

BigFix Compliance Analytics Setup Guide



Special notice

Before using this information and the product it supports, read the information in [Notices](#) *(on page 30)*.

Edition notice

This edition applies to version 9.5 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

- Chapter 1. Introduction..... 1**
 - System Requirements..... 2
 - Setup Considerations..... 6
- Chapter 2. Installing Security and Compliance Analytics..... 11**
 - Download HCL BigFix Analytics..... 11
 - Running the installer..... 11
 - Upgrading..... 15
 - Migrating keystores..... 17
 - Performing initial set up and configuration..... 19
 - Configure HTTPS..... 23
 - Configuring LDAP..... 25
 - Log files..... 25
- Appendix A. Support..... 29**
- Notices..... 30

Chapter 1. Introduction

HCL® BigFix Compliance Analytics (previously known as Security and Compliance Analytics or SCA) is a component of HCL® BigFix Compliance, which includes vulnerability detection libraries and technical controls and tools based on industry best practices and standards for endpoint and server security configuration (SCM checklists). The vulnerability detection libraries and the technical controls enable continuous, automated detection and remediation of security configuration issues.

BigFix Compliance Analytics provides report views and tools for managing the vulnerability of SCM checks.

BigFix Compliance Analytics generates the following reports, which can be filtered, sorted, grouped, customized, or exported using any set of BigFix properties:

- Overviews of Compliance Status, Vulnerabilities and History
- Checklists: Compliance Status and History
- Checks: Compliance Status, Values, and History
- Vulnerabilities: Rollup Status and History
- Vulnerability Results: Detailed Status
- Computers: Compliance Status, Values, Vulnerabilities, and History
- Computer Groups: Compliance Status, Vulnerabilities, and History
- Exceptions: Management, Status, and History

New features

The following features and enhancements are included in BigFix Compliance version 1.9.

- Policy feature, which is a collection of checklists for PCI users that allows for aggregation and rollups across multiple checklists. For more information, see the [BigFix Compliance Payment Card Industry \(PCI\) Add-on User's Guide](#).
- Receive e-mail notifications for failed imports and when unexpected changes to target reports occur (which includes disparity in expected number of rows and when the number of rows are updated on a saved report.)

- Lines with lengthy content entries are wrapped on the Grid Report View and on PDF grid reports.
- Use of BigFix Compliance and BigFix Inventory on the same server without any session key conflicts.
- Improved viewing - The Overview page does not display the Vulnerability Overview if there is no report about vulnerability.
- Upgrade to Ruby on Rails version 4.2
- Update of HCL JRE to 8.0.4.10.
- Support of upgrades from earlier versions of Compliance.

System Requirements

Set up your deployment according to the system requirements to successfully deploy BigFix Compliance Analytics.

Configure your BigFix Compliance Analytics deployment according to the following requirements:

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

Components	Requirements
Supported browser versions	<ul style="list-style-type: none"> • Internet Explorer v11.0 • Firefox v31 and later • Firefox Extended Support Release (ESR) 24 and 31 • Google Chrome v35.0 and later • Safari v13.1.1
Supported HCL BigFix component versions	<ul style="list-style-type: none"> • Platform, console, client versions: 9.5, 10.0
BigFix Compliance Analytics server	<ul style="list-style-type: none"> • Microsoft Windows Server 2012 • Microsoft Windows 2012 R2

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

(continued)


Components	Requirements
operating system requirements	<ul style="list-style-type: none"> • Microsoft Windows Server 2016 • Microsoft Windows Server 2019
<p> Note: BigFix Compliance Analytics supports operating systems with the 64-bit versions only.</p>	
BigFix Compliance Analytics data-base server requirements	<ul style="list-style-type: none"> • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 • Microsoft SQL Server 2019
BigFix Compliance Analytics server	You must have Administrator privileges on the target BigFix Compliance Analytics server.
BigFix Compliance Analytics database base	You must have dbcreator permissions on the target BigFix Compliance Analytics database server.
HCL BigFix database user permissions	HCL BigFix database user permissions
SCM mastheads and Fixlet sites	<ul style="list-style-type: none"> • You might have earlier BigFix Fixlets, and custom Fixlets for security compliance in your deployment. These Fixlets continue to function correctly, but only certain Fixlets display within the BigFix Compliance Analytics reports. • To view the current list of SCM checklist sites that are supported with BigFix Compliance Analytics, see the SCM Checklists.

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

(continued)


Components	Requirements
HCL BigFix DB2 database permissions	<p>You must have data administration authority (DATAACCESS) to perform the following tasks:</p> <ul style="list-style-type: none"> • Access to create objects • Access to data within an BigFix DB2 database
HCL BigFix database permissions for datasources	<p>You must have the following MSSQL and DB2 permissions to perform tasks related to datasource.</p>
	<p>MSSQL</p>
	<p> Note: MSSQL requires membership in the sysadmin fixed server role, or ownership of the database (dbo).</p>
	<ul style="list-style-type: none"> • SELECT, EXECUTE • During set up or when upgrading: CREATE SCHEMA, CREATE TABLE, CREATE VIEW, CREATE FUNCTION
	<p>DB2</p>
	<ul style="list-style-type: none"> • DATAACCESS • During set up or when upgrading: DBADM
Server API credentials for PCI DSS policy sites users	<p>Using the PCI DSS policy sites requires providing additional BigFix API user credentials for each datasource that uses PCI. Users must have master operator credentials or must meet the following minimum requirements:</p>

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

(continued)

Components	Requirements
	<ul style="list-style-type: none"> • Can use REST API • Have reader permission for the PCI DSS Reporting site

SQL 2019 support

The tables in this section provide information about the system requirements for BigFix and BigFix Inventory

Table 2. BigFix

Components	Product minimum
Microsoft SQL Server 2019	10.0.2
Windows Server 2019 Datacenter Edition, Essentials Edition, and Standard Edition	10.0.0

Table 3. BigFix Inventory

Components	Product minimum
Microsoft SQL Server 2019 - All editions - Standard, Enterprise, and Express	10.0.5



Note:

- For more information on the SQL 2019 for BigFix support, see https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0087327#win.

