

BigFix
Client Compliance User Guide



Special notice

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

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. BigFix Client Compliance Configuration..... 5**
 - Deploying an existing BigFix Client Compliance document..... 5
 - Creating a new BigFix Client Compliance document..... 7
 - Deploying a task to the computer..... 11
- Chapter 2. BigFix Client Compliance Windows (IPSec Framework)..... 14**
- Notices.....xvii

Chapter 1. BigFix Client Compliance Configuration

BigFix Client Compliance Configuration allows you to deploy client compliance document to a set of computers. You can also create a new policy document using BigFix Client Compliance Configuration Wizard.

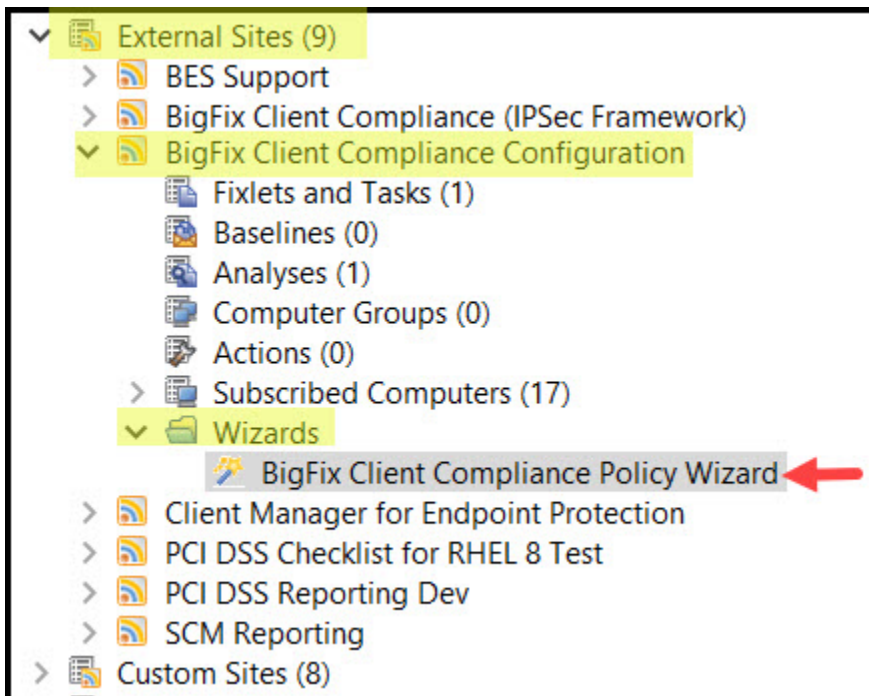
Deploying an existing BigFix Client Compliance document

Use BigFix Client Compliance Policy Wizard to modify and deploy policy to one or more computer or client endpoints.

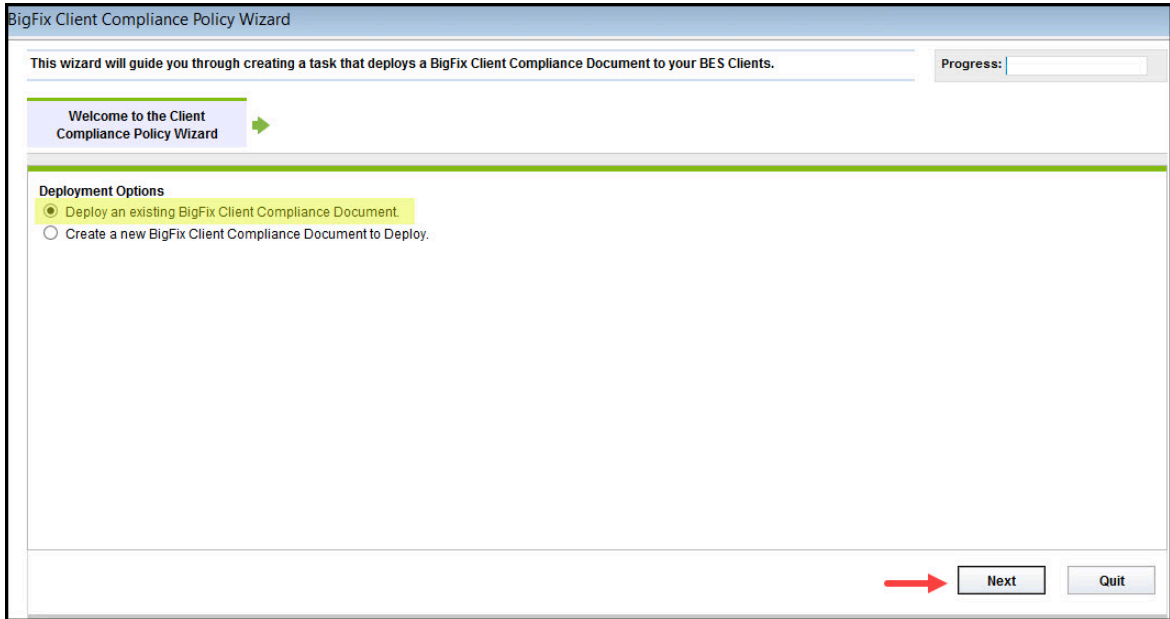
1. Login to BigFix console and select **BigFix Management** from the list of available domains.



