

**BigFix Compliance
Analytics Setup Guide**



Special notice

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

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

- Chapter 1. Introduction..... 5**
 - System Requirements 5
 - Setup Considerations..... 8
- Chapter 2. Installing BigFix Compliance Analytics..... 11**
 - Download BigFix Compliance Analytics..... 11
 - Running the Installer..... 12
 - Upgrading..... 15
 - Migrating Keystores..... 17
 - Performing initial set up and configuration..... 18
 - Configure HTTPS..... 21
 - Configuring LDAP..... 22
 - Updating National Vulnerability Database Data Feeds..... 22
 - Log files..... 23
- Chapter 3. Uninstalling..... 26**
 - Uninstalling the server in interactive mode..... 26
- Chapter 4. Configuring report definitions using REST API..... 27**
- Chapter 5. Disaster recovery for BigFix Compliance Analytics..... 28**
 - Creating a backup of the application server..... 28
 - Recovering the backup application server..... 28
 - Verifying the success of the recovery procedure..... 29
- Appendix A. Support..... 30**
- Notices..... xxxi

Chapter 1. Introduction

BigFix Compliance Analytics is a component of BigFix Compliance, that aggregates and reports on the compliance statuses of all endpoints against deployed policies that are continually collected, aggregated, and reported using a powerful Compliance Analytics engine, database and user interface.

BigFix Compliance Analytics is a component of BigFix Compliance, that includes technical controls and tools that are based on industry practices and standards for endpoint and server security configuration.

The compliance statuses of all endpoints against deployed policies are continually collected, aggregated, and reported using a powerful Compliance Analytics engine, database and user interface in BigFix Compliance. Various compliance reports, showing both current status and historical trend for the entire deployment or individual endpoint, provide comprehensive analytics to meet the various needs of security, IT operation, or compliance teams. With BigFix Compliance Analytics, you can track the effectiveness of the compliance efforts and quickly identify security exposures and risks.

BigFix Compliance Analytics provides consistent report across three security domains:

- Security Configuration Reporting
- Patch Reporting
- Vulnerability Reporting

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, 11.0

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

(continued)





Components	Requirements
BigFix Compliance Analytics server operating system requirements	<ul style="list-style-type: none"> • Microsoft Windows Server 2012 • Microsoft Windows 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2022 <p data-bbox="573 659 1390 701"> Note: Microsoft Windows Server 2022 is supported from version 2.0.10.</p> <p data-bbox="493 768 1377 848"> Note: BigFix Compliance Analytics supports operating systems with the 64-bit versions only.</p>
BigFix Compliance Analytics database server requirements	<ul style="list-style-type: none"> • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 • Microsoft SQL Server 2019 • Microsoft SQL Server 2022 • SCA 2.0.10 and later versions utilize the SPLIT_STRING function, which is not available in SQL Server 2012/2014 versions and needs to be added manually. Refer to the BigFix Forum for more details • Ensure that the SQL Server has a compatibility level set to 130 or higher before performing an upgrade or the first import <p data-bbox="573 1388 1338 1430"> Note: Microsoft SQL Server 2022 is supported from version 2.0.10.</p>
BigFix Compliance Analytics server	You must have Administrator privileges on the target BigFix Compliance Analytics server.
BigFix Compliance Analytics database	You must have dbcreator permissions on the target BigFix Compliance Analytics database server.
HCL BigFix database user permissions	HCL BigFix database user permissions

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

(continued)

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

BigFix Compliance End of Support (EOS)

BFC Server 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 2. 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 3. BFC Analytics 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
10.0.x	1.9.x, 1.10.x, 2.0.x
11.0.x	2.0.x

Setup Considerations

When configuring your system, ensure that your ideal deployment size aligns with your hardware specifications. Utilize the provided recommendations as general guidance to effectively set up BigFix Compliance Analytics for optimal performance.

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

- 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 8 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.

Use the following suggested sizing matrix for your deployment environment.

Table 4. Suggested sizing matrix for BigFix Compliance Analytics 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, 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 BigFix Compliance Analytics 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 BigFix Compliance Analytics 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 IBM Java to run on top of IBM 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 BigFix Compliance Analytics

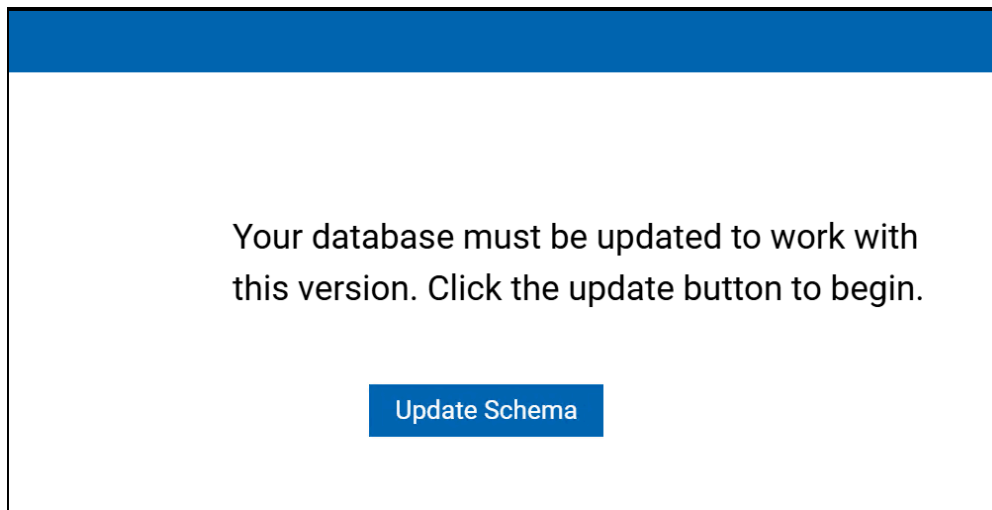
Follow this comprehensive guide to successfully deploy and configure the BigFix Compliance for optimal performance and data insights.