BigFix Compliance End of Support (EOS)

BFC Server or BFC Analytics (previously SCA) is a BigFix Compliance application that has a versioning property. BigFix Compliance version is the official marketing version of BigFix Compliance. The BFC application version updates are independent of BigFix Compliance version. However, the EOS date of BFC is same as BigFix Compliance.

The following table lists the EOS date of BigFix Compliance (previously Security and Compliance) and the BFC Servers.

Table 4. End of Support date of BigFix Compliance (previously Security and Compliance) and BFC Server

BigFix Compliance versions	BigFix Compliance Analytics/BFC versions	End of Support date
8.2.x	1.4.x	2016-04-30
9.0.x	1.4.x	2016-04-30
9.1.x	1.5.x	2017-09-30
9.2.x	1.6.x, 1.7.x, 1.8.x	2020-03-31

Table 5. SCA and BES: Support Matrix

BigFix Compliance versions	BigFix Compliance Analytics/BFC versions
9.5.x	1.8.x, 1.9.x, 1.10.x, 2.0.x

Setup Considerations

During setup, match your optimum deployment size to your hardware specifications. Use the suggestions as general guidance to setup BigFix Compliance Analytics.

Consider the requirements of the following servers when you are calculating the data sizing for SCA.

- BigFix Compliance Analytics database server
- BigFix Compliance Analytics application server

Although you can install the BigFix Compliance Analytics server on the same computer as your SQL Server, doing so might affect the performance of the BigFix Compliance Analytics application. Carefully manage the SQL Server memory and if necessary, use a dedicated SQL Server computer.

BigFix Compliance Analytics database server

The size of the BigFix Compliance Analytics database server depends on the following factors.

- The number of computers
- The amount of content that is subscribed onto these computers
- The number of imports that are run

You can add more disk space for future growth of endpoints and more security compliance checks.

- CPU and memory considerations

A minimum of 2 to 3 GHz CPU with 4 GB RAM is sufficient for hosting a BigFix Compliance Analytics database server. The database server would gather analytics data for several hundred BigFix clients. The requirements scale with the number of computers and compliance checks.

It is suggested that you add more RAM for the SQL Server as the deployment environment scales up.

BigFix Compliance Analytics runs on a 64-bit environment with 64-bit JVM. The maximum JVM memory limit is 2 GB physical memory space.

Use the following suggested sizing matrix for your deployment environment.

Table 6. Suggested sizing matrix for SCA deployment environments

Deployment Size (Number of computers)	Data Size	CPU	Memory
1 - 500	0 - 15 GB	quad core	8 GB
500 - 5,000	15 - 25 GB	quad core	8 GB
5,000 - 30,000	25 - 60 GB	quad core	16 GB
30,000 - 100,000	60 - 165 GB	quad core	32 GB
100,000+	165 GB + 1.5 GB for every 1,000 endpoints	2 x quad core	64 GB+



Note: The sizing matrix does not include the database log size. For BigFix Compliance Analytics 1.6, the log size generally requires the same size as the database size.

- Disk space considerations and assumptions

An example deployment size of 30,000 BigFix Clients that are subscribed to SCM contents must take into account the following disk space considerations and assumptions:

- A 60 GB of free disk space is needed by the BigFix Compliance Analytics database server with 30,000 BigFix Clients.
- Add 1.5 GB free disk space for the SCA database server for every 1,000 more clients.
- The disk space suggestions are based on the following assumptions:
 - Your deployment environment has an average of 2,000 SCM checks and 200 SCM checks per computer
 - 2% check result change over each import (daily)
 - 5% of the checks have associated exceptions that are managed in BigFix Compliance Analytics

- 1% of the measured value change over each import (daily)
- All measured value analyses for all checks are activated
- Your deployment contains one year of archived compliance data (365 imports)



Note: Disk space size is affected by the sum of the following key elements:

(Number of check results and their compliance change over time) +
(Number of vulnerability results and their compliance change over time)
+ (Number of measured values change over time) + (Computer Group
* Checks * Number of imports over time) + (Number of exceptions +
Number of Measured Values)

BigFix Compliance Analytics application server

- A minimum of 3 GB of free disk space is needed by the SCA Server. 10 GB of free disk space can be sufficient for up to 250,000 computers.
- A 2 to 3 GHz CPU Quad-cores with 8 GB RAM free memory space to support 30,000 computers.

It is suggested that you have at least 1 GB of available memory space to facilitate PDF generation tasks. Each PDF generation task runs as a separate process and each process takes as much as 150 MB of memory space.

Firewall considerations

- The BigFix Compliance application uses HCL Java to run on top of HCL WebSphere Liberty. The service launches prunsvr.exe, a packaged executable file. By default, the protocol encryption layer and port options are set to TLS 1.0 on port 9081, but you can configure the options during the initial set up.