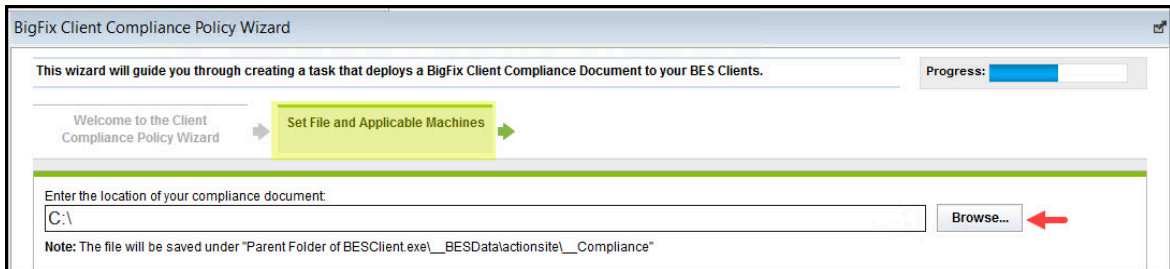
2. To access **BigFix Client Compliance Policy Wizard**, select **External Sites > BigFix Client Compliance Configuration > Wizards > BigFix Client Compliance Policy Wizard** from the navigation tree.



3. In the **Welcome to the Client Compliance Policy Wizard** tab, select **Deploy an existing BigFix Compliance Document** and click **Next**.



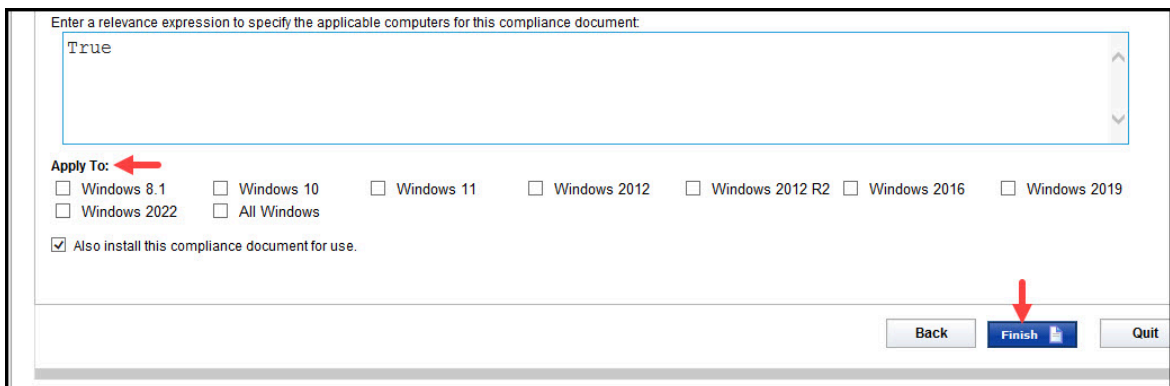
4. In the **Set File and Applicable Machines** tab, click **Browse...** to select a policy document to modify.



5. Select the applicable operating system and click **Finish** to save the changes.



Note: The relevance expression changes as per the operation system selected.