Before installing BigFix Compliance Analytics, ensure that your system meets all prerequisites as described in [Systems Requirements \(on page 5\)](#). 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.

When upgrading from an earlier version, you also need to update the data schema. To do this, the operator should log in to the Security and Compliance Analytics web interface on the server that hosts Security and Compliance Analytics. Then, click **Upgrade Schema**.

Figure 1. Upgrade Schema



Note: It is highly recommended, especially in large environments, to first test the upgrade in a test environment. To do this, back up your production database, restore it on the test server, and perform the upgrade there. If the upgrade is successful, you can then proceed to upgrade the production server.

Download BigFix Compliance Analytics

You can download BigFix Compliance Analytics by completing the following steps:

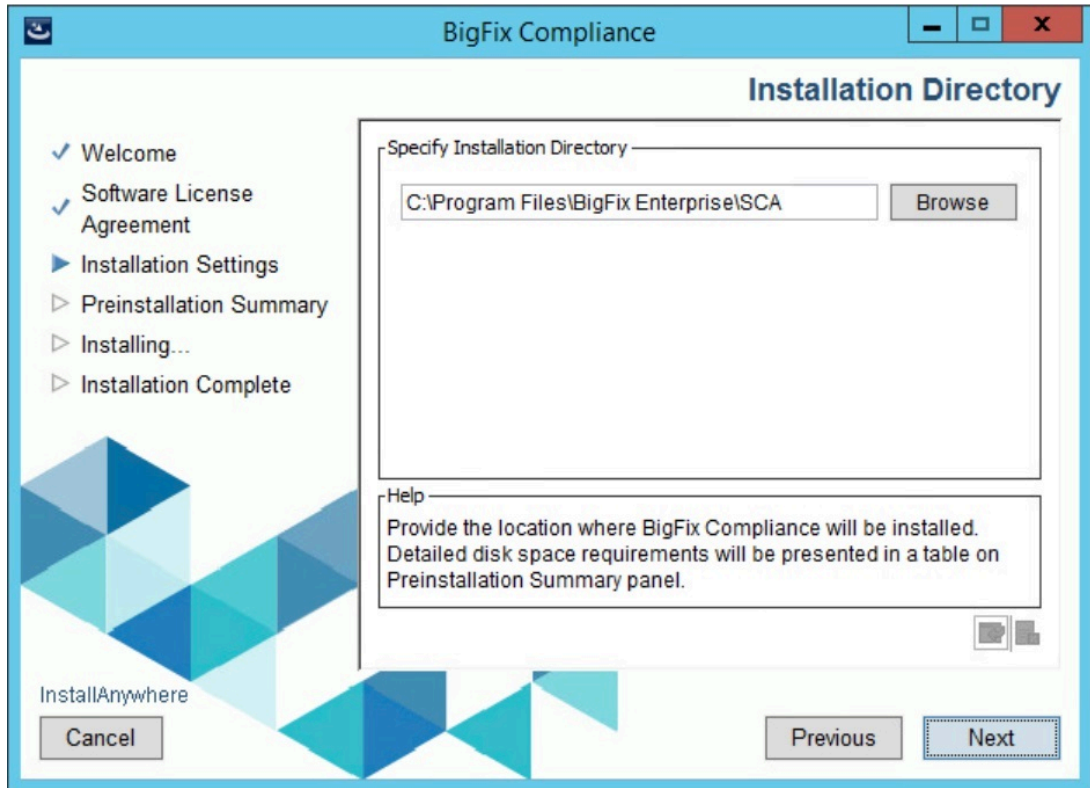
1. In the BigFix console, enable the SCM Reporting site from the License Overview dashboard.
2. In the Security Configuration domain in the console, open the Configuration Management navigation tree. Click the **BigFix Compliance Server 2.0 - First time Install** Fixlet under the **BigFix Compliance Install/Upgrade** menu tree item.
3. Take the associated action and follow the installation steps in the description of the Fixlet.