- You can configure the connection for the report mailing feature. The application must be able to contact the mail server.
- The PDF export functionality uses pdf.exe, an external executable file that is packaged with the application. This executable file does not make any outside connections.

Chapter 2. Installing Security and Compliance Analytics

Before installing Security and Compliance Analytics, ensure that your system meets all prerequisites as described in [Systems Requirements \(on page 2\)](#).

Install and configure HCL BigFix Analytics by completing the following steps:

- Install by using the `InstallAnywhere` installer.
- Perform initial configuration by using the web interface.

Upgrading from an earlier version requires updating the data schema as well. To do this, the operator must access the Security and Compliance Analytics web interface from the server hosting Security and Compliance Analytics. Click **Upgrade Schema**.



Note: It is strongly recommended, especially in big environments, to first perform an upgrade in the test environment. To do this, back up your production database, restore it on the test server, and perform the upgrade there. If it is successful, perform the upgrade on the production server.

Download HCL BigFix Analytics

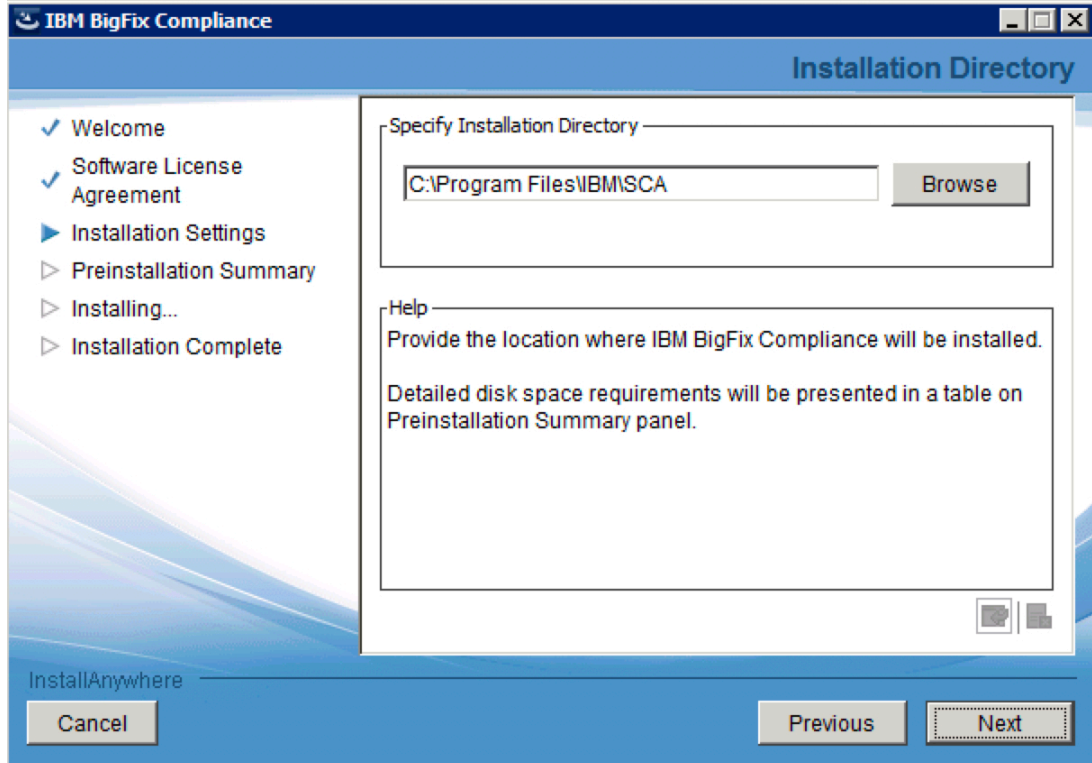
To download BigFix Compliance Analytics, perform the following steps:

1. In the HCL BigFix console, add the SCM Reporting masthead.
2. In the Security Configuration domain in the console, open the Configuration Management navigation tree. Click the **HCL BigFix Compliance 1.9 First-time Install** Fixlet under the **HCL BigFix Compliance Install/Upgrade** menu tree item.
3. Take the associated action and follow the installation steps in the description of the Fixlet.