For more information on deploying the tasks to the computer, see [Deploying a task to the computer \(on page 11\)](#).

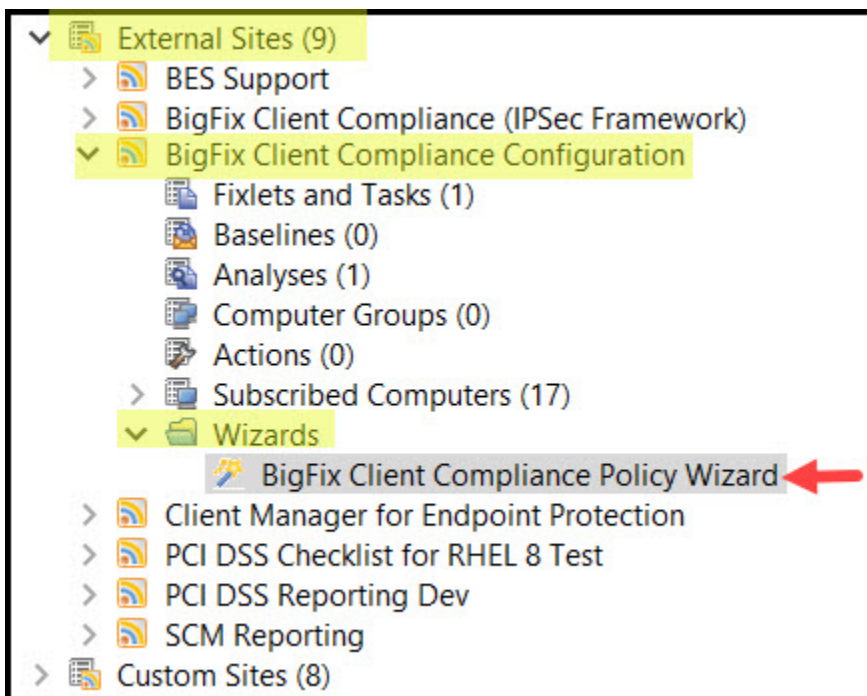
Creating a new BigFix Client Compliance document

Use BigFix Client Compliance Policy Wizard to create a new policy document and deploy policy to one or more computer or client endpoints.

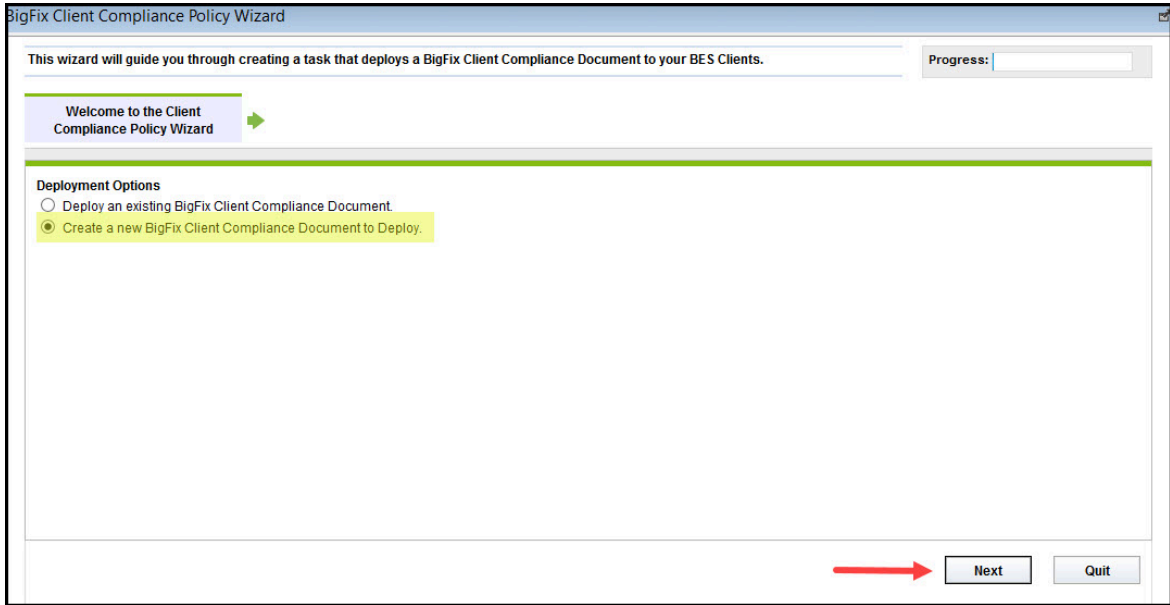
1. Login to BigFix console and select **BigFix Management** from the list of available domains.