Running the Installer

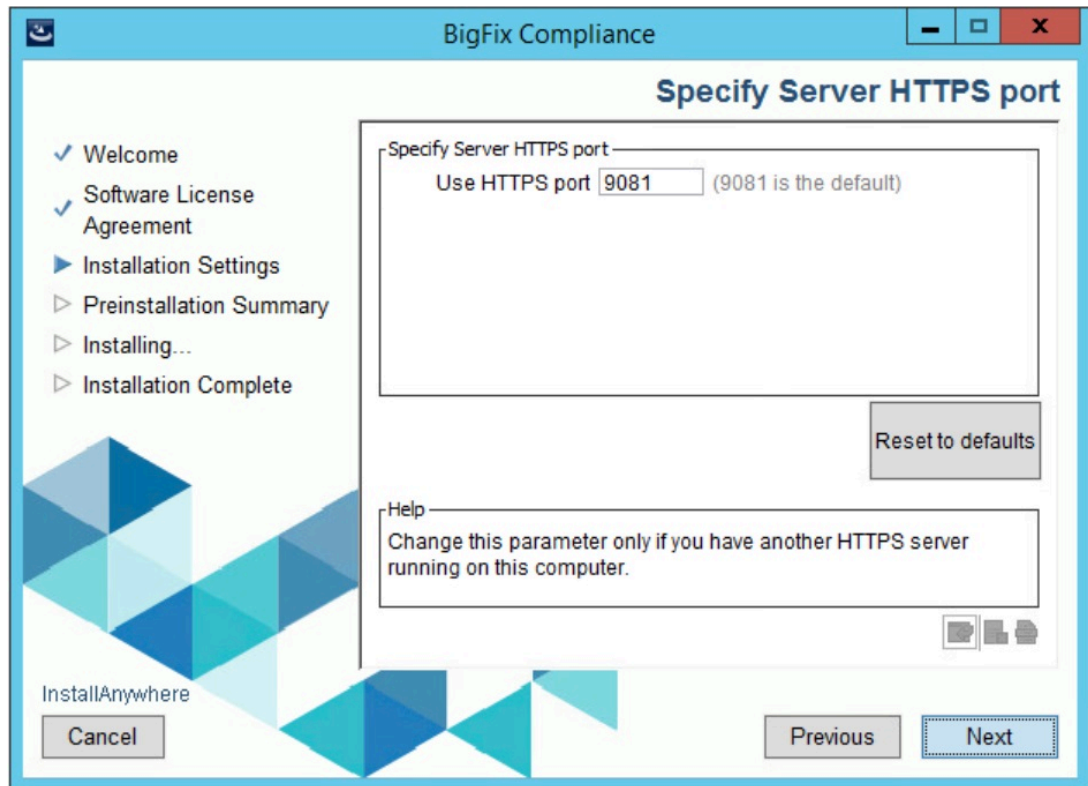
Follow these steps to install BigFix Compliance Analytics.


1. Run the installer executable file as administrator. When you are prompted, extract the installer file to a folder. If you cannot run the installer from the folder, copy the installer outside the folder and run the file.
2. Run bfc-server.exe from within the folder to begin the installation.
3. You can change the installation path and port during installation.