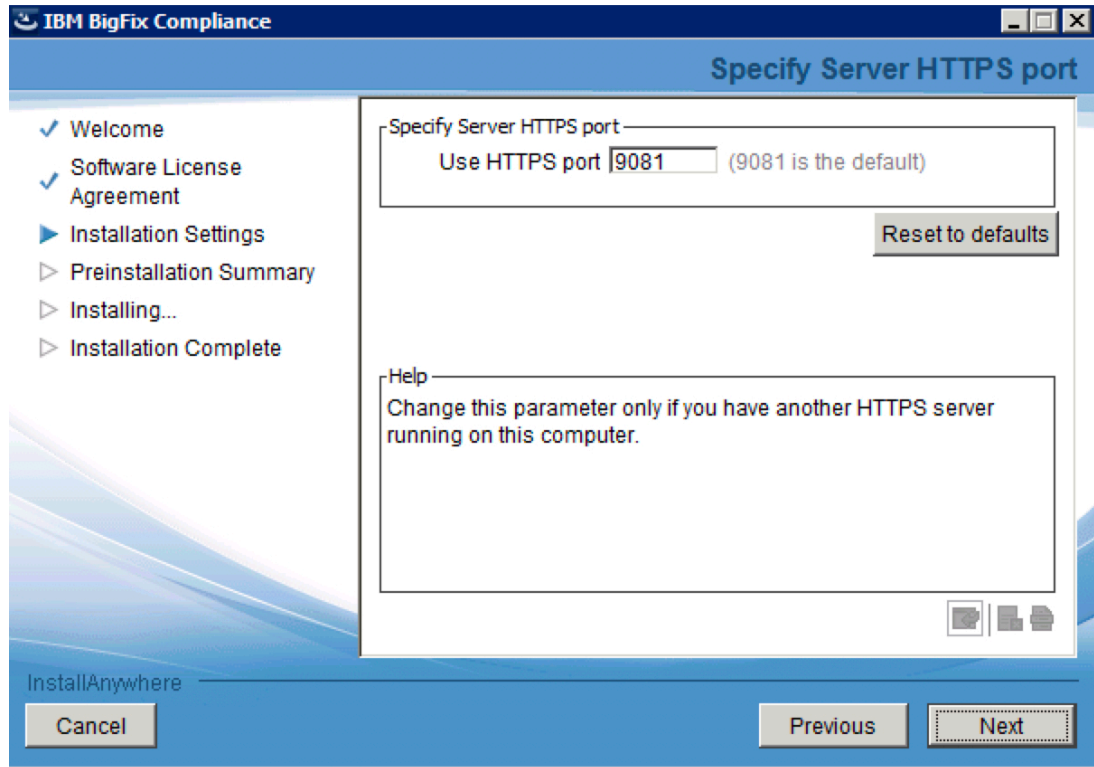
Running the installer

Follow these steps to install BigFix Compliance Analytics.

1. Run the installer executable file. When you are prompted, extract the installer file to a folder.
2. Run tema-windows-x86_64.exe from within the folder to begin the installation.
3. You can change the installation path and port during installation.
 - a. Installation path