2. To access **BigFix Client Compliance Policy Wizard**, select **External Sites > BigFix Client Compliance Configuration > Wizards > BigFix Client Compliance Policy Wizard** from the navigation tree.



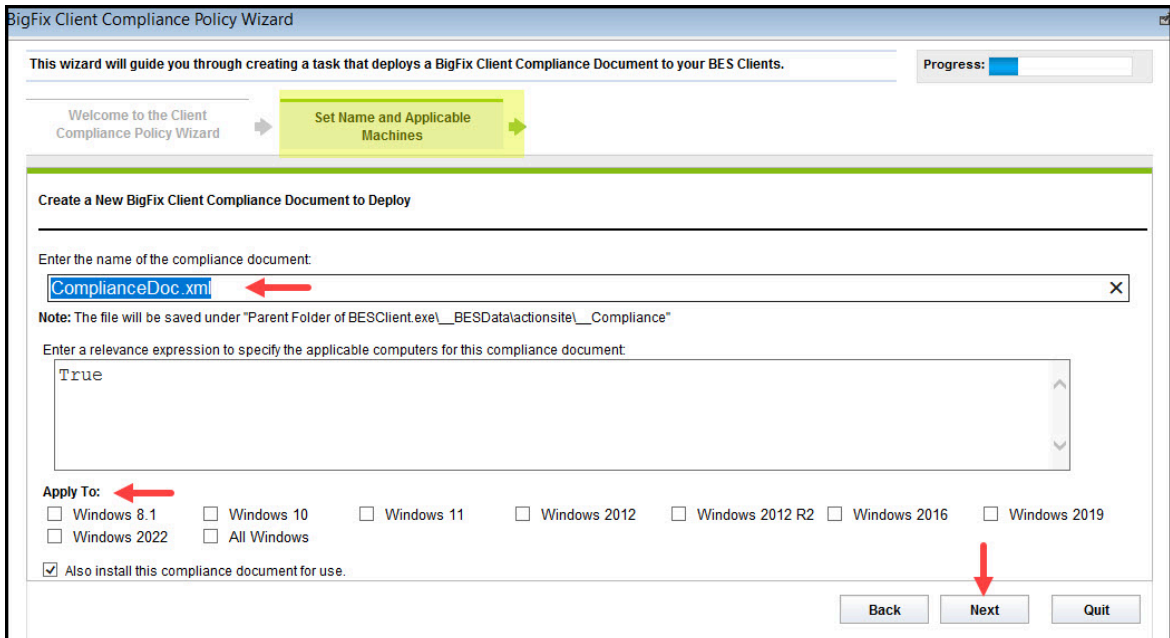
3. In the **Welcome to the Client Compliance Policy Wizard** tab, select **Deploy an existing BigFix Compliance Document** and click **Next**.



4. In the **Set Name and Applicable Machines** tab, provide the required information such as **Name**, **operating system** and click **Next**.



Note: The relevance expression is auto generated based on the operating system and other parameters.



5. In the **Set Basic Quarantine Settings** tab, check the required settings from the list, define its parameter and click **Next**. For example, check **Maximum number of relevant critical patches** and define its parameter.

BigFix Client Compliance Policy Wizard

This wizard will guide you through creating a task that deploys a BigFix Client Compliance Document to your BES Clients. Progress:

Welcome to the Client Compliance Policy Wizard → Set Name and Applicable Machines → **Set Basic Quarantine Settings** →

Note: Leave check boxes cleared and click "Next" if you do not want to set any basic settings.

Maximum number of relevant critical patches: ←

Maximum age of any relevant critical patch: In day(s)

Name of a process required to be running:

Back Next Quit

6. In the **Set Anti-Virus Quarantine Settings** tab, check the required **antivirus application** from the list, define its maximum age in day(s) and click **Next**.

