



# **BigFix® Firewall Deployment Guide**

BigFix, Inc.  
Emeryville, CA

Last Modified: 7/23/08  
Version 2.0

© 1998–2008 BigFix, Inc. All rights reserved.

BigFix®, Fixlet® and "Fix it before it fails"® are registered trademarks of BigFix, Inc. iprevention, Powered by BigFix, Relevance Engine, and related BigFix logos are trademarks of BigFix, Inc. All other product names, trade names, trademarks, and logos used in this documentation are the property of their respective owners. BigFix's use of any other company's trademarks, trade names, product names and logos or images of the same does not necessarily constitute: (1) an endorsement by such company of BigFix and its products, and (2) an endorsement of the company or its products by BigFix.

Except as set forth in the last sentence of this paragraph: (1) no part of this documentation may be reproduced, transmitted, or otherwise distributed in any form or by any means (electronic or otherwise) without the prior written consent of BigFix, Inc., and (2) you may not use this documentation for any purpose except in connection with your properly licensed use or evaluation of BigFix software and any other use, including for reverse engineering such software or creating derivative works thereof, is prohibited. If the license to the software which this documentation accompanies is terminated, you must immediately return this documentation to BigFix, Inc. and destroy all copies you may have. You may treat only those portions of this documentation specifically designated in the "Acknowledgements and Notices" section below as notices applicable to third party software in accordance with the terms of such notices.

All inquiries regarding the foregoing should be addressed to:

BigFix, Inc.

1480 64th Street, Suite 200

Emeryville, CA 94608

## CONTENTS

# Contents

---

<b>PREFACE</b>	<b>1</b>
AUDIENCE .....	1
ORGANIZATION OF THIS GUIDE.....	1
CONVENTIONS USED IN THIS GUIDE .....	1
VERSIONS .....	1
 <b>INTRODUCTION</b>	 <b>2</b>
 <b>QUICK-START</b>	 <b>3</b>
BEGINNING SETUP .....	3
ACCESSING THE BIGFIX FIREWALL DASHBOARD .....	4
<i>Launching the Dashboard.....</i>	<i>4</i>
<i>Using the BigFix Firewall Dashboard Controls .....</i>	<i>4</i>
<i>Reading the Dashboard's Overview Statistics and Charts .....</i>	<i>6</i>
<i>Understanding the General Statistics.....</i>	<i>7</i>
 <b>USING BIGFIX FIREWALL</b>	 <b>9</b>
DEPLOYING BIGFIX FIREWALL .....	9
UPDATING BIGFIX FIREWALL .....	11
 <b>SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS</b>	 <b>12</b>
CONFIGURING FIREWALL POLICIES.....	12
CONFIGURING CLIENT COMPLIANCE POLICIES .....	18
ENABLING CLIENT COMPLIANCE .....	26
ENABLING DYNAMIC LOADING OF FIREWALL POLICIES .....	26
USING THE EXAMPLE CLIENT COMPLIANCE CONFIGURATION BASELINE .....	27
 <b>PERFORMING ADDITIONAL TASKS</b>	 <b>29</b>
UPLOADING BIGFIX FIREWALL LOGS .....	29
CHANGING COMPLIANCE EVALUATION SETTINGS .....	29
ENSURING BIGFIX CLIENTS CAN COMMUNICATE .....	29
DISABLING WINDOWS FIREWALL .....	29
 <b>ADVANCED SETTINGS</b>	 <b>30</b>
 <b>FIREWALL RULE SORTING</b>	 <b>31</b>
 <b>FREQUENTLY ASKED QUESTIONS</b>	 <b>32</b>
GENERAL QUESTIONS.....	32
REPORTING .....	33
 <b>ACKNOWLEDGEMENTS AND NOTICES</b>	 <b>34</b>

# Preface

---

## Audience

This document describes the installation and operation of BigFix Firewall. It is intended for BigFix administrators and operators, as well as people evaluating the product.

## Organization of this Guide

This guide is composed of five major sections:

- **Introduction:** This section introduces BigFix Firewall.
- **Quick Start:** This section provides brief instructions for deploying and using BigFix Firewall.
- **Using BigFix Firewall:** This section provides instructions for performing the most common tasks with BigFix Firewall.
- **Setting Policies Using the BigFix Firewall and Client Compliance Wizards:** This section provides instructions for setting firewall policies.
- **Frequently Asked Questions:** This section provides answers for frequently asked questions about BigFix Firewall.

## Conventions Used in this Guide

This document makes use of the following conventions and nomenclature:

Convention	Use
<b>Bold Sans</b>	A bold sans-serif font is used for chapter headers.
<b>Bold text</b>	Bold text typically refers to a program interface.
<i>Italics</i>	Italics are used for BigFix document titles.
<code>Mono-space</code>	A mono-spaced font is used to indicate scripts or code snippets.

## Versions

The document describes the functionality in BigFix Firewall, Version 2.0 and later.

## INTRODUCTION

## Introduction

---

BigFix Firewall consolidates management of endpoint-based firewall defenses through the BigFix console. In addition, BigFix Firewall provides fine-grained policy enforcement, location-awareness, and integrated network access control functionality.

BigFix Firewall can be deployed and managed by BigFix administrators or operators, using the BigFix Console. It provides:

- Real-time visibility and control through the BigFix Console to integrate firewall defense with antivirus, anti-spyware, and other proactive information security measures
- Robust packet inspection and filtering technology for policy-defined regulation of all inbound and outbound network traffic

BigFix Firewall works in two distinct modes: static and dynamic.

- In the **static** mode, firewall rules are loaded once and do not change until a specific action is taken to load a new set of rules. This is standard practice for firewall software and will be familiar to most administrators. However, even in this static configuration, BigFix Firewall can automatically trigger changes in the firewall rules based on predefined client policies. The static mode also allows an operator to change policies immediately (or at any specified time) by simply issuing an Action. Thus, even the static mode has great flexibility within the BigFix environment.
- In the **dynamic** mode, BigFix Firewall can load a new firewall policy based on any desired network state change. This provides an unprecedented degree of situational control over your firewall. For instance, if a client initiates a VPN connection, BigFix Firewall compares the state of that client to your customized compliance policies. Based on that comparison, it selects an appropriate set of firewall rules for that particular connection on that particular client. Similarly, acquiring new IP addresses or adding new interfaces can be handled quickly and seamlessly. In this way, BigFix can automatically enforce a unique set of firewall rules based on the connection type, compliance state, physical location or any other criteria that can be expressed using the BigFix Relevance language.

A common use case for the dynamic mode is to load different policies based on location. For instance, the device may be connected to the internal LAN, somewhere on the public internet, or over a VPN. In this case, BigFix Firewall automatically applies the proper set of firewall rules, depending on the client's location. A second example might be the application of different firewall rules based on adherence to a security baseline. Secured machines could be allowed looser firewall rules and insecure machines could be placed in quarantine.

To implement the static mode, you will use the **Firewall Policy Wizard**. For the dynamic mode, you will also use the **Client Compliance Policy Wizard**. These two policies combined will provide you with a dynamic, highly granular solution to your firewall issues.

## Quick-Start

---

This section will help you get started with BigFix Firewall.

### Beginning Setup

This procedure assumes that you already have installed BigFix.

1. Obtain a masthead for the BigFix Firewall site.

Email [licensing@bigfix.com](mailto:licensing@bigfix.com) to request the masthead.

2. Add the BigFix Firewall site:

- a. Double-click on the masthead file.

A dialog box will appear, asking if you want to proceed with adding the site.

- b. Click **Yes**.