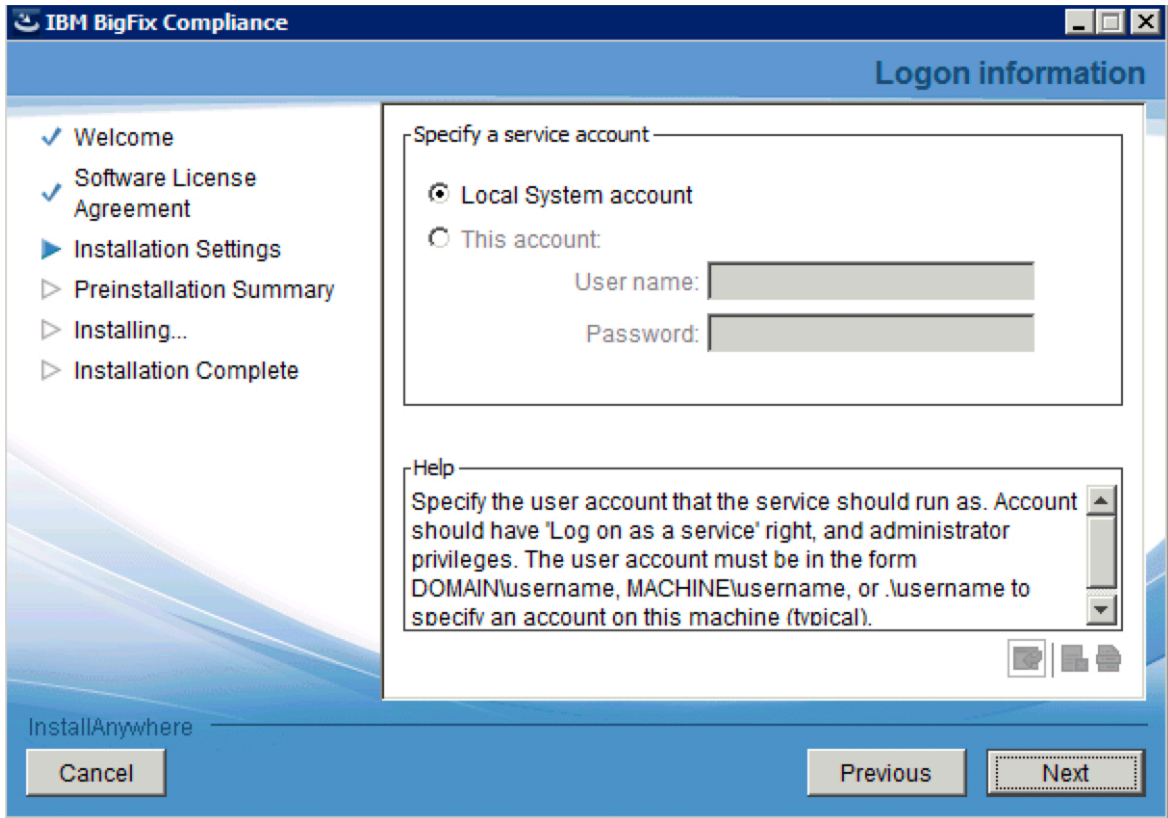


- b. TCP port

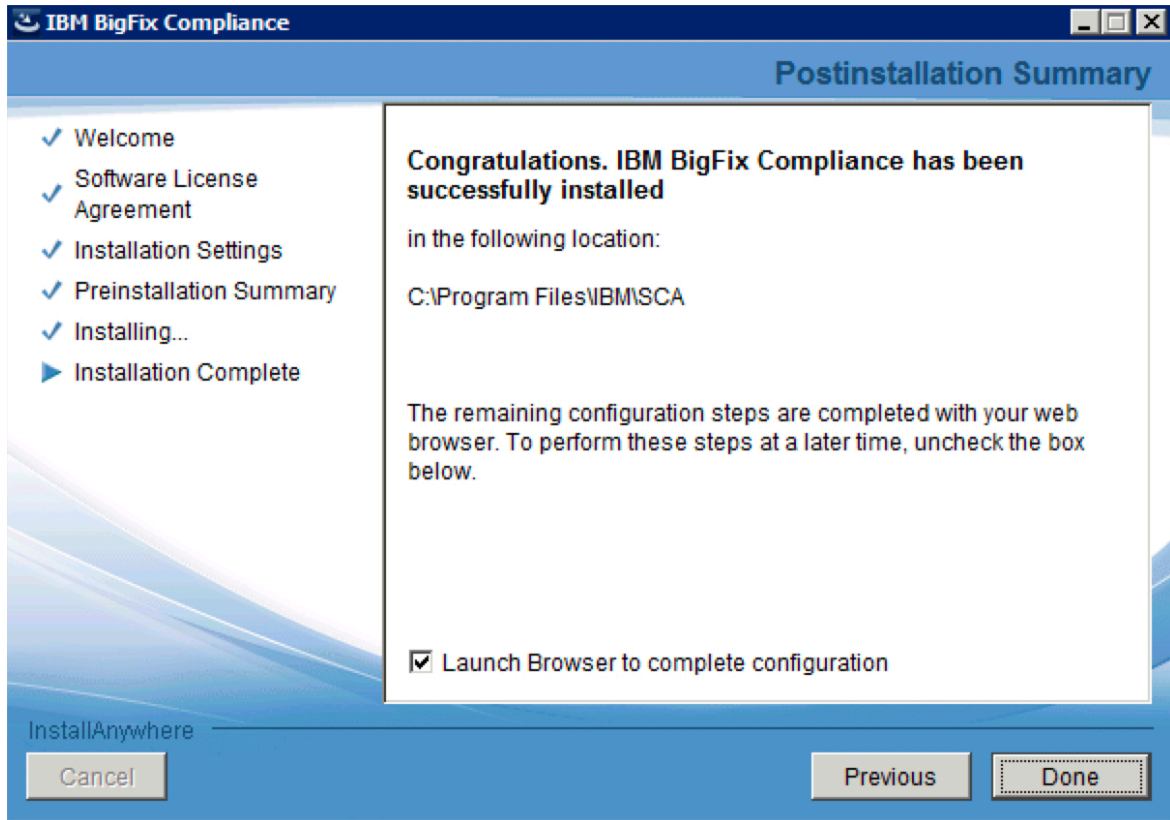


Note: BigFix Compliance Analytics uses HTTPS by default from version 1.6 and later.

4. Specify the user account that runs the HCL BigFix Analytics service. If you configure HCL BigFix Analytics to connect to the SQL Server through a user that is authenticated through Windows, the HCL BigFix Analytics service must be configured to run as that same user.



5. When the installation is completed, use the web interface to complete the setup of the HCL BigFix Analytics server.
6. The final window of the installer prompts you to launch a web browser to complete the setup. Click **Done**.



The BigFix Compliance Analytics web server may take a while to fully load. Allow time for the server to initialize.

While the server is loading or during the database configuration, you might receive a message stating Not Found. This is expected. The page automatically reloads when it is ready.

Not Found

Please wait while the application finishes loading...

Upgrading

Updating from an earlier version requires updating the data schema as well. The operator must access the BigFix Compliance Analytics web interface from the server hosting BigFix Compliance Analytics. Click **Upgrade Schema**.



Note:

Before you start the upgrade process, it is strongly recommended that you perform server and database back-up.

When upgrading from earlier versions of BigFix Compliance Analytics, the installer replaces the previously supplied server certificate and private key pair with a new self-signed certificate and key pair.



Note: BigFix Compliance version 1.5.78 is the minimum version required to upgrade to BigFix Compliance 1.8 and BigFix Compliance 1.9. Refer to the following table for the upgrade steps required for the different BigFix Compliance Analytics version.

Table 7. Upgrade steps for BigFix Compliance Analytics versions

If you're in version	Follow these upgrade steps:
1.5.78 or earlier	1. Upgrade to version 1.5.78 2. Upgrade to version 1.7 or 1.8 3. Upgrade to version 1.9
1.6.139 or earlier	Upgrade to 1.7 or 1.8, then upgrade to 1.9

BigFix Compliance Analytics 1.6 and later uses HCL WebSphere. Earlier versions use Jetty as an application server.

To upgrade from earlier versions of BigFix Compliance Analytics, you must configure your SSL certificate settings again. To apply the settings again, go to **Management > Server Settings** when installation is completed.

1. Click **Replace** in the Certificate section.
2. Click **Browse...** and select your server certificate and private key.
3. Enter the private key password.
4. Click **Save** and restart BigFix Compliance Analytics.

If the original certificate and key pair are difficult to get or are unavailable, follow the steps in [Migrating Keystores \(on page 17\)](#).

Migrating keystores

Follow these steps to migrate keystores in BigFix Compliance Analytics. A keystore is a database file that stores security certificates, such as authorization or public key certificates.

The BigFix Compliance Analytics installer will save the following files for your reference under `<TEMA_ROOT>\wlp\usr\servers \server1\resources\security\`.