BigFix Client Compliance Policy Wizard

This wizard will guide you through creating a task that deploys a BigFix Client Compliance Document to your BES Clients. Progress:

Welcome to the Client Compliance Policy Wizard → Set Name and Applicable Machines → Set Basic Quarantine Settings → **Set Anti-Virus Quarantine Settings** →

Please specify any AntiVirus applications that are required to be running and specify the maximum AntiVirus definition age. A computer will be considered compliant if at least one of the selected AntiVirus applications is running with definitions less than the specified number of days old.

AntiVirus Applications

McAfee VirusScan 8i/8.5i/8.7i/8.8i: day(s) ←

McAfee Endpoint Security 10.x: day(s)

Symantec Anti-Virus Corporate or Endpoint Protection: day(s)

Sophos Anti-virus 10.x: day(s)

Sophos Anti-virus / Endpoint Security 10.x: day(s)

Trend Micro OfficeScan 11.x/12.x: day(s)

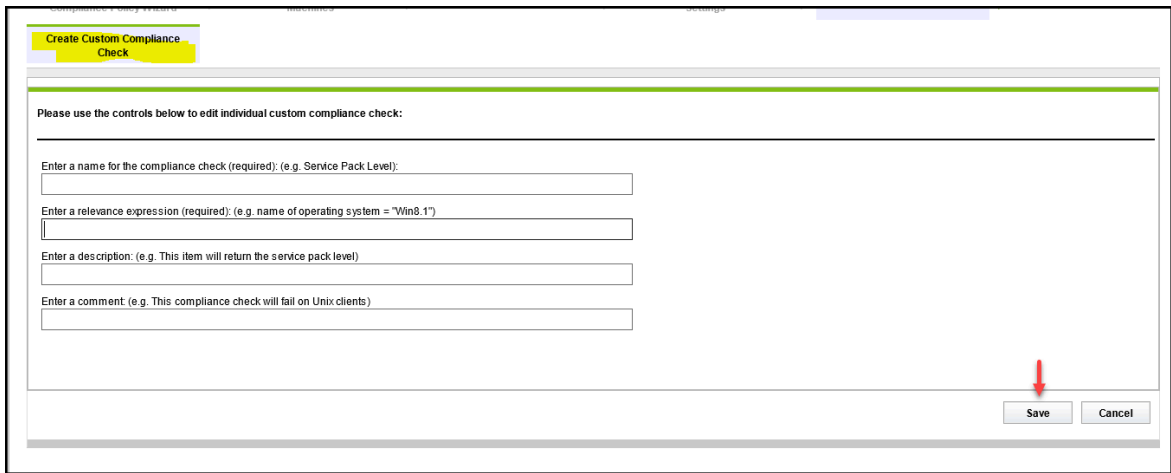
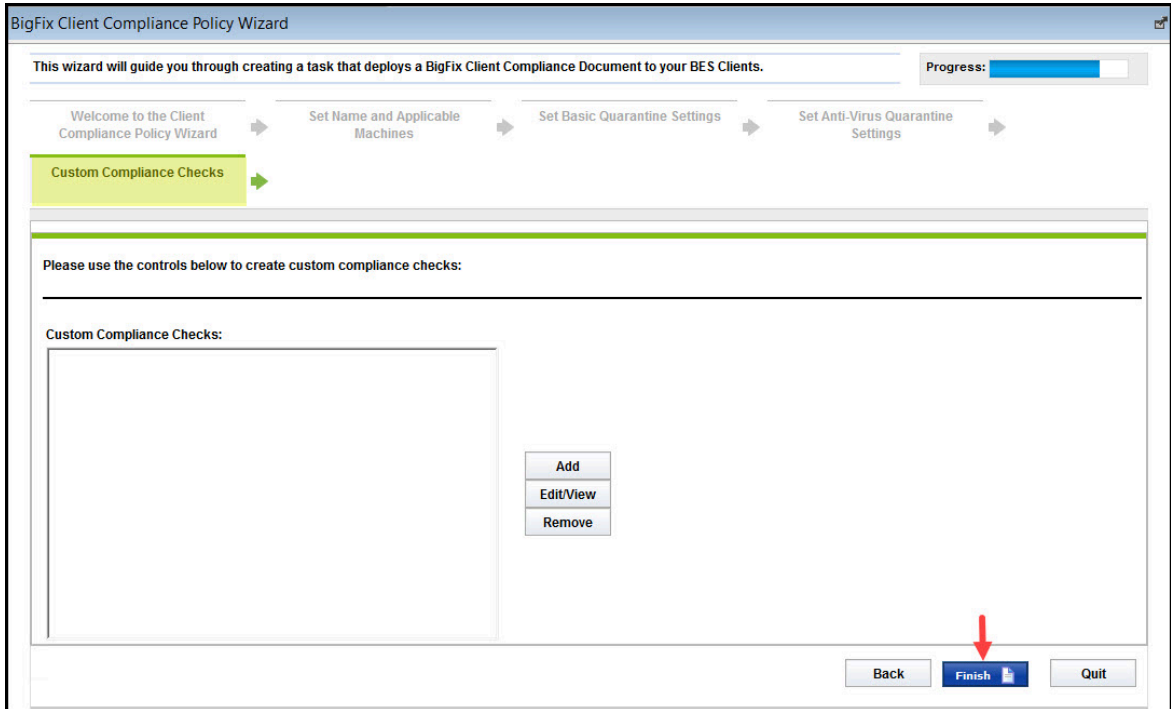
Trend Micro Server Protect 5.x: day(s)