a. Installation path

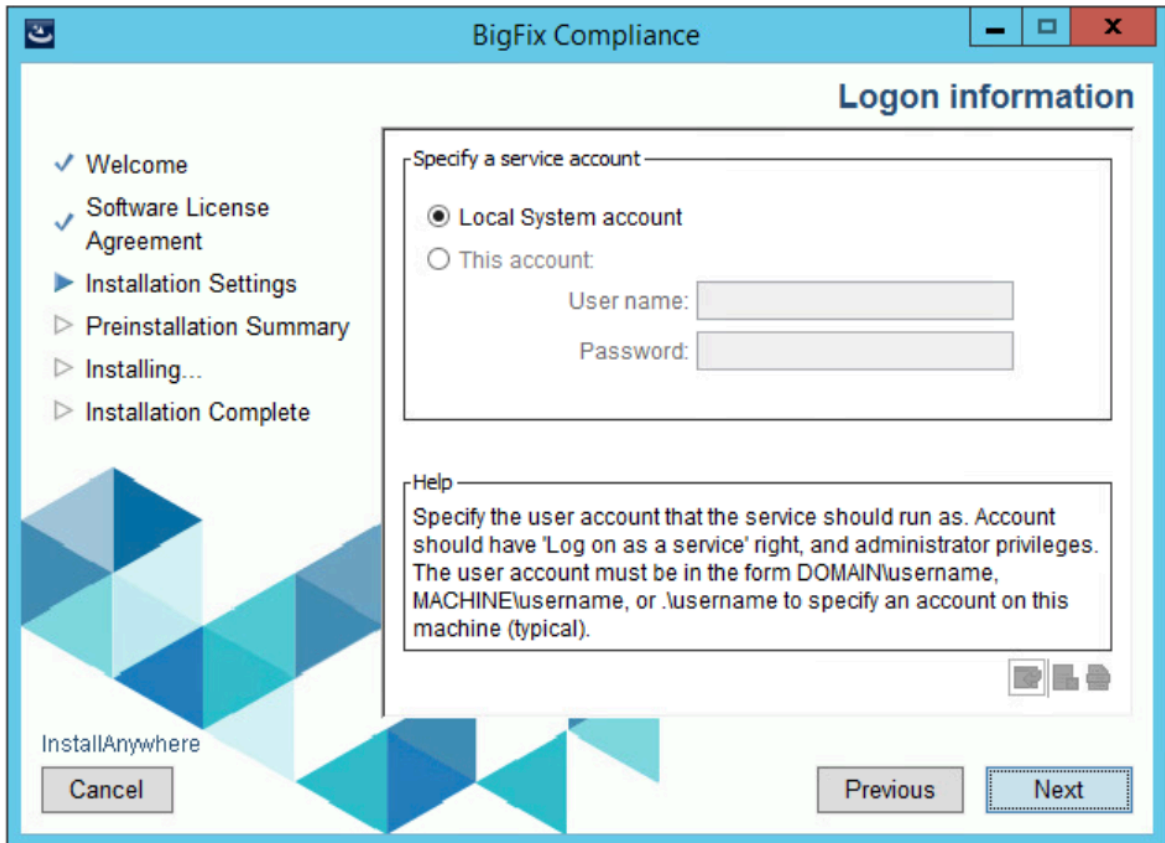


b. TCP port

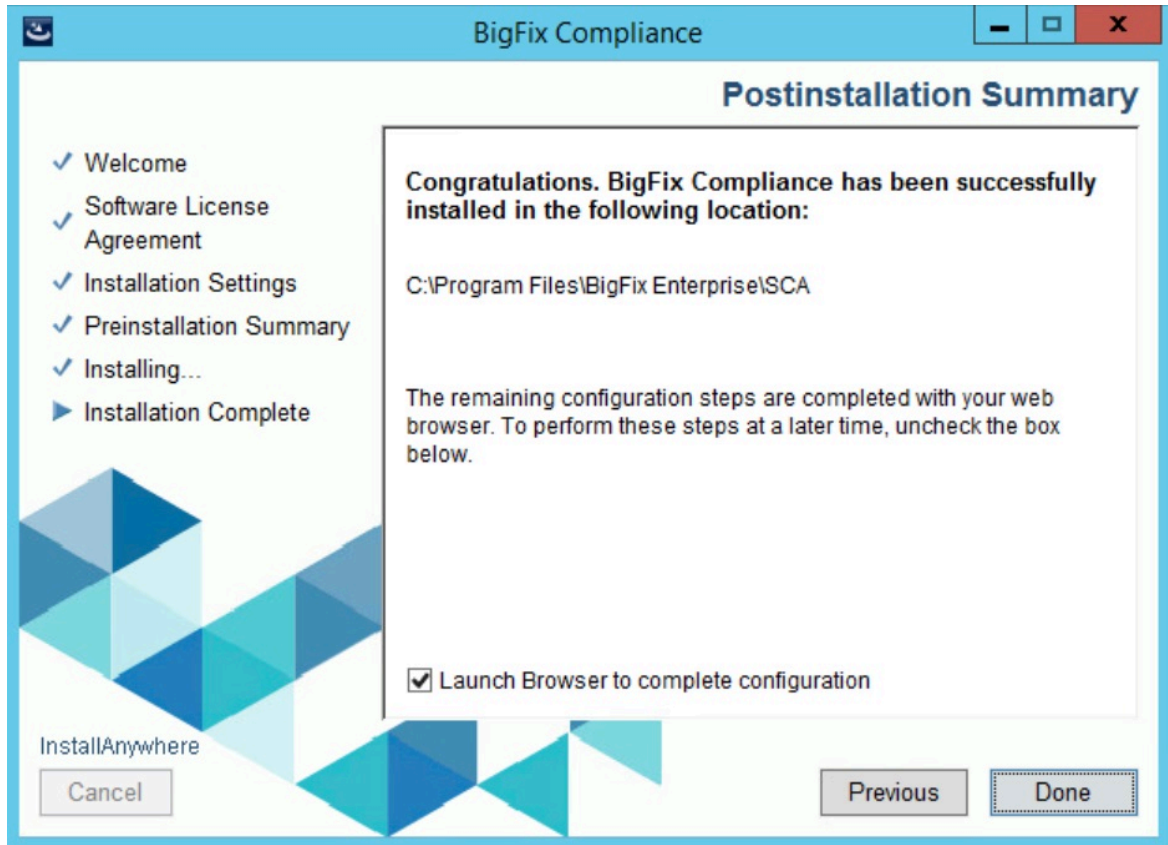


 **Note:** BigFix Compliance Analytics uses HTTPS by default.

- Specify the user account that runs the BigFix Compliance 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

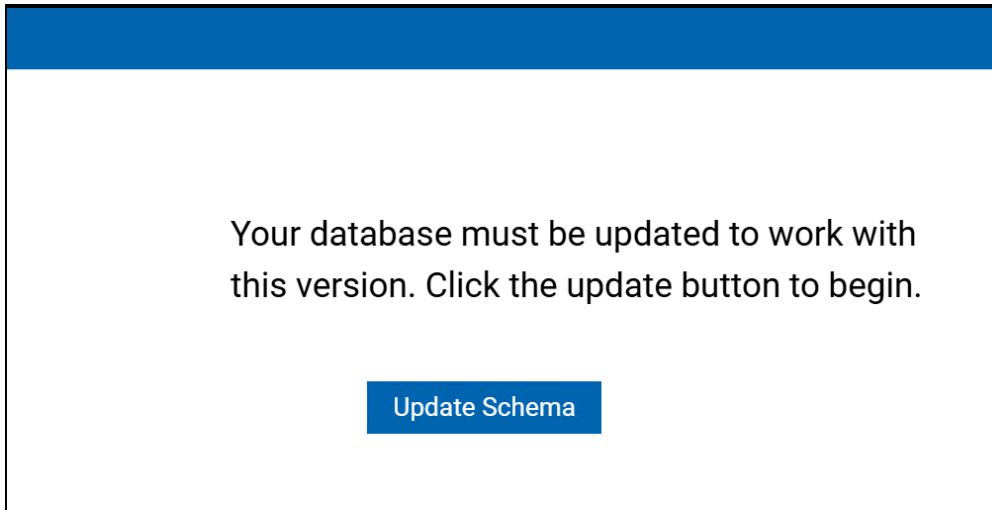
Please wait while the application finishes loading...