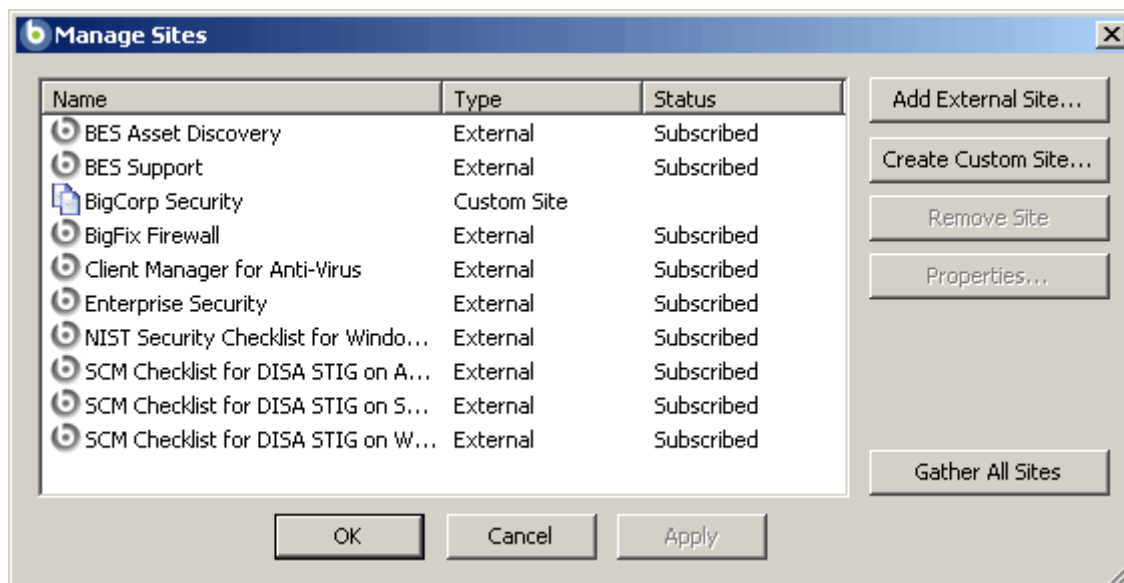
- c. Enter your Private Key Password and click **OK**.

At this point, the BigFix Firewall site will begin the gathering process, in which Fixlets, Tasks, Analyses, etc. are gathered from the central BigFix server.

When the gathering process is complete, the status will change to **Subscribed**.

Refer to the *Console Operators Guide* for more information about mastheads.

You will see a new BigFix Firewall entry in the **Dashboards** menu and your Navigation Bar. The site will show as **Subscribed** in the **Manage Sites** dialog.



## QUICK-START

## Accessing the BigFix Firewall Dashboard

BigFix Firewall provides a dashboard view with overview statistics and charts that enable administrators to gauge the current status of their system and to track statistics as BigFix Firewall enforces Firewall policies throughout the network. In addition, you can use the Dashboard as a central point to manage important tasks such as deployment, updates, and configuration.

To open the Dashboard, select **Dashboards > BigFix Firewall**.



### Launching the Dashboard

The first time you launch the Dashboard, you will be prompted to activate any necessary analyses.



1. Click the link to activate the analyses.
2. Enter your private key password when prompted, and click **OK**.

After activation, you might also see a notice to install Office Web Components. If necessary, install Office Web Components following the instructions in the linked Knowledge Base Article.

Once analyses are activated and Office Web Components is installed, close and then reopen the Dashboard.

### Using the BigFix Firewall Dashboard Controls

At the top of the Dashboard, you see the BigFix Firewall Controls. This is a central interface for the BigFix Firewall, where you can find most of the key commands:

Deploy	Configure	Additional Tasks
<a href="#">Deploy BigFix Firewall</a>	<a href="#">Configure BigFix Firewall Policies</a>	<a href="#">Uninstall BigFix Firewall</a>
<a href="#">Update BigFix Firewall</a>	<a href="#">Configure Compliance Policies</a>	<a href="#">Disable Windows Firewall</a>
	<a href="#">View BigFix Firewall Configurations</a>	<a href="#">Upload BigFix Firewall Logs</a>
	<a href="#">View Compliance Configurations</a>	<a href="#">Change Compliance Evaluation Settings</a>
	<a href="#">View BigFix Firewall Engine Configurations</a>	<a href="#">Ensure BigFix Clients Can Communicate</a>

## QUICK-START

The controls available from the Firewall Dashboard include:

### Deploy

Use the controls in this section to deploy or update BigFix Firewall.

- **Deploy BigFix Firewall:** Brings up the Firewall Deployment Task. For more information see Deploying BigFix Firewall, page 9.
- **Update BigFix Firewall:** Brings up the Firewall Update Fixlet, which allows you to update any out-of-date components in the Firewall site. See Updating BigFix Firewall, page 11.

### Configure

Use the controls in this section to configure BigFix Firewall or to view your existing configurations.

- **Configure BigFix Firewall Policies:** Runs the BigFix Firewall Policy Wizard, where you can define your firewall and zone rules for a specified policy. The Wizard constructs a Task that you can hand-edit if you desire. You can also run this from the **Wizards** menu.
- **Configure Compliance Policies:** Runs the BigFix Client Compliance Policy Wizard, where you can define a client compliance document, including the applicable operating systems and compliance criteria (such as service packs and anti-virus versions) and the firewall policies to enforce on those clients that are compliant. This Wizard constructs an editable Task. You can also run this from the **Wizards** menu.
- **View BigFix Firewall Configurations:** Displays the BigFix Firewall Policy Analysis, which includes active and available policy and zone rules. As with all the firewall analyses, this allows you to display an in-depth report for each firewalled client, including firewall policies and detailed inbound/outbound statistics.
- **View Compliance Configurations:** Displays the BigFix Client Compliance Policy Analysis, which includes the current policies, policy items and firewall mappings.
- **View BigFix Firewall Engine Configurations:** Displays the BigFix Firewall Configuration Analysis, which includes the current versions of the firewall engine and logging service as well as the installation date and the status of the client compliance, BES port, ICMP, DNS, NetBIOS and more.

### Additional Tasks

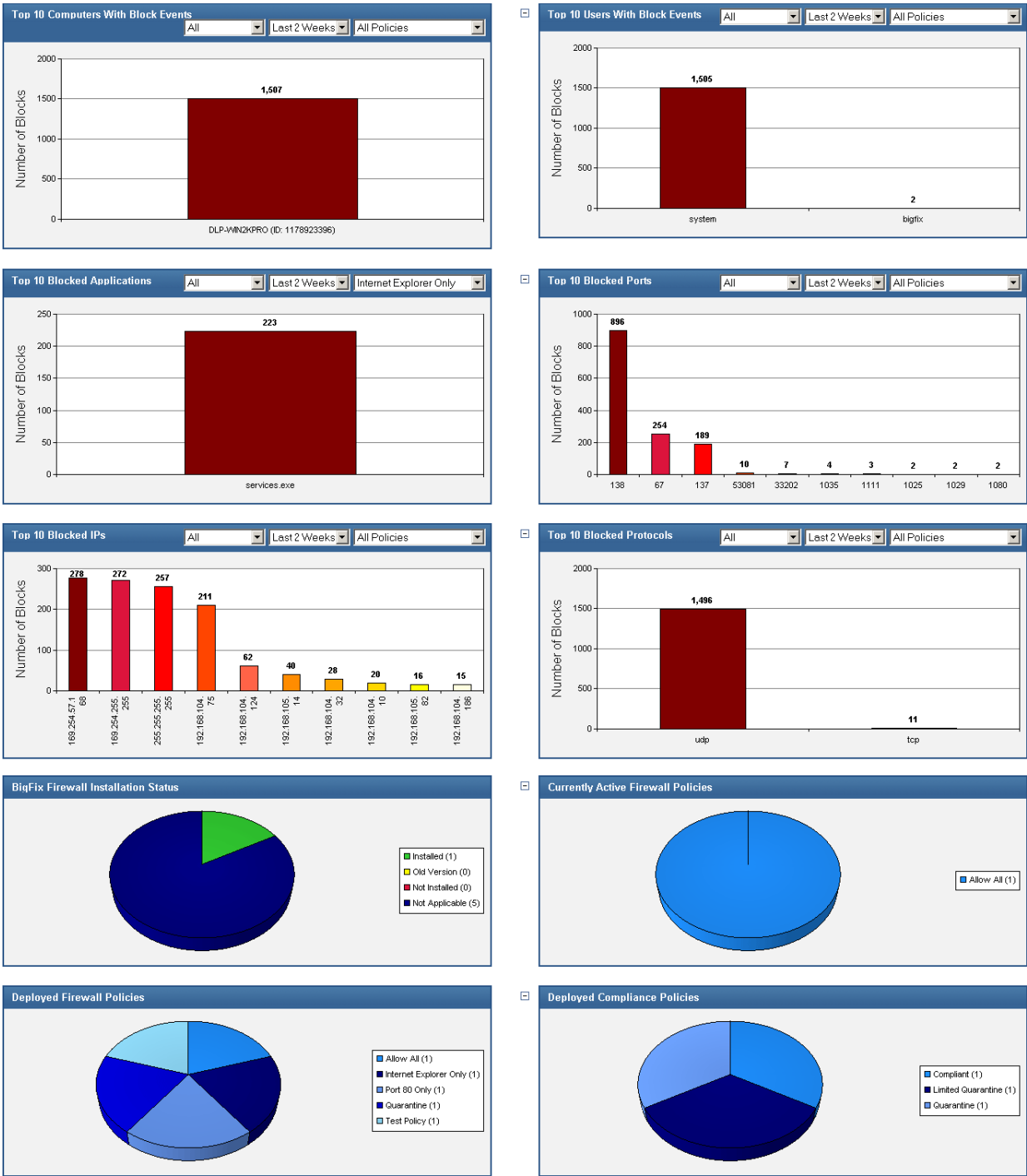
Use these controls for extra BigFix Firewall housekeeping chores.