Back Next Quit

7. In the **Custom Compliance Checks** tab, users can try various options to **Create Custom Compliance Check** such as:

- a. user can add a new custom compliance checks
- b. user can edit the existing custom compliance checks
- c. user can view the existing custom compliance checks
- d. user can remove the existing custom compliance checks

and click **save** and then click **Finish** on the **Custom Compliance Checks** tab.



8. In the **Security Warning** dialog window, click **Continue**.

- Use the **Create in site** and **Create in domain** drop-down to select the **site** and **domain**, and click **OK**.

The screenshot shows the 'Create Task' dialog box. At the top, the 'Name' field is filled with 'Client API Compliance Rule Document - ComplianceDoc.xml'. To the right, there are two dropdown menus: 'Create in site' is set to 'Master Action Site' and 'Create in domain' is set to 'BigFix Management'. Below these are tabs for 'Description', 'Actions', 'Relevance', and 'Properties'. The 'Description' tab is selected, showing a rich text editor with a toolbar. The description text reads: 'This task will create and deploy BigFix client API compliance rule document ComplianceDoc.xml.' Below the description is an 'Actions' section with a single action: 'Click [here](#) to deploy this task.' At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. A red arrow points to the 'OK' button.

A new policy document is created as a task in the selected site and this task will become relevant when the computer in site matches the parameters defined in the policy.

For more information on deploying the tasks to the computer, see [Deploying a task to the computer \(on page 11\)](#).

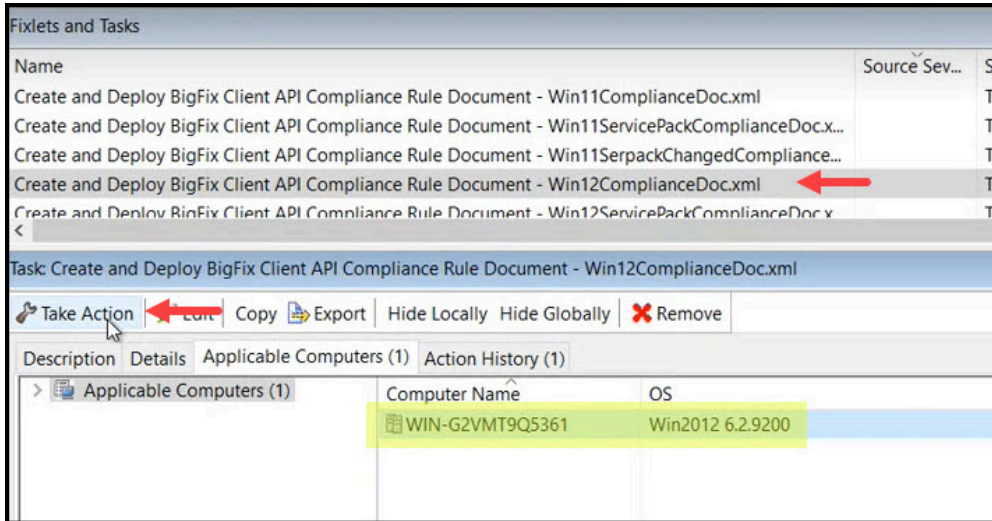
Deploying a task to the computer

Understand how to deploy the task to the computer or client endpoint.