Upgrading

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.

When upgrading from an earlier version, you also need to update the data schema. To do this, the operator should log in to the Security and Compliance Analytics web interface on the server that hosts Security and Compliance Analytics. Then, click **Upgrade Schema**.

Figure 2. Upgrade Schema

**Note:**

- Before you start the upgrade process, it is strongly recommended that you perform server and database back-up.
- You must manually change the Java Heap size to 4GB (or comment out the current java heap size default of 4GB from the `jvm.options` file under the path: `C:\Program Files\IBM\SCA\wlp\usr\servers \server1`) for Upgrade fixlet to upgrade the existing v1.9.x and v1.10.x to 2.0.4.x deployment.
- Even after the upgrade, it is recommended to change the Java Heap size to 8GB in `jvm.options` file under the path: `C:\Program Files\IBM\SCA\wlp\usr\servers \server1`.
- A fixlet *Warning: Low Heap Size Setting - Bigfix Compliance Server* is introduced to help you check the heap size before you start using the Upgrade fixlet.
- Restart the BigFix Compliance from BigFix Services.

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 `<BFC_ROOT>\wlp\usr\servers\server1\resources\security\`.

- Under `<BFC_ROOT>\wlp\usr\servers\server1\resources\security\`, a copy of your original keystore file
- Under `<BFC_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 `<BFC_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 5. Example command line of converting the keystore format from JKS to PKCS12

Command line example	Reference
<pre>> keytool -importkeystore -srckeystore keystore -srckeystore.jks -srckeypass <password_string> -destkeystore keystore.p12 -destkeypass <key_pass> -alias 1</pre>	<ul style="list-style-type: none"> ◦ Input file: <code>keystore</code> ◦ Output file: <code>keystore.p12</code> ◦ <code><password_string></code>: The password string saved in the deobfuscated_password file ◦ <code>key_pass</code>: The new password of your choice for <code>keystore.p12</code>. The password must be a minimum of 6 characters.

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

Table 6. Example command line of converting the keystore format from PKCS12 to PEM

Command line example	Reference
<pre>> openssl pkcs12 -in keystore.p12 -out keystore.pem</pre>	<ul style="list-style-type: none"> ◦ Input file: <code>keystore.p12</code> ◦ Output file: <code>keystore.pem</code>

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**.

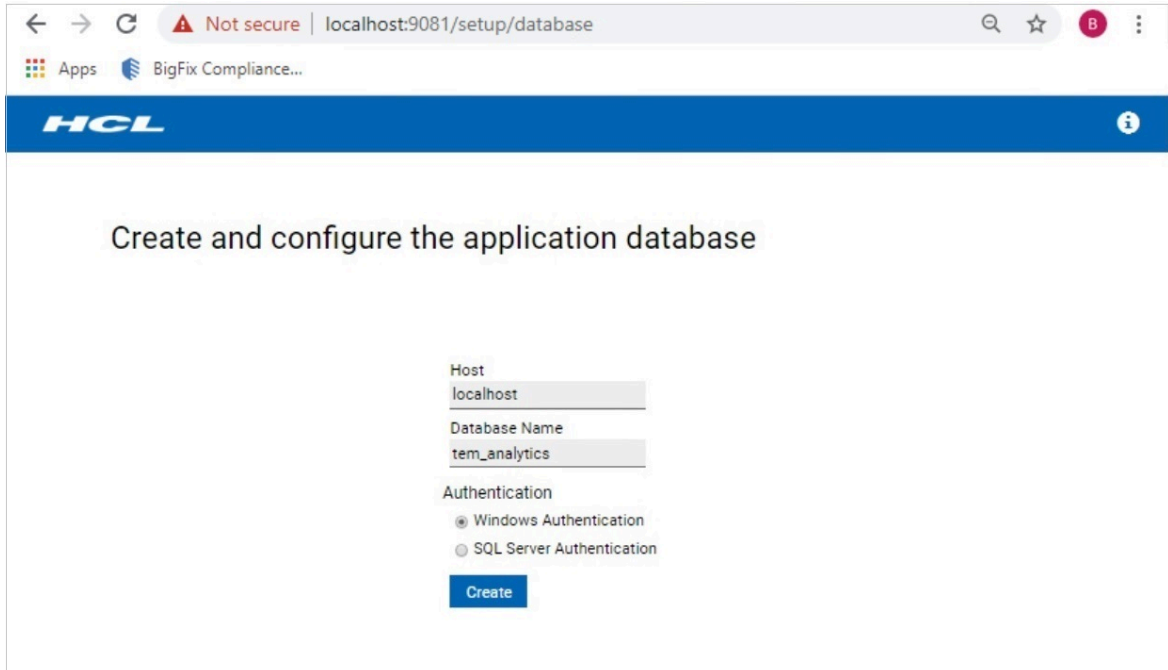
Apply the following in BigFix Compliance Analytics.