- **Uninstall BigFix Firewall:** Brings up a task allowing you to uninstall the firewall site.
- **Disable Windows Firewall:** Brings up a task allowing you to disable the firewall on all listed computers.
- **Upload BigFix Firewall Logs:** Brings up a task allowing you to upload the firewall logs to the BigFix Server.
- **Change Compliance Evaluation Settings:** Brings up a task allowing you to run, enable, disable or change the interval of client compliance evaluation.
- **Ensure BigFix Clients Can Communicate:** Brings up a Fixlet allowing you to reopen any BigFix communication channels that have been inadvertently blocked.



Reading the Dashboard's Overview Statistics and Charts

Below the main control interface, you see several graphs illustrating your BigFix Firewall status.



## QUICK-START

BigFix Firewall provides charts illustrating:

- **Top 10 Computers with Block Events:** A bar chart showing the ten computers with the most block events, and the number of blocks per computer.
- **Top 10 Users with Block Events:** A bar chart showing the ten users with the most block events, and the number of blocks per user.
- **Top 10 Blocked Applications:** A bar chart showing the ten applications most often blocked, and the number of times each was blocked.
- **Top 10 Blocked Ports:** A bar chart showing the ten ports most often blocked, and the number of times each was blocked.
- **Top 10 Blocked IPs:** A bar chart showing the ten IP addresses most often blocked, and the number of times each was blocked.
- **Top 10 Blocked Protocols:** A bar chart showing the ten protocols most often blocked, and the number of times each was blocked.
- **BigFix Firewall Installation Status:** A pie chart showing on which machines BigFix Firewall is installed and whether the version is up-to-date.
- **Currently Active Firewall Policies:** A pie chart showing which firewall policies are currently active.
- **Deployed Firewall Policies:** A pie chart showing on how many machines each policy is deployed.
- **Deployed Compliance Policies:** A pie chart depicting the relative number of deployed compliance policies.

### Understanding the General Statistics

Below the graphs, you see the **General Statistics** section.

General Statistics		All	Last 2 Weeks	All Policies
Total number of computers with BigFix Firewall		1		
Total number of blocks		1,507		
Average number of blocks		1,507.00		
Computers that blocked application	services.exe	more than	10	times
Computers that blocked traffic on port	138	more than	10	times
Computers that blocked traffic to/from ip address	*	more than	10	times
Computers that blocked traffic using protocol	Any Protocol	more than	10	times

## QUICK-START

The statistics you can gather on your deployment include:

- Total number of computers with BigFix Firewall installed
- Total number of blocked I/O attempts
- Average number of blocked attempts
- Computers that blocked <application, Any Application> <less than, more than, exactly> <number> times
- Computers that blocked traffic on port <number> <less than, more than, exactly> <number> times
- Computers that blocked traffic to/from IP address <address> <less than, more than, exactly> <number> times
- Computers that blocked traffic using protocol <protocol> <less than, more than, exactly> <number> times

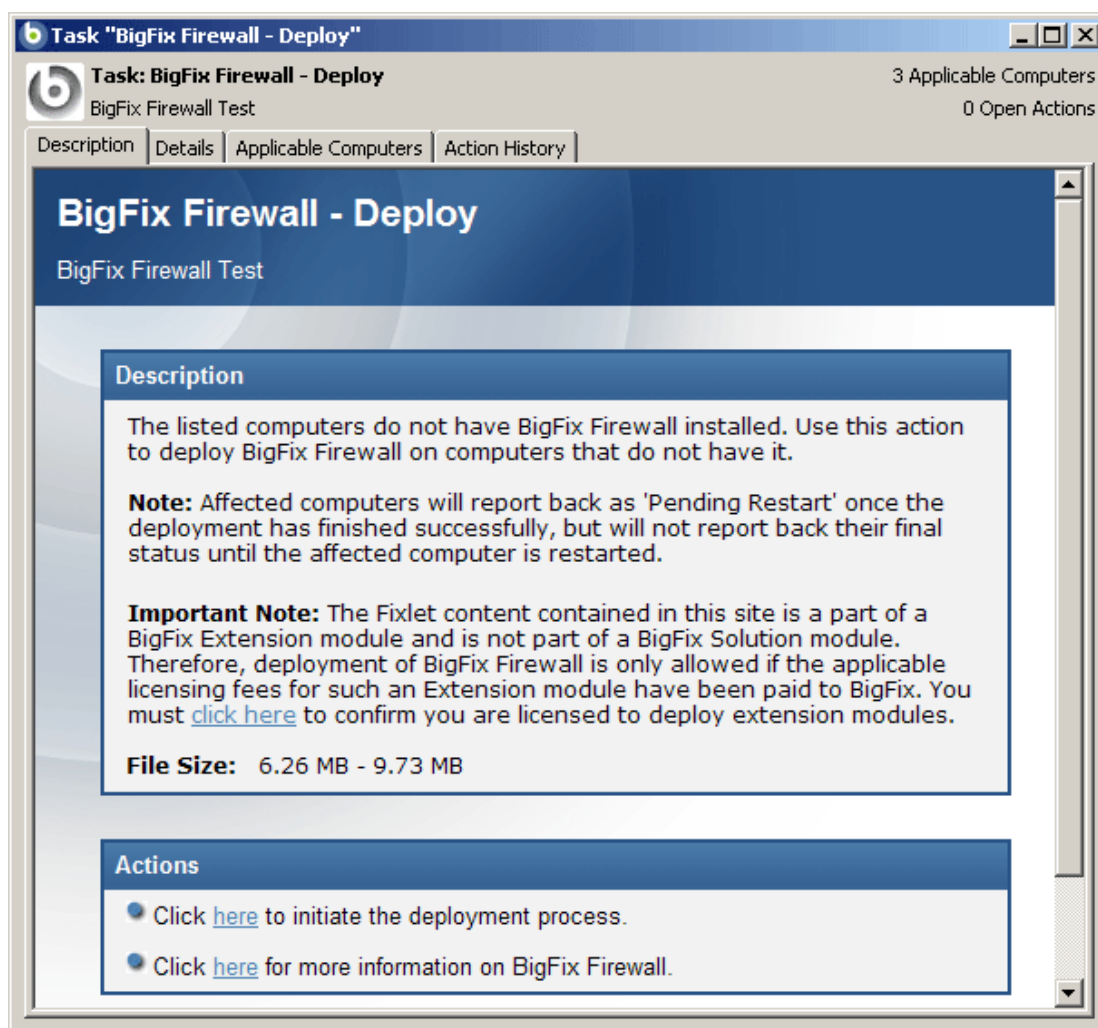
**Tip:** You can use the drop-down menus in the title bars to filter graphs by direction (inbound/outbound), time period, and policy.

