”.
4. The most recently published version of BigFix Server is listed at the top.

4.3 Updating

A TOE update is not a patch applied to the existing TOE; it is a new version of the TOE. When TOE updates are made available, the Site Administrator can obtain and install the update.

Please refer to Section 2.3 for the instructions of installing updates.

5 TLS Protocol

The default TLS configuration of the TOE is suitable for the Common Criteria evaluated configuration. No additional configuration is required to ensure proper usage. The cryptographic algorithm and key size are selected automatically during the negotiation of TLS session establishment.

5.1 TLS Versions and Cipher Suites

The TOE includes OpenSSL to implement the TLS protocol. The TOE supports the TLS protocol versions 1.2 and 1.3. The TOE does not support TLS version 1.1 or below. The TOE claims conformance to Functional Package for Transport Layer Security v1.1 (pkg_tls_v1.1), which does not cover TLS version 1.3. Therefore, TLS version 1.3 is out of scope of the evaluation and this document focuses on TLS version 1.2.

The table below lists the TLS cipher suites supported by the TOE as TLS client and TLS server, respectively.

TOE	Cipher Suites
TLS client	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS server	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Table 2: TLS cipher suites

5.2 Setting TLS Cipher Suites

The default setting of TLS cipher suites is suitable for the Common Criteria evaluated configuration. No additional configuration of TLS cipher suites is required.

5.2.1 Setting TLS Client Cipher Suites

The cipher suites supported by the TOE as TLS client are not configurable.

5.2.2 Setting TLS Server Cipher Suites

The cipher suites supported by the TOE as TLS server can be configured. The TOE represents the TLS cipher suites with the TLS cipher list in the masthead. The TLS cipher list is a colon-delimited list of cipher suites. To disable a cipher suite, precede the name with "!".

The default TLS 1.2 cipher list used by the TOE as server is:

```
HIGH:!ADH:!AECDH:!kDH:!kECDH:!kRSA:!PSK:!SRP:!SHA1
```

This setting is used when no TLS cipher list is present in the masthead.

The Site Administrator can manage the TLS cipher list by using the BigFix Administration Tool in Command Line Interface (CLI). Since the default setting of TLS cipher suites is suitable for the evaluated configuration, the Site Administrator does not need to run that command to set the TLS server cipher suites. Instead, the Site Administrator may use that command to review the cipher suites supported by the TOE as TLS server (refer to Section 5.2.2.2).

The TOE installation process automatically downloads the BigFix Administration Tool program, BESAdmin.exe, into the folder C:\Program Files (x86)\BigFix Enterprise\BES Server

To run the Administration Tool CLI, the Site Administrator performs the following steps:

1. Open a Windows command prompt.
2. Change to the following folder:
   cd C:\Program Files (x86)\BigFix Enterprise\BES Server\
3. Execute BESAdmin.exe with appropriate parameters and arguments:
   .\BESAdmin.exe */service {arguments}*

5.2.2.1 Set TLS cipher list

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

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

5.2.2.2 List TLS cipher list

To view the content of cipher list, use the following command:

1. .\BESAdmin.exe /securitysettings /listTLSCiphers
2. When prompted, provide the Site Admin password and private key file.

5.2.2.3 Reset TLS cipher list to default

To remove the TLS cipher list from the masthead and return to the default cipher list, run the following command:

1. .\BESAdmin.exe /securitysettings /removeTLSCipherList
2. When prompted, provide the Site Admin password and private key file.

5.3 Setting Reference Identifier

The TOE communicates with subscribed Internet sites, i.e., Fixlet servers and vendor sites, using the HTTPS protocol as a client. For the purposes of validating the certificates of Internet sites, the TOE automatically establishes the reference identifiers from the URLs that the TOE uses when connecting to the Internet sites.

There is no security management function to change this behavior.

6 Error Messages and Handling

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

The following sections summarize common group of errors and related corrective actions.

6.1 Administration Tool Errors

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

Error	Corrective Action	Who
Database connection errors	Verify that the database is running. If the problem persists, contact the BigFix support.	System Administrator
Invalid Action Site Masthead	Select the correct Action Site Masthead in the error dialog.	Site Administrator
Invalid signing key location	Select a valid signing key location.	Site Administrator
Invalid certificate	Select the correct private key file. If the problem persists, contact the BigFix support.	Site Administrator
Incorrect password	Use the correct password and correct private key file.	Site Administrator
Database not initialized	Initialize the database. If the problem persists, contact the BigFix support.	System Administrator
Invalid database version	Upgrade the product (and DB version). If the problem persists, contact the BigFix support.	System Administrator
Invalid site certificate	Use a valid site certificate. If the problem persists, contact the BigFix support.	Site Administrator
Invalid edit masthead option	Use the correct option (error suggests the correct option or the invalid set).	Site Administrator
Invalid command	Use the correct command option (error shows the list of options or the invalid set).	Site Administrator
Invalid advanced options	Use the correct option (error suggests the corrects options or the invalid set).	Site Administrator
Report encryption errors	Select the correct option (error suggests the corrects options or the invalid set).	Site Administrator
Security settings errors	Select the correct option (error suggests the corrects options or the invalid set).	Site Administrator

Table 3: Administration Tool errors

6.2 Console Errors

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

© 2025 HCL Technologies Ltd. All rights reserved.

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

Table 4: Console errors

6.3 REST API Errors

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

Error	Corrective Action	Who
Database connection errors	Verify that the database is running. Verify network connection between the server and the REST client. If the problem persists, contact the BigFix support.	System Administrator
Server connection errors	Verify that the BigFix Server is running. Verify network connection between the server and the REST client. If the problem persists, contact the BigFix support.	System Administrator
Incorrect user or password	Use the correct password and correct Operator name.	MO or NMO
Unable to login	Ask the Master Operator to grant the login permission.	NMO
Password is expired	Ask the Master Operator to reset the Operator password.	NMO
Operator	Ask the Master Operator to grant the missing	NMO

Permission errors	permission.	
Import objects error	The imported object has an invalid format. Use a valid BES object.	MO or NMO
Objects with the same name	An object with the same name already exists. Use a different name.	MO or NMO
REST API syntax errors (xml)	Use the correct REST syntax (error shows the invalid line).	MO or NMO
Invalid REST API options	Use the correct option (error suggests the corrects options or the invalid set).	MO or NMO
Login timeout	Session is expired. Log into the server with Operator name and password.	MO or NMO

Table 5: REST API errors

End of Document

© 2025 HCL Technologies Ltd. All rights reserved.