- Under `<TEMA_ROOT>\wlp\usr\servers \server1\resources\security\`, a copy of your original keystore file
- Under `<TEMA_ROOT>\wlp\usr\servers \server1\config\`
 - A copy of your original jetty.xml file
 - The keystore password in deobfuscated_password file

Migrating keystores require the following:

- Java Runtime Environment (installed in `<TEMA_ROOT>\jre\bin\`)
- The original keystore file
- The deobfuscated_password file
- Command prompt (Windows) with appropriate PATH set

1. Convert the keystore from JKS to PKCS12 format.

Table 8. Example command line of converting the keystore format from JKS to PKCS12

Command line example

```
> keytool -importkeystore -srckeystore keystore
-srcstoretype jks -srcstorepass <password_string>
-srckeypass <password_string> -destkeystore
keystore.p12 -deststoretype pkcs12 -deststorepass
<key_pass> -destkeypass <key_pass> -alias 1
```

Reference

- Input file: `keystore`
- Output file: `keystore.p12`
- `<password_string>`: The password string saved in the `deobfuscated_password` file
- `key_pass`: The new password of your choice for `keystore.p12`. The password must be a minimum of 6 characters.

2. Convert the PKCS12 format keystore into PEM format certificate and key using OpenSSL.

Table 9. Example command line of converting the keystore format from PKCS12 to PEM

Command line example

```
> openssl pkcs12 -in keystore.p12 -out key-
store.pem
```

Reference

- Input file: `key-store.p12`
- Output file: `key-store.pem`

You will be prompted to enter the following passwords:

- Password (Import password) for `keystore.p12`
 - New password of your choice for the private key. The password must be a minimum of 4 characters.
3. Open the PEM encoded certificate and key (`keystore.pem`). Save it as certificate and a private key file.
 - a. The file `keystore.pem` contains both the certificate and private key in sections.
 - b. Copy then save the following section `server.crt`.

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
-----END CERTIFICATE-----
```

c. Copy then save the following section as server.key.