## Using BigFix Firewall

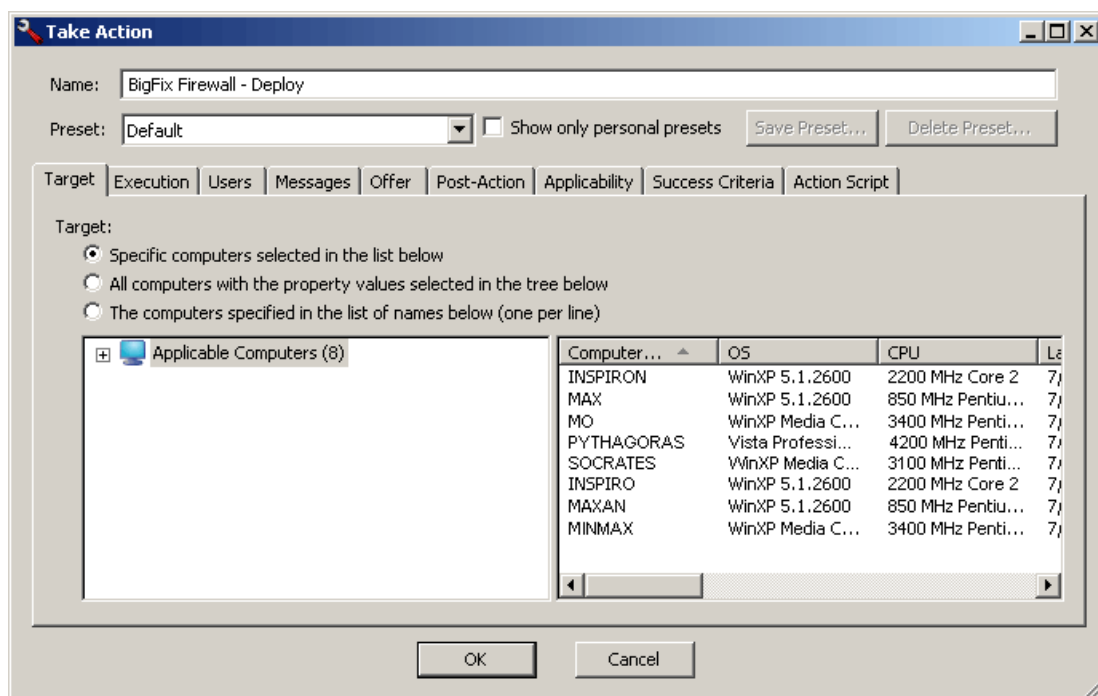
This section provides instructions for performing the most common tasks with BigFix Firewall.

### Deploying BigFix Firewall

1. From the Dashboard, click on the **Deploy BigFix Firewall** link. The **Deploy BigFix Firewall** Task will open.
2. Click the link located in the **Description** section to accept the extension license. This will present you with a new action to initiate the deployment process.



3. Click the initiation link in the **Actions** section to start the deployment process.  
The **Take Action** dialog box opens.



4. In the **Take Action** dialog box:
  - a. Select the computer(s) where you want the BigFix Firewall deployed.
  - b. Set any desired options such as for scheduling, messages to users, etc.  
For more information about setting options using the tabs in the Take Action dialog box, consult the *Console Operators Guide*.
  - c. Click **OK** when you are finished.
5. Enter your **Private Key Password** to continue. An Action window will appear, allowing you to track the progress of your deployment.
6. Restart the client computers using the BigFix Console.

For more information about restarting computers using the BigFix Console, see the *Console Operators Guide*. After restarting, your deployment will be complete.

## Updating BigFix Firewall

BigFix provides a Fixlet to update BigFix Firewall.

You should check the **Update BigFix Firewall** link periodically to see if it has been updated; BigFix recommends once a week. Use this Fixlet message to look at the number of relevant computers, or set up a scheduled report in web reports that tells you when the number of computers relevant to the Fixlet has passed a threshold that you can set.

1. From the Dashboard, click the **Update BigFix Firewall** link.

The **BigFix Firewall—Update** Fixlet window opens.

2. Click the **here** hyperlink located in the **Actions** section.

The **Take Action** dialog box opens.

3. In the **Take Action** dialog box:

- a. Select the computers on which you would like to update BigFix Firewall.
- b. Set any desired constraints and other options.
- c. Click **OK** when you are finished.

4. Enter your Private Key Password.

An Action window appears, in which you can track the progress of the update.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

## Setting Policies Using the BigFix Firewall Wizards

BigFix Firewall works in two distinct modes. You can statically load a policy file, or you can dynamically load policies based on machine state. When no policy is applied, the default is to allow all traffic. Use the Wizards to create policies.

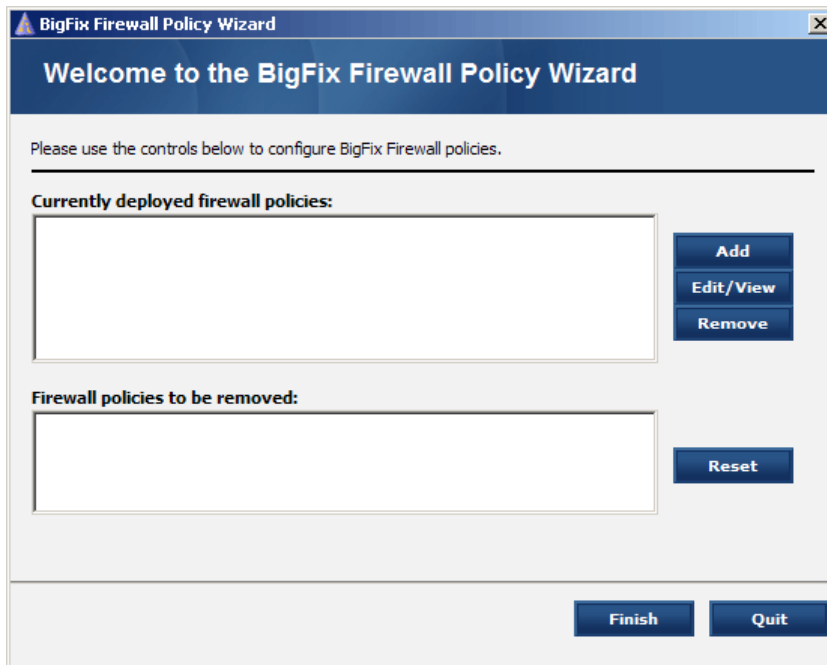
### Configuring Firewall Policies

Use the BigFix Firewall Policy Wizard to create firewall policies, and then apply these policies using the generated task. This is also where you specify zone rules, which allow you to implement interface-level blocking. You can designate certain interfaces as safe and others as dangerous. You can then make firewall rules that apply specifically to safe zones, dangerous zones, or both. You might allow FTP over safe interfaces but deny it over dangerous interfaces. Your VPN adapters could then be all in the safe zone while your wireless adapters could be in the dangerous zone. You put adapters in a zone by using a string match against the interface name (case sensitive, partial match starting from the left).

To configure firewall policies:

1. From the Dashboard, click the **Configure BigFix Firewall** link or select **Wizards > BigFix Firewall Policy Wizard**.