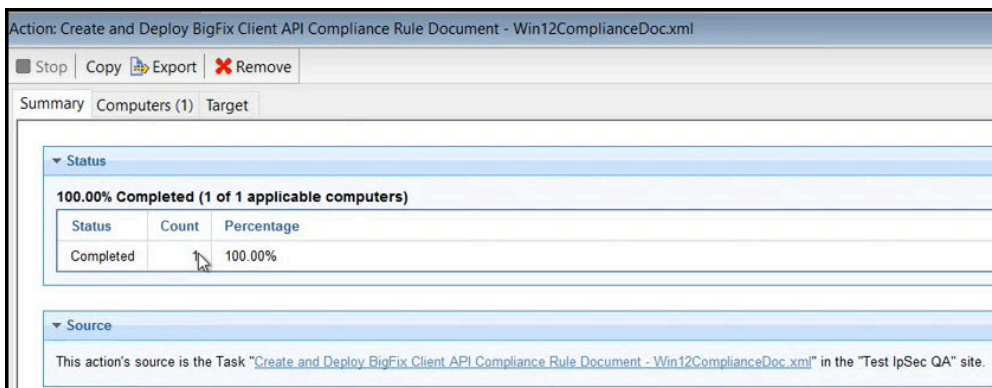
- Select the **Task** from the list of Fixlets and Tasks and click **Take Action**.



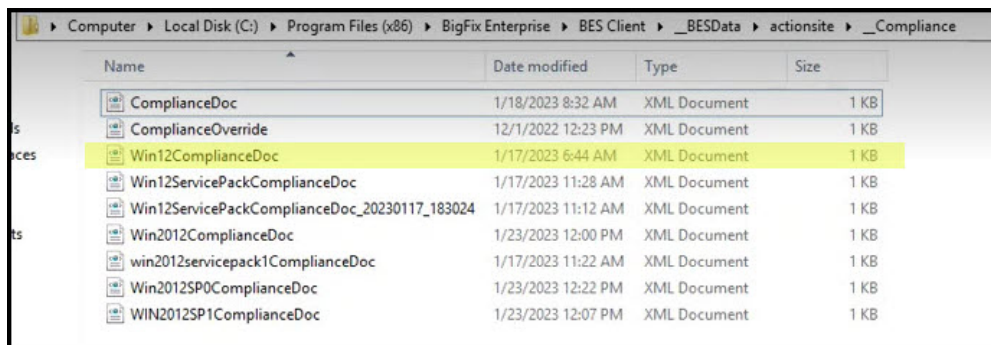
Note: You can see the applicable computer in the work area.



2. To see the progress, click **Action History**.



When the task is successfully deployed, a `.xml` file is created in the respective computer. Along with the `.xml` file, the relevant registry folders and keys are generated in the computer.



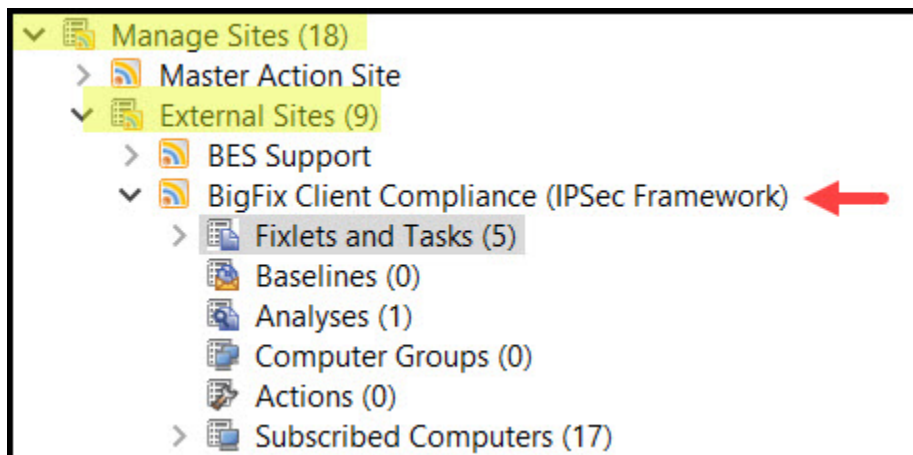
Chapter 2. BigFix Client Compliance Windows (IPSec Framework)