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

Performing initial set up and configuration

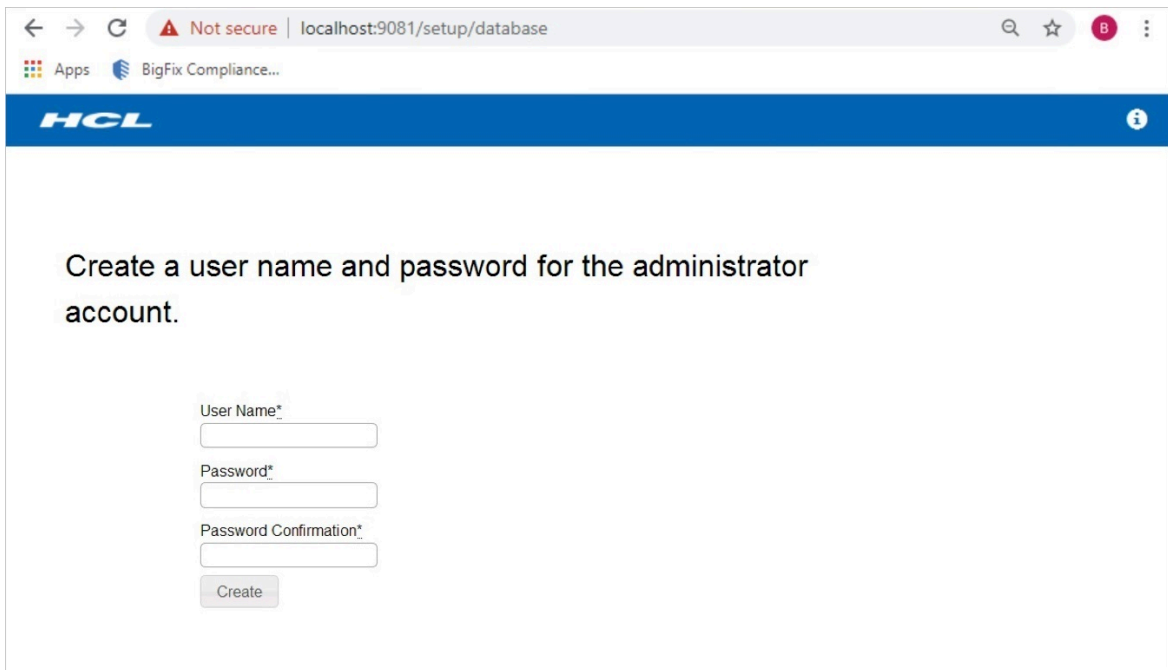
To set up the database connection, perform the following steps:

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



The screenshot shows a web browser window with the URL `localhost:9081/setup/database`. The page features the HCL logo in the top left corner. The main heading is "Create and configure the application database". Below this, there are three input fields: "Host" with the value "localhost", "Database Name" with the value "tem_analytics", and "Authentication" with two radio button options: "Windows Authentication" (selected) and "SQL Server Authentication". A blue "Create" button is positioned below the authentication options.

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



The screenshot shows the same web browser window with the URL `localhost:9081/setup/database`. The main heading is "Create a user name and password for the administrator account." Below this, there are three input fields: "User Name*", "Password*", and "Password Confirmation*", each followed by a text input box. A grey "Create" button is located at the bottom of the form.

5. Connect to your BigFix Enterprise Server 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.

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.

The screenshot shows a web browser window at localhost:9081/setup/database. The page has an HCL logo at the top left and a blue header bar. The main content area is titled "Provide the connection parameters to the databases and the BigFix server". Below the title is a paragraph explaining that the application connects to the BigFix server database to import scan data and to the Web Reports database for optional access. The form contains three main sections: "Database for the BigFix Server*", "BigFix Server", and "Web Reports Database". Each section has fields for "Database Type" (SQL Server), "Host", and "Database Name". The "BigFix Server" section also includes a "Server API Port" field with a default value of 52311 and an "Authentication (Console Operator)" section with "User Name" and "Password" fields. The "Web Reports Database" section has an "Authentication" section with radio buttons for "Windows Authentication" (selected) and "SQL Server Authentication". A "Create" button is located at the bottom left of the form.

Provide the connection parameters to the databases and the BigFix server

The application connects to the BigFix server database to regularly import scan data. It connects to the 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 BigFix Server*

Database Type*
SQL Server

Host*
localhost

Database Name*
BFEnterprise

Authentication

Windows Authentication
 SQL Server Authentication

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 Manger Analytics server.

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 [replace](#)

Common name

Expiration Date: 11/13/2023

[Download Certificate](#)

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.

[Save](#)

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.

[Remediate](#)

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.

Configuring LDAP

BigFix for BigFix Compliance Analytics supports authentication through the Lightweight Directory Access Protocol (LDAP) server.

You can add LDAP associations to 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](#).

Updating National Vulnerability Database Data Feeds

Administrator updates the BigFix Compliance Analytics periodically to upload and synchronize the latest vulnerabilities.