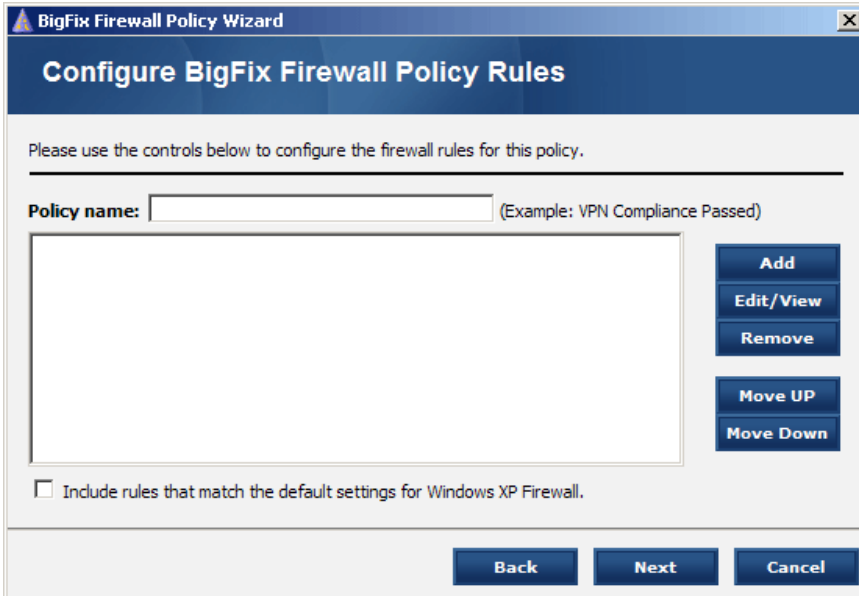
The **BigFix Firewall Policy Wizard** opens.



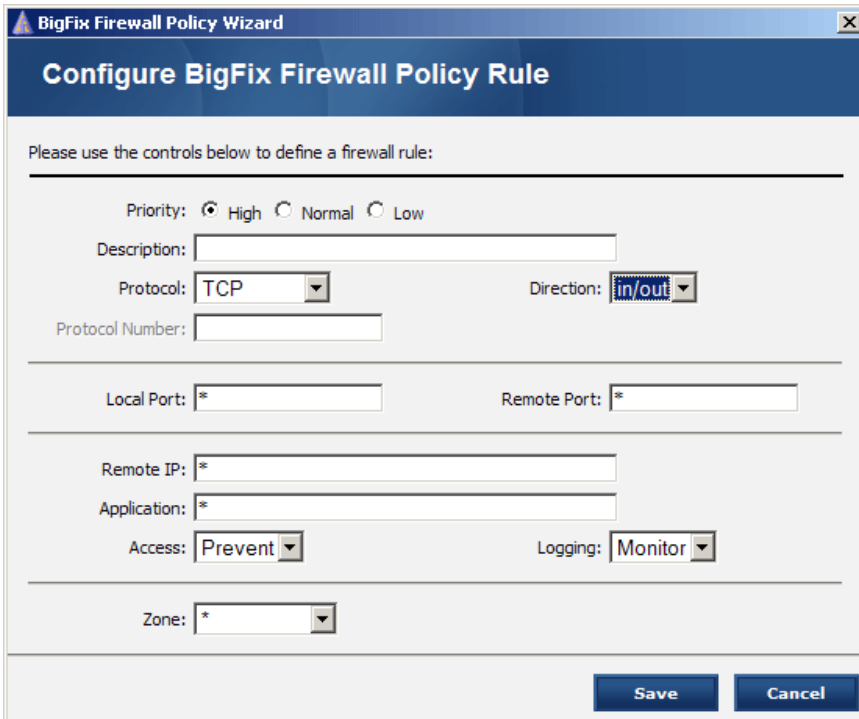
2. When you bring up the first screen of the Wizard, you may see a message that reads: “**The analyses necessary to display deployed policies and available network devices are not activated.**” This message appears whenever the Deployed Firewall Policies analysis is not active. Click the link to reactivate the analyses.
3. To add a new policy, click the **Add** button.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

The **Configure BigFix Firewall Policy Rules** window opens.



4. Provide a **Policy name** that will describe the set of firewall and zone rules you are about to define, and then click the **Add** button to create the rules themselves. The **Configure BigFix Firewall Policy Rule** window opens.





## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

5. In the **BigFix Firewall Policy Rule** window:

- a. Choose the **Priority** for your rule (High, Normal or Low).
- b. Enter a **Description** for your rule.
- c. Choose the applicable **Protocol**: TCP, UDP, TCP\_UDP or Other. If Other is selected provide the appropriate protocol number
- d. Choose the **Direction** for your rule: In, Out, or Both.
- e. In the **Local Port**, **Remote Port**, **Remote IP**, and **Application** fields you can enter specific values or leave the default wildcard (\*).
- f. Choose whether to Allow or Prevent **Access** to the Remote IP or Application.
- g. Choose whether to turn on (monitor) **Logging** or ignore it. Note that logging is an option only if you are defining a prevention rule (Access = Prevent).
- h. Designate this rule to be either in a Safe or Dangerous zone. A rule that is not designated for a particular zone applies to both zones.
- i. Click **Save**.

Add additional rules by repeating these steps. The new rules you add will show up in the list on the first page of the Wizard.

BigFix Firewall Policy Wizard

### Configure BigFix Firewall Policy Rules

Please use the controls below to configure the firewall rules for this policy.

**Policy name:**  (Example: VPN Compliance Passed)

Test rule prevents port 80  
Prevent port 80 safe zone  
Prevent port 80 danger zone

**Add**  
**Edit/View**  
**Remove**  
**Move UP**  
**Move Down**

☐ Include rules that match the default settings for Windows XP Firewall.

**Back** **Next** **Cancel**

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

6. Check the box if you wish to include rules that match Windows XP Firewall default settings. This will add several rules to your list.

The screenshot shows the 'Configure BigFix Firewall Policy Rules' window. At the top, it says 'Please use the controls below to configure the firewall rules for this policy.' Below this is a 'Policy name' field containing 'XP Rules' and a hint '(Example: VPN Compliance Passed)'. A list box contains the following rules: 'File and Printer Share TCP\_139', 'File and Printer Share TCP\_445', 'File and Printer Share UDP\_137', 'File and Printer Share UDP\_138', 'Remote Desktop TCP\_3389', 'UPnP Framework TCP\_2869', and 'UPnP Framework TDP\_1900'. To the right of the list are buttons for 'Add', 'Edit/View', 'Remove', 'Move UP', and 'Move Down'. At the bottom left, there is a checked checkbox labeled 'Include rules that match the default settings for Windows XP Firewall.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

This set includes all the XP defaults with the exception of ICMP, which can conflict with proper BigFix communication.

7. Use the **Move Up/Down** buttons to change the order of the rules. Typically, rules are sorted by other criteria, but the order defined here can be used to break ties.
6. Click **Next** to continue on to the Zone Rules, which enable you to implement interface-level blocking.

The screenshot shows the 'Configure BigFix Firewall Policy Zone Rules' window. It says 'Please use the controls below to configure the zone rules for this policy.' Below this, it says 'Zone rules for policy: Basic.' and shows an empty list box. To the right are buttons for 'Add', 'Edit/View', 'Remove', 'Move UP', and 'Move Down'. At the bottom left, there is an unchecked checkbox labeled 'Create a one-time action. Leave this unchecked to create a Task you can reuse.' At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

7. Click the **Add** button to bring up the Zone Rule interface.

The screenshot shows a window titled "BigFix Firewall Policy Wizard" with a sub-header "Configure BigFix Firewall Policy Zone Rule". Below the header, it says "Please use the controls below to define a firewall zone rule:". There are three input fields: "Description:" with the value "Safe 1394" and "(Optional)" to its right; "Zone:" with a dropdown menu showing "Safe"; and "Network Device Name:" with the value "1394". Below these fields, a text box contains the text: "The following network devices in your environment will match this zone rule. Matching is case-sensitive and starts from the left." followed by a list box containing "1394 Net Adapter" and "1394 Net Adapter #2". At the bottom right are "Save" and "Cancel" buttons.