```
-----BEGIN RSA PRIVATE KEY-----
```

```
...
```

```
-----END RSA PRIVATE KEY-----
```

4. Go to **Management > Server Settings**.

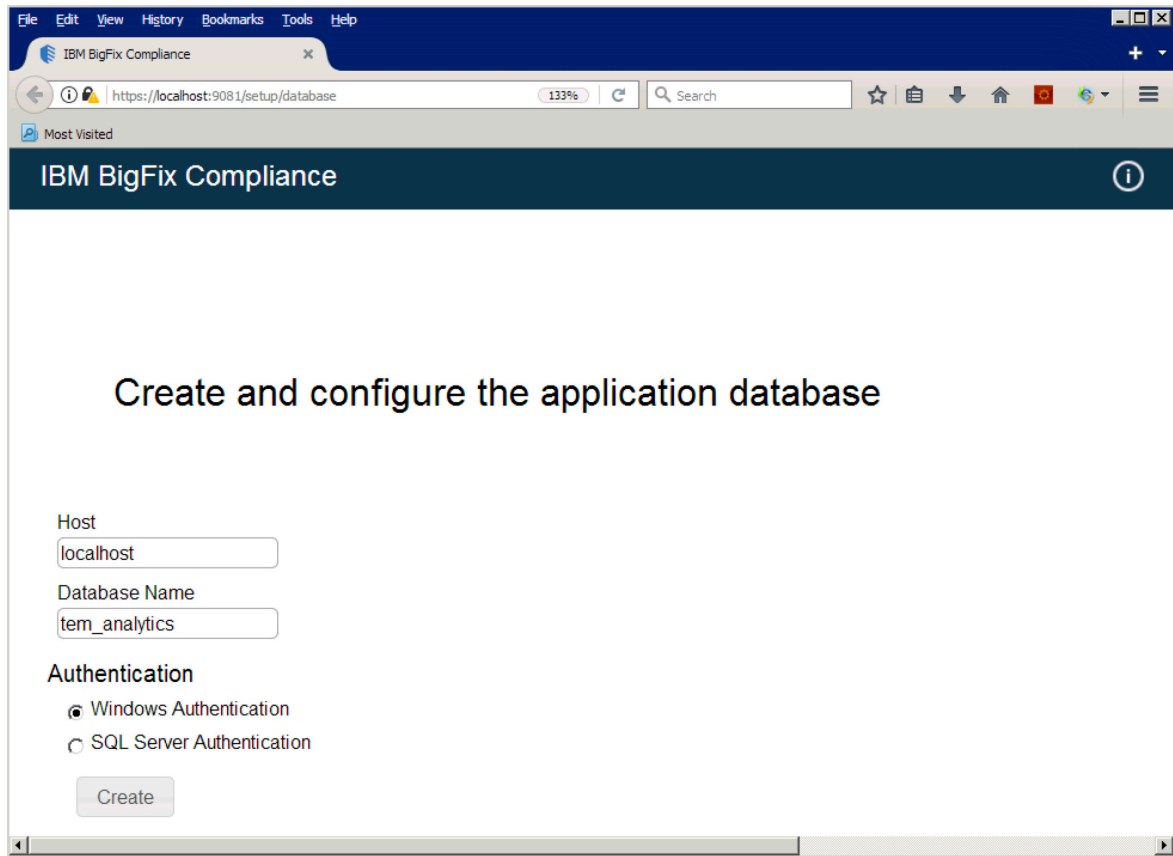
Apply the following in BigFix Compliance Analytics.

- certificate (server.crt)
- key pair (server.key)
- password (PEM pass phrase entered in Step 2.)

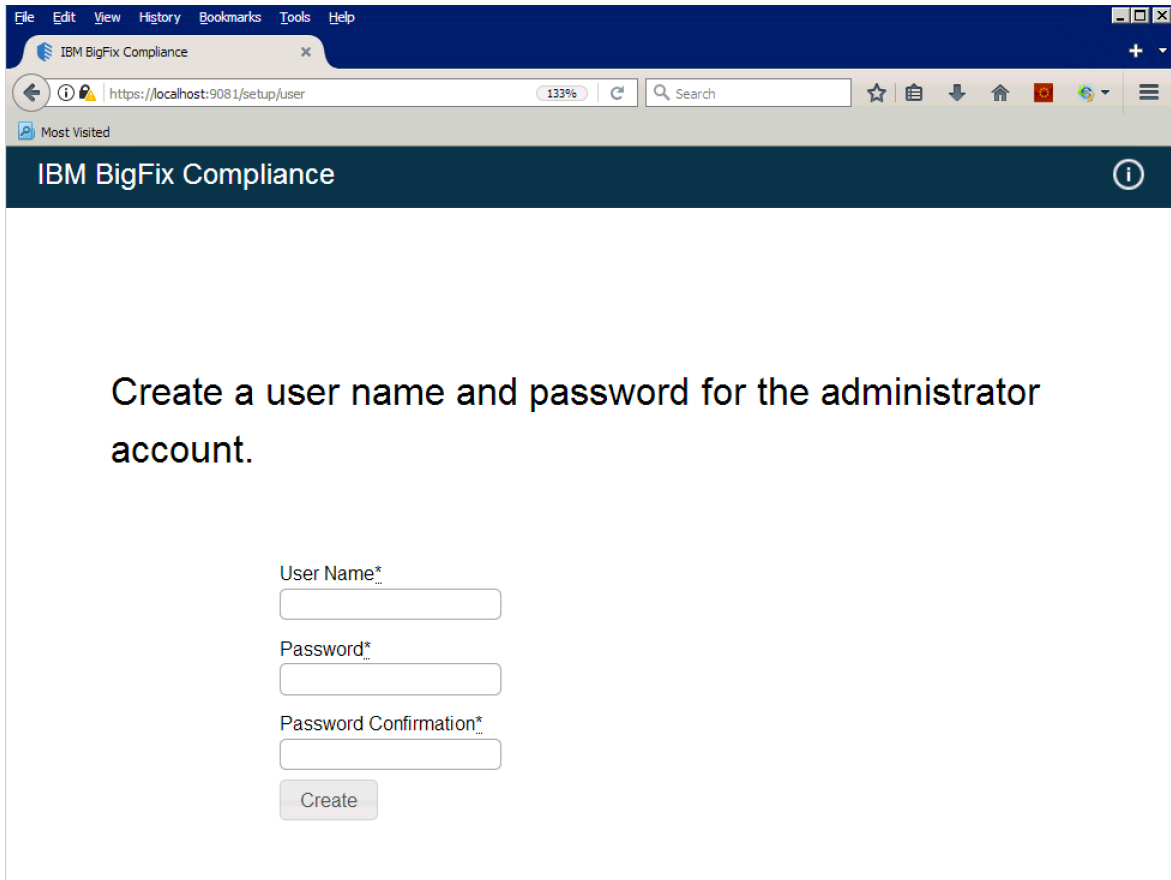
Performing initial set up and configuration

To set up the database connection, perform the following steps:

1. Enter the host and database name fields.
2. Select a type of authentication.
3. Click **Create** to create a new administrative user.



4. In the next screen, enter a username and password for the new administrator account. Click **Create**.



The screenshot shows a web browser window with the URL `https://localhost:9081/setup/user`. The page title is "IBM BigFix Compliance". The main content area contains the following text and form:

Create a user name and password for the administrator account.

User Name*

Password*

Password Confirmation*

5. Connect to your HCL Enterprise Manager database. Enter the host, database name, and authentication method for your primary HCL BigFix database. Click **Create**.
6. Configure the connection to the BigFix server. The host name or IP address and the server API Port number are automatically retrieved from the database. Specify only the administrative user that you created during the installation of BigFix.

IBM BigFix Server

Host

Server API Port

52311 is default

Authentication (Console Operator)

User Name

Password

The advanced policy functionality is currently used only for PCI content. To enable the advanced policy functionality, you must provide the credentials for a BigFix console operator. It is recommended that this is a master operator, but at the minimum, the console operator must meet the following permissions:

- Can use REST API
- Have reader permission for the PCI DSS Reporting site

If you do not use this feature, you may leave these fields blank.

You can also set up a Web Reports database in the fields on the right side of the window.

Provide the connection parameters to the databases and the IBM BigFix server

The application connects to the IBM BigFix server database to regularly import scan data. It connects to the IBM BigFix server to run remote operations that automate the infrastructure management. The application can also connect to the Web Reports database to enable Web Reports users to access the application (optional). The information that you provide on this panel is used to create a data source. You can configure additional data sources at a later time.

Name*
Data Source

Database for the IBM BigFix Server*

Database Type*
SQL Server

Host*
localhost

Database Name*
BFEnterprise

Authentication

Windows Authentication
 SQL Server Authentication

IBM BigFix Server

Host
[]

Server API Port
52311 is default

Authentication (Console Operator)

User Name
[]

Password
[]

Web Reports Database

Database Type
SQL Server

Host
[]

Database Name
[]

Authentication

Windows Authentication
 SQL Server Authentication

Create

Configure HTTPS

HCL BigFix Compliance Analytics administrators can configure SSL and the TCP ports from the **Management > Server Settings** section of the web interface. When turning on SSL, you can provide a pre-existing private key and certificate or have the system automatically generate a certificate. If you change the port or SSL settings, you must restart the service for the changes to take effect.

If you generate a certificate, you must specify a certificate subject *common name*. The common name must correspond to the DNS name of the HCL Endpoint Manager Analytics server.

IBM BigFix Compliance
Home Reports ▾ Management ▾ ⓘ 👤

Management: Server Settings

Server Settings

Port*

Use SSL

Use TLSv1.2 (your browser must have TLSv1.2 enabled). TLSv1.2 is required for NIST SP800-131 compliance.

Certificate [cancel](#)

Import a PEM encoded private key and certificate

Generate a self-signed certificate

Certificate* No file chosen

Private key* No file chosen

Private key password

For changes to the port, the SSL, or certificate settings to take effect, restart the application server. Changes to the data retention settings take effect immediately after saving.

Additional Options

This runs a specialized import that performs a complete re-fetch from the data sources. This may help resolve issues with repeated import failures or inconsistent report data.