To maintain accuracy and timeliness of BigFix Compliance Analytics Vulnerability reports, the BigFix Compliance Analytics administrator must periodically upload and synchronize the latest vulnerabilities, as the original data feed initiated during the BigFix Compliance Analytics vulnerabilities domain activation will become obsolete over time.

Many fixlets from BigFix Server patch sites with known vulnerabilities have corresponding CVE-IDs in the BES Console details tab. New or updated fixlets in BigFix patch sites have corresponding vulnerability with CVE-IDs that match the new CVE-IDs of the NVD data feeds. The new CVEs can be uploaded manually by the BigFix Compliance Analytics administrator from the NVD data feeds site, and the BigFix Compliance Analytics ETL Import must be initiated to include the new CVEs patch and vulnerability reports. After the import is complete, the new or updated vulnerabilities in BigFix Compliance Analytics vulnerability reports will have updated CVEs.

The .gz NVD files are uploaded for ETL import, and these files are located in the National Vulnerability Database [website](#). The file must be in the format `nvdCVE-n.n-yyyy.json.gz` to initiate the ETL import process. A .zip file can also be used.

Fixlet 1005 - Download NVD CVE Data Files in the SCM Reporting site can be used to download and cache the current and previous year's data files.



Note:

- Due to frequently changing data feeds, this Fixlet cannot perform an integrity check on the downloads.
- Depending on your current CVE data requirements, you can set the Fixlet in the SCM reporting site as a recurring task, or create a scheduled task and script to download and cache new files regularly, monthly, weekly, or more often depending on your requirements.

Steps to initiate the ETL import:

1. Download new or update .gz files using the JSON .gz links.



Note: Before initiating an ETL import, copy .gz files into the BigFix Compliance Analytics directories depending on whether the current version is upgraded to BigFix Compliance Analytics V10 (Location 1), or if the BigFix Compliance Analytics V10 was installed new without an upgrade (Location 2).

- Location 1: `C:\Program Files\IBM\SCA\wlp\usr\servers\server1\apps\tema.war\WEB-INF\data\pr\nvd\`
- Location 2: `C:\Program Files\Bigfix Enterprise\SCA\wlp\usr\servers\server1\apps\tema.war\WEB-INF\data\pr\nvd\`

2. Start the Import.

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.

Chapter 3. Uninstalling on Windows

To remove BigFix Compliance from your infrastructure, stop the application-specific actions and analyses that are running on the computers and uninstall the scanner. Remove the VM Manager tool. Subsequently, uninstall the BigFix Compliance server, and optionally eliminate the associated database as well.

Uninstalling the server on Windows in interactive mode

To uninstall the BigFix Compliance server on Windows, run the `uninstall.bat` file. Follow the instructions in the installation wizard. The wizard does not uninstall the MS SQL Server or the BigFix server. These components need to be removed separately.

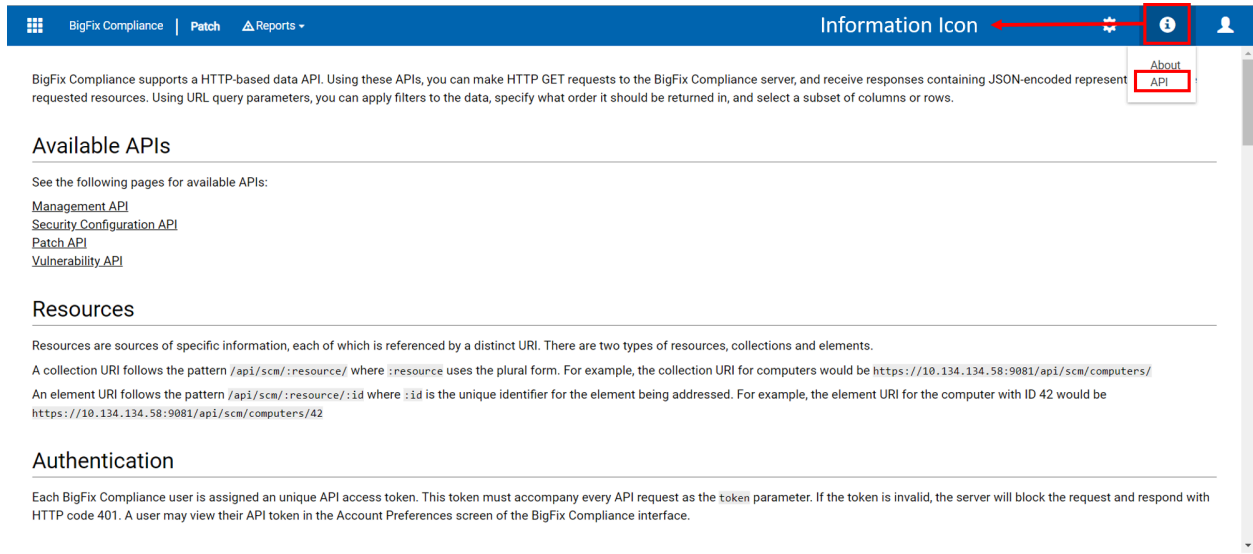
1. Log in to the computer where the BigFix Compliance server is installed as the same user who performed the installation.
2. Go to the `C:\Program Files\BigFix Enterprise\SCA\Uninstall` directory and run the `uninstall.bat` file. Start the uninstallation with the **Run as administrator** option.
3. Follow the instructions in the uninstallation wizard. When the uninstallation finishes, click **Done**.