8. Create a Zone Rule by filling out the form:

- Provide the zone rule with an optional **Description**.
- Mark this zone as **Safe** or **Dangerous**.
- Enter the name of a **network device** for this zone. The name is used for a substring match starting from the leftmost character, so 1394, for instance, will match all similar adapters.
- Click **Save**.

The starting Zone rule screen is displayed.

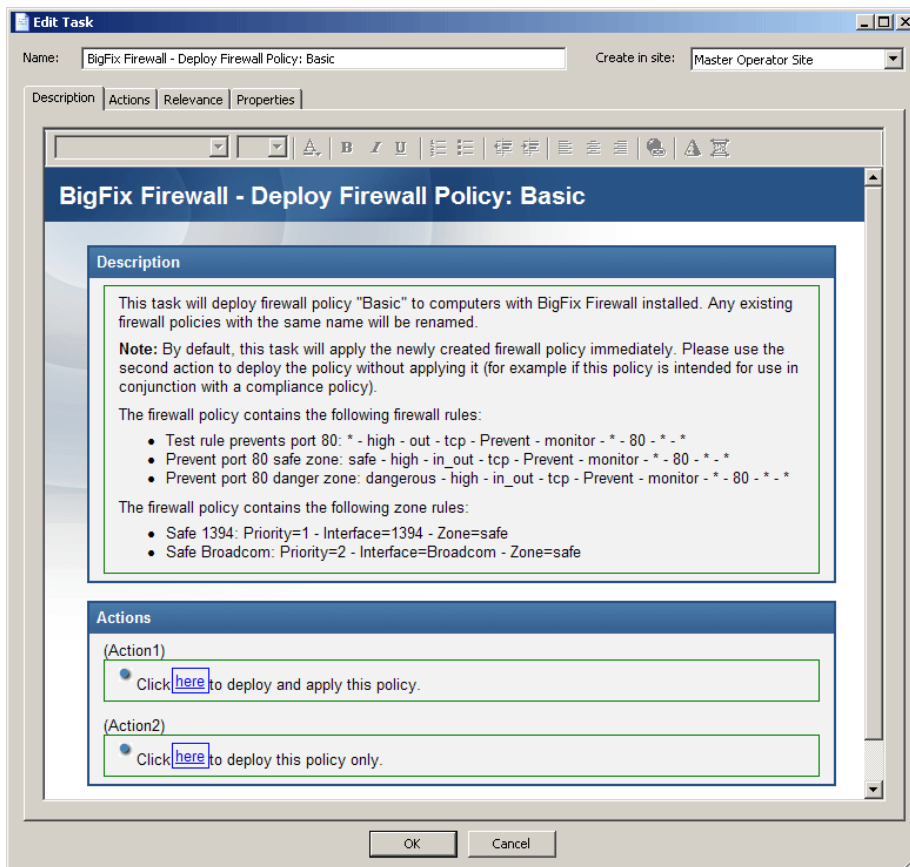
The screenshot shows a window titled "BigFix Firewall Policy Wizard" with a sub-header "Configure BigFix Firewall Policy Zone Rules". Below the header, it says "Please use the controls below to configure the zone rules for this policy.". There is a section titled "Zone rules for policy: Basic." containing a list box with two entries: "Safe 1394" and "Safe Broadcom". To the right of the list box are four buttons: "Add", "Edit/View", "Remove", and "Move UP" above "Move Down". At the bottom left, there is a checkbox labeled "Create a one-time action. Leave this unchecked to create a Task you can reuse.". At the bottom right are "Back", "Finish", and "Cancel" buttons.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

Repeat these steps to add new zones to the list. You can sort the list by highlighting a rule and then clicking the **Move Up/Down** buttons. Order is important when matching interfaces to a zone rule. The first zone rule that matches an interface will be used to categorize that interface.

9. Check the box to create a **one-time action**. To create a persistent Task that you can reuse, leave the box unchecked. If you select a one-time action, you will be taken to the Take Action dialog box, in which you can target any machines to which to apply your policy and choose other deployment options.
10. Click **Finish**.

If you selected a one-time action in the previous step, you are presented with a **Take Action** dialog box, in which you can target any machines to which to apply your policy and choose other deployment options. Otherwise, an **Edit Task** window opens, summarizing your policy.



The Task description lists the firewall and zone rules you have just defined. The Edit Task dialog allows you to modify the appearance of the Task, including fonts, sizes and styles. Simply highlight the sections of text you want to modify and use the toolbar above the Task to make the desired changes. Click the **Action** tab to examine the Action that will run when this Task is activated. Click the **Relevance** tab to examine the Relevance clause that will trigger the Task. Note that it will not be activated until all the necessary services are running.

The Task includes two Action buttons. One button allows the operator to deploy and apply the policy; the other lets you deploy the policy without applying it. Use the second action if you intended to load this firewall policy via a client compliance policy.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

11. Select the **site** you want this Task to reside in from the pull-down menu, upper right. The default is your operator site.
12. When you are satisfied with your Task, click **OK** and enter your private key password to propagate it. Once deployed, you can view the Task in the Console by clicking the Task tab and selecting the Site you placed it in from the left filter panel.

## Configuring Client Compliance Policies

BigFix Firewall enables you to load different dynamic firewall policies based on the state of an endpoint. For example, you might have one firewall policy for use when an endpoint is connected to VPN, another for when it is connected to the company LAN, and a third for when the endpoint is off the LAN. Alternatively, you might have one firewall policy for machines that satisfy your company's security policies, e.g. current patches and virus definitions, and a different firewall policy for machines that fail your compliance check.

To set up dynamic loading of firewall policies, you use client compliance policies to define criteria under which each different firewall policy is loaded. Each client compliance policy is mapped to a particular firewall policy.

When you map a Client Compliance Policy to a Firewall Policy, you must assign the mapping a priority level. Mappings are evaluated in priority order, from highest to lowest. If you deploy a new mapping with the same priority as an existing installed mapping, the new mapping will replace the old one. Typically, the highest priorities map to the least restrictive firewall rules and the lowest priority will have the most restrictive firewall rules. There is no limit to the number of compliance policies you can have, but each must have a unique priority.

**Note:** When setting dynamically-loaded Firewall policies using client compliance documents, the lowest priority compliance document should always evaluate successfully. To ensure that a known Firewall policy is always loaded, create as your lowest priority mapping a compliance policy that contains a single custom QuickEval check where the relevance is "true". If all compliance documents fail to evaluate successfully, the behavior of the Firewall is "undefined" and the last loaded policy will remain in effect.

BigFix Firewall will load the firewall policy that maps to the first client compliance document that evaluates successfully. Successful evaluation is defined as all compliance checks evaluating to TRUE.

You create client compliance policies using the **BigFix Client Compliance Policy Wizard**. You can create four different types of client compliance checks. When a compliance document is evaluated, its checks are sorted by type. Internal to each type, checks are evaluated in the order in which they are listed. The types are evaluated in the following sequence:

- **QuickEval:** This type of check uses a relevance expression that returns a singular Boolean value. QuickEval compliance checks are evaluated using a locally loaded version of the relevance engine. The majority of client compliance checks are QuickEval.
- **VPN:** This type of check ensures that there is an active network adapter whose name matches the supplied adapter name.
- **Hostname:** This type of check performs an nslookup query using the hostname to ensure that the hostname resolves to a particular provided IP address. This check is useful for determining network location. For example, you would use a hostname that is only resolvable on the internal company network to determine that the client is connected via VPN or LAN.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

- **Client Context:** This check uses a relevance expression that returns a singular Boolean value. Client context queries evaluate expressions that require knowledge specifically available to the BigFix Client. For example, “How many critical Fixlets are currently relevant?” or “What is the distance to my relay?” These queries are parsed to the BigFix Client for evaluation and have a 60-second timeout.