If you provide a pre-existing private key and certificate, they must be PEM-encoded. If your private key is protected with a password, you must enter it in the *Private key password* field.

IBM BigFix Compliance
Home Reports ▾ Management ▾
i 👤

Management: Server Settings

Server Settings

Port*

Use SSL

Use TLSv1.2 (your browser must have TLSv1.2 enabled). TLSv1.2 is required for NIST SP800-131 compliance.

Certificate [cancel](#)

Import a PEM encoded private key and certificate

Generate a self-signed certificate

Common name*

Expiration Date*

For changes to the port, the SSL, or certificate settings to take effect, restart the application server. Changes to the data retention settings take effect immediately after saving.

Additional Options

This runs a specialized import that performs a complete re-fetch from the data sources. This may help resolve issues with repeated import failures or inconsistent report data.

Configuring LDAP

HCL BigFix for BigFix Compliance Analytics 1.9 supports authentication through the Lightweight Directory Access Protocol (LDAP) server. You can add LDAP associations to HCL BigFix Analytics so you and other users can log in using credentials based on your existing authentication scheme.

For more information about LDAP and user provisioning, see the Compliance User Guide.

Log files

This section describes how to access log files and the options associated with BigFix Compliance Analytics.

The server log (`tema.log`) saves all the actions related to the server, whereas the import log saves import date and time from BigFix server to BigFix Compliance. These log files are mainly used for following operations:

- Troubleshooting.
- Auditing.
- Inspecting import date and time.
- Error analysis.

By default, the log files are stored in the path: `C:\Program Files\BigFix Enterprise\SCA\wlp\usr\servers\server1\logs\`.

Server log

The server log file `tema.log` also contains the backup.

When a BigFix Compliance service is restarted a backup of `tema.log` is created. The backup file is named as `tema_<yy.mm.dd_hh.mm.ss.0>.log`.



Note: The time stamp (yy.mm.dd_hh.mm.ss) in the backup file is the local time (for example, PST) at which time the BigFix Compliance service was restarted.

With some exceptions, most of the time stamp entries are in UTC time zone.

Import log

An import is created when you run an import. Import log files are stored within the import subfolders. Import logs are named as `<yyyy_mm_dd-hh_mm_ss>-<import id>.log`.



Note: The time stamp (yy.mm.dd_hh.mm.ss) in the import files are in UTC time zone.

To view the log in local time, go to **Management > Data Imports page**. The Start Time column shows the local time of the import.

Options in log files

Using the following options, you can turn on/off various properties of the log files. When you modify any of the properties BigFix Compliance services must be restarted.

By default, the `jvm.options` file is stored under the path: `C:\Program Files\BigFix Enterprise\SCA\wlp\usr\servers\server1.`

Turn on/off debug log

When enabled, this applies to both `tema.log` and import log files. Access the `jvm.options` file and edit the file with the following line:

```
#-DTEMA_LOG_DEBUG=true
```

Use the following line to turn on/off the debug log:

- `-DTEMA_LOG_DEBUG=true`: Turn on log service memory.
- `#-DTEMA_LOG_DEBUG=true`: Turn off log service memory.



Important: Make sure that you do not change true/false.

Turn on/off debug log using Fixlets

Use the fixlets to turn on/off the debug logging under SCM Reporting site.

- ID 1006: Turn on Debug Logging - BigFix Compliance Server.
- ID 1007: Turn off Debug Logging - BigFix Compliance Server.

Log service memory

When enabled, this applies to both `tema.log` and import log files. BigFix Compliance server memory usage can be turned on/off with help of the `jvm.options` file.

Access the `jvm.options` file and edit the file with the following line:

```
-DLOG_MEMORY=true
```

Use the following line to turn on/off the log service memory:

- `-DLOG_MEMORY=true`: Turn on log service memory
- `#-DLOG_MEMORY=true`: Turn off log service memory



Important: Make sure that you do not change true/false.

Appendix A. Support

For more information about this product, see the following resources:

- [Knowledge Center](#)
- [BigFix Support Center](#)
- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Wiki](#)
- [HCL BigFix Forum](#)

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or

any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.