The BigFix Compliance server is uninstalled but the database, user logins, and passwords are preserved. To remove them, [delete the BigFix Compliance database](#). You can also remove the [BigFix server](#).

Chapter 4. Configuring report definitions using REST API

Administrators can use REST API to create, update, and delete saved report view definitions across BFC instances.

For more information about the APIs, click **Information** icon on the header and select **API** from the dropdown.



The screenshot shows the top navigation bar of the BigFix Compliance interface. On the left, there are menu items for 'BigFix Compliance', 'Patch', and 'Reports'. On the right, there is an 'Information Icon' (an 'i' in a circle) which is highlighted with a red box and a red arrow. A dropdown menu is open below the icon, showing 'About' and 'API' (the latter is highlighted with a red box). Below the navigation bar, the 'API' page content is visible, including sections for 'Available APIs', 'Resources', and 'Authentication'.

BigFix Compliance supports a HTTP-based data API. Using these APIs, you can make HTTP GET requests to the BigFix Compliance server, and receive responses containing JSON-encoded representations of requested resources. Using URL query parameters, you can apply filters to the data, specify what order it should be returned in, and select a subset of columns or rows.

Available APIs

See the following pages for available APIs:

- [Management API](#)
- [Security Configuration API](#)
- [Patch API](#)
- [Vulnerability API](#)

Resources

Resources are sources of specific information, each of which is referenced by a distinct URI. There are two types of resources, collections and elements.

A collection URI follows the pattern `/api/scm/:resource/` where `:resource` uses the plural form. For example, the collection URI for computers would be `https://10.134.134.58:9081/api/scm/computers/`

An element URI follows the pattern `/api/scm/:resource/:id` where `:id` is the unique identifier for the element being addressed. For example, the element URI for the computer with ID 42 would be `https://10.134.134.58:9081/api/scm/computers/42`

Authentication

Each BigFix Compliance user is assigned a unique API access token. This token must accompany every API request as the `token` parameter. If the token is invalid, the server will block the request and respond with HTTP code 401. A user may view their API token in the Account Preferences screen of the BigFix Compliance interface.

Chapter 5. Disaster recovery for BigFix Compliance Analytics

Use the standard cold standby method of creating a backup and restoring the system in your disaster recovery plan for BigFix Compliance Analytics.

Similar to the HCL BigFix disaster plan, BigFix Compliance Analytics uses a standard backup/restore method that is called the Cold Standby method. This method does periodic backups of the application server and database files, usually done nightly. If there is a problem, the database and application server files can be restored to the HCL BigFix Application Server computer or another computer. The system is also restored.

Table 7. Pros and cons of using the cold standby method

Pros	Cons
<ul style="list-style-type: none">• Simple and allows for multiple backups over time.• Does not require any additional hardware. Hot or cold standby computer is optional.	<ul style="list-style-type: none">• All information since the last backup is lost in the event of a failure.• Restoring the system from the backup might have significant downtime.

The disaster recovery plan covers steps for the following procedures:

1. Backup procedure
2. Recovery procedure
3. Recovery verification procedure

Creating a backup of the application server

Create backups of the files and folders that the application server uses.

Establish a maintenance plan for nightly backups for the BFC_Analytics databases using SQL Server Enterprise Manager. Multiple backup copies give greater recovery flexibility. Consider backing up to a remote system to allow for higher fault tolerance.

For recovery purposes, create backups of the following files and folders that the application server uses:

- `[BFC Application folder]\config` -- Configuration (HTTPS, Port number, database connection information, and others)
- `[BFC Application folder]\log` -- Archived Import, error, and access logs

Recovering the backup application server

Restore the backup of your BigFix Compliance Analytics application server.

1. Install the same version of SQL Server that was previously used in either a previous application server computer or a new computer.



Note: If you used Mixed Mode Authentication on the previous application server, you must enable it for your new SQL installation.

2. Restore the BFC_Analytics databases from backup.
3. Install the application server. Use the same version of the application installation binary as was previously used.
4. At the end of installation, skip the launch web configuration step. Instead, go to NT Services Manager and stop 'BigFix Compliance Analytics' service.
5. Restore/Replace the backed up configuration and log files and folders. Create the directory structure as needed.
6. Go to **NT Services Manager** and start the **BigFix Compliance Analytics** service.

Ensure that the new application server computer can access the following datasources: BFEnterprise and BESReporting. For NT Auth to access the BFC_Analytics and BFEnterprise databases, ensure that the service user has the necessary DB/File access rights).

Verifying the success of the recovery procedure

Check the historical log and run an import action to verify that the Compliance Application is successfully restored.

Do the following steps to ensure that the Compliance Application Server is successfully restored.

1. Go to Compliance web interface and login with Administrator rights to verify that the login works properly.
2. Go to **Management > Import** and verify the historical log shown in the page frame.

Appendix A. Support

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

- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Playlist on YouTube](#)
- [BigFix Tech Advisors channel on YouTube](#)
- [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.