There is no limit to the number of compliance checks you can put in a compliance document. However, to ensure speedy switching among policies, follow these guidelines:

- Limit the number of checks as much as possible.
- Use QuickEval as much as possible.
- Use the Relevance Debugger to ensure that your queries do not take a long time to evaluate.
- Put checks you expect to fail most frequently first.
- If possible, avoid Client Context checks.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

The following is a sample compliance document containing all four types of compliance checks:

```
<?xml version="1.0"?>
<BESClientComplianceDocument Version="1.0">
  <ComplianceItem>
    <Designator>true</Designator>
    <VPN>SafeNet Virtual Adapter Interface</VPN>
    <Expression>True</Expression>
    <Description>true</Description>
    <Comment>true</Comment>
  </ComplianceItem>
  <ComplianceItem>
    <Designator>DNSCheck</Designator>
    <Host>bigdisk.bigfix.com=192.168.104.10</Host>
    <Expression>True</Expression>
    <Description>bigdisk.bigfix.com must resolve to 192.168.104.10 from the client
computer</Description>
    <Comment>Compliant if True</Comment>
  </ComplianceItem>
  <ComplianceItem>
    <Designator>NumCritical</Designator>
    <Expression>10 &gt;= number of relevant fixlets whose (value of header "x-fixlet-
source-severity" of it as lowercase = "critical") of sites</Expression>
    <Description>Total number of relevant critical patches must be less than
10</Description>
    <Comment>Compliant if True</Comment>
  </ComplianceItem>
  <ComplianceItem>
    <Designator>OSRequirement</Designator>
    <Expression>(name of operating system = "Win2000" AND csd version of operating
system &gt;= "Service Pack 4") OR (name of operating system = "WinXP" AND csd version of
operating system &gt;= "Service Pack 1") OR (name of operating system =
"Win2003")</Expression>
    <Description>Win2K OR WinXP OR Win2003</Description>
    <Comment>Compliant if True</Comment>
    <QuickEval>true</QuickEval>
  </ComplianceItem>
</BESClientComplianceDocument>
```

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

To configure a Client Compliance Policy:

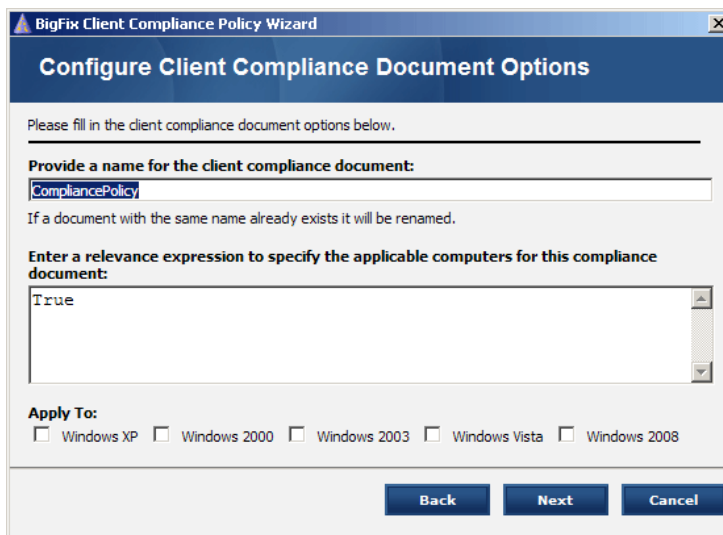
1. Choose **Wizards > Client Compliance Policy Wizard**.

The **Client Compliance Policy Wizard** opens.



2. When you bring up the first screen of the Wizard, you may see a message that reads: “**The analyses necessary to display deployed policies and available network devices are not activated.**” This message appears whenever the Deployed Firewall Policies or the Configuration Information analysis is not active. Click the link to reactivate the analyses.
3. Click the **Add** button.

The **Configure Client Compliance Document Options** window opens.



4. In this window:
  - a. **Name** your Client Compliance Document.
  - b. Enter a **relevance expression** to specify the applicable computers for this document (the default Relevance expression is True).



## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

- c. Check the Windows XP, 2000, 2003, Vista or 2008 buttons if appropriate. The default is to apply it to all operating systems. When you select one of the operating systems, an appropriate Relevance expression will be inserted in the text box.
- d. Click **Next**.

The **Configure Firewall Policy Options** window opens.

The screenshot shows the 'Configure Firewall Policy Options' window of the BigFix Client Compliance Policy Wizard. The window has a title bar with the BigFix logo and the text 'BigFix Client Compliance Policy Wizard'. Below the title bar is a blue header with the text 'Configure Firewall Policy Options'. The main content area contains the following elements:

- A paragraph of text: 'If you would like to enforce a firewall policy when this client compliance document evaluates successfully, you can use the controls below to specify the mapping. Use the [BigFix Firewall Policy Wizard](#) to view more details of currently deployed firewall policies.'
- A section titled 'Firewall policy to enforce when compliant:' with a drop-down menu currently showing '<none>'.
- A section titled 'Specify a hostname that must resolve to be considered compliant:' with a checkbox, a text box containing 'dnsHost.mycompany.com', and a text box containing '10.10.10.10'.
- A section titled 'Set a priority level for this client compliance policy to firewall policy map:' with a text box containing '100'.
- A section titled 'Existing mappings:' containing a table with three columns: 'Priority', 'Compliance Policy', and 'Firewall Policy'. The table is currently empty.
- A paragraph of text: 'Policies will be evaluated in order from highest to lowest. The minimum priority is 0. New policy mapping will replace existing mappings with the same priority.'
- At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

5. In this window:

- a. Choose which **Firewall policy** to enforce when compliant. Note that Firewall policies will not appear in the drop-down list until the policy has been deployed to at least one client.
- b. If you wish, specify a **hostname** that must resolve to be compliant.
- c. Set a **priority level** for this compliance policy to firewall policy map. The window will show your existing mappings.
- d. Click **Next**.

The **Configure Basic Compliance Options** window opens.

BigFix Client Compliance Policy Wizard

Configure Basic Compliance Options

Please configure any basic checks that must pass to be considered compliant.

☐ Maximum number of relevant critical patches:

10

☐ Minimum service pack level for Windows 2000:

Service Pack

4

☐ Minimum service pack level for Windows XP:

Service Pack

2

☐ Minimum service pack level for Windows 2003:

Service Pack

2

☐ Minimum service pack level for Windows Vista:

Service Pack

1

☐ Minimum service pack level for Windows 2008:

Service Pack

0

☐ Maximum age of any relevant critical patch:

In day(s)

30

☐ Name of a process required to be running:

DefWatch.exe

Back

Next

Cancel

6. Select and configure any basic checks that must pass, and then click **Next**.

The **Configure AntiVirus Compliance Options** window opens.

BigFix Client Compliance Policy Wizard

Configure AntiVirus Compliance Options

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

☐ BigFix AntiVirus:

☐ eTrust Anti-Virus 7.x:

☐ eTrust Anti-Virus 6.x:

☐ McAfee VirusScan 8i/8.5i:

☐ McAfee VirusScan 7.x:

☐ McAfee VirusScan 6.x:

☐ Symantec Anti-Virus Corporate or Endpoint Protection:

☐ Sophos Anti-virus 6.x:

☐ TrendMicro OfficeScan 7.x:

Maximum AntiVirus Definition Age

10 day(s)

10 day(s)

10 day(s)

10 day(s)

10 day(s)

10 day(s)

10 day(s)

10 day(s)

10 day(s)