The BigFix Client Compliance Windows (IPSec Framework) Fixlet site provides self-quarantine capabilities using the BigFix Client Compliance extension. In this solution, the BES Client restricts or enables inbound and outbound network connectivity based on the compliance status of the computer (but still passing BES network traffic to allow management of the computer through BES).

The following Fixlets, Task and Analysis are available in the BigFix Client Compliance Windows (IPSec Framework):

- **Fixlets:**
 - IPSec - Automatically Quarantine New Clients
 - IPSec - Determine Compliance
 - IPSec - Quarantine Needed
 - IPSec - Quarantine No Longer Needed
- **Task:**
 - IPSec - Quarantine Override
- **Analysis:**
 - IPSec - Compliance Evaluation Information

To access BigFix Client Compliance Windows (IPSec Framework), select **BigFix Management > Manage Sites > External Sites > BigFix Client Compliance (IPSec Framework) > Fixlets and Tasks or Analyses**.



Fixlets

IPSec - Automatically Quarantine New Clients

This Fixlet message ensures that when a new workstation computer or client endpoint first joins the network, it will be quarantined. This Fixlet message should be applied before any other IPSec Fixlet messages. It is recommended that you deploy this as a policy action to ensure that any new computers joining the network will be automatically quarantined until it can be determined that they are compliant.

IPSec - Determine Compliance

This Fixlet message determines if a client computer is compliant with the security standards defined in the compliance document. The Fixlet message will become relevant periodically (the current setting is every 5 minutes). It is recommended that you deploy this Fixlet as a policy action so that the compliance status of computers on the network will be periodically evaluated.

IPSec - Quarantine Needed

If the computer in question is NOT in compliance and is NOT already in quarantine, then this Fixlet message will quarantine the computer, leaving ONLY the communication between the BES client and the BES server open. When you take this action from the BES console, use the options under the Message tab to send a notification message to users. It is recommended that you deploy this Fixlet message as a policy action.

IPSec - Quarantine No Longer Needed

If a client computer is quarantined and it is compliant, then this Fixlet will remove the computer from quarantine. When you take this action from the BES console, use the options under the Message tab to send a notification message to users. It is recommended you deploy this Fixlet message as a policy action.

Task

IPSec - Quarantine Override

This task will take a computer out of quarantine regardless of its compliance status. This is meant to be a temporary measure to release a computer from quarantine. The action will install a compliance document containing one compliance expression that always evaluate to true, causing the client to be compliant. The next part of the action takes the computer out of quarantine. This two-part action ensures that any policy actions already in effect will not return the computer to the quarantined state.

Analysis

IPSec - Compliance Evaluation Information

Retrieves the current compliance and quarantine statuses on computers with the BigFix Client Compliance extension installed.



1. The "Compliance Status" is calculated based on the results of the last compliance evaluation, while the "Quarantine Status" property is determined by the results of quarantine actions. A computer that is out of quarantine is not necessarily in compliance, and vice versa. If the compliance and quarantine statuses are inconsistent, make sure that you determine compliance and quarantine policy actions are set up correctly.
2. Once a client computer has been quarantined, the BES console administrator should apply any necessary Fixlet messages or custom actions to bring that computer into compliance. At that time, the "IPSec - Quarantine No Longer Needed" Fixlet message will



become relevant, and it can be removed from quarantine. The BES console administrator can automate remediation and removal of computers from quarantine by deploying the appropriate Fixlet messages as policy actions.

3. This Fixlet site is designed to be used in conjunction with the "BigFix Client Compliance Windows (IPSec Framework)" Fixlet site. For more information on BigFix Client Compliance visit <https://support.bigfix.com/bes/sites/clientcompliance.html>.

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.