Back

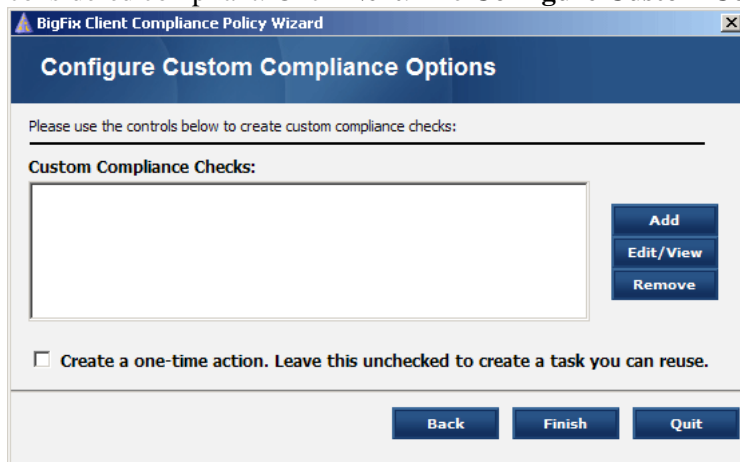
Next

Cancel

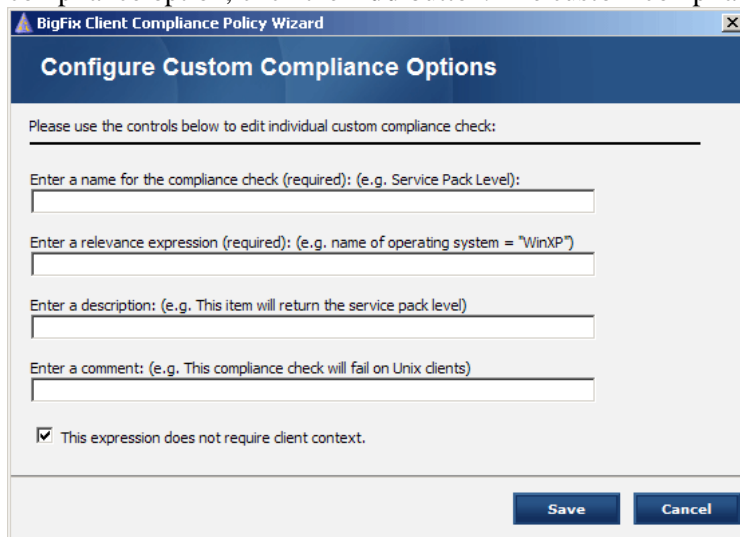
© 2008 by BigFix, Inc.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

7. Specify any antivirus applications required and the maximum definition age for a computer to be considered compliant. Click **Next**. The **Configure Custom Compliance Options** window opens.



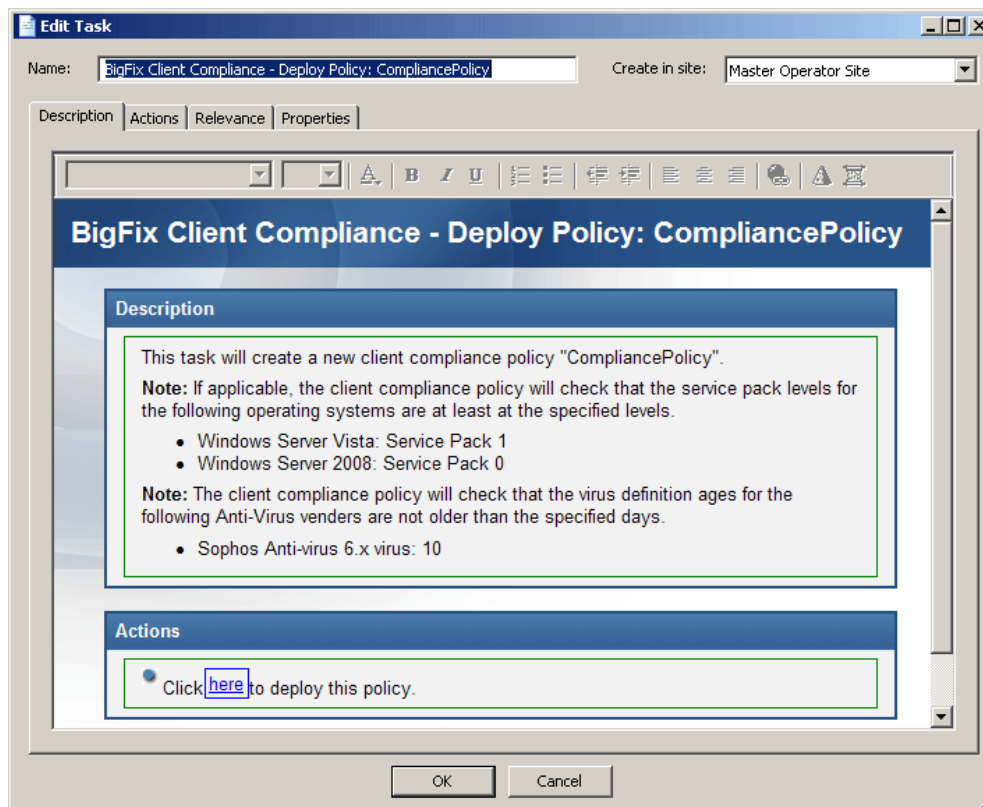
8. In this window, you can add, edit, or remove any custom compliance checks you want. To add a compliance option, click the **Add** button. The custom compliance dialog opens.



9. Enter the field values to describe your custom compliance check:
- e. Create a **name** for the compliance check.
  - f. Enter a **relevance** clause to trigger the check.
  - g. Create a short **description**.
  - h. You can also enter an optional **comment**.
  - i. Check the box if your relevance expression does not require client context. This toggles quick evaluation on and off.
  - j. Click **Save** to finish the definition of your custom compliance check.
10. Your newly defined compliance check will be added to the list. Leave the check box unchecked to create a reusable Task, or check the box to create a **one-time action**.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

11. Click **Finish**. If you selected a one-time action in this step, you will see a **Take Action** dialog box, where you can target any machines with this policy and choose other deployment options. Otherwise, you will be taken to an **Edit Task** dialog box, where you can edit descriptions and other parameters of the Client Compliance Task.



12. As with the Firewall Policy Task, this interface describes the parameters you entered in the Wizard and lets you edit the look and feel of the Task using the toolbar at the top. Click on the various tabs to examine and modify the Actions, Relevance and Properties. Using the pull-down menu at the top, select the site you wish to contain this Task. When you are satisfied with the Task, click the **OK** button and provide your private key password to deploy it.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

## Enabling Client Compliance

Once you have created and deployed your Firewall and Client Compliance policies, you are ready to turn on client compliance evaluation. This will switch the firewall into dynamic mode.

1. From the Dashboard, click the **Change Compliance Evaluation Settings** link.  
The **Configure Client Compliance Evaluation** Task window opens.
2. Click the link to enable client compliance evaluation located in the **Actions** section.  
The **Take Action** dialog box opens.
3. In the **Take Action** dialog box:
  - a. Select the computers on which you would like to turn on client compliance.
  - b. Set any desired constraints and other options.
  - c. Click **OK**.
4. Enter your **Private Key Password**.  
An Action window appears, in which you can track the progress of the action.

## Enabling Dynamic Loading of Firewall Policies

There are a number of steps detailed in the preceding sections required to enable dynamically-loaded Firewall policies based on client state. The following represents a summary of the procedure:

1. Deploy BigFix Firewall.
2. Create firewall policies you would like to enforce using the **Firewall Policy Wizard**:
  - a. Do not check the **apply immediately** box.
  - b. Do not check the **one-time action** box.
3. Deploy your firewall policies to at least one machine.
4. Create compliance policies using the Compliance Policy Wizard, mapping each to a firewall policy.
  - a. Set unique priorities for each mapping.
  - b. Set priorities so that the highest priority is the mapping you would like evaluated first, and so on.
  - c. Make sure your lowest priority mapping has a single custom compliance check of type QuickEval, with relevance 'true' and no other compliance checks.
5. Deploy your compliance policies to at least one machine.
6. Turn on client compliance evaluation using the **Configure Client Compliance Evaluation Task**.
7. Test that all the compliance states behave as expected.
8. Once you are satisfied that everything is working correctly, create a baseline using the Fixlets and Tasks from steps 1-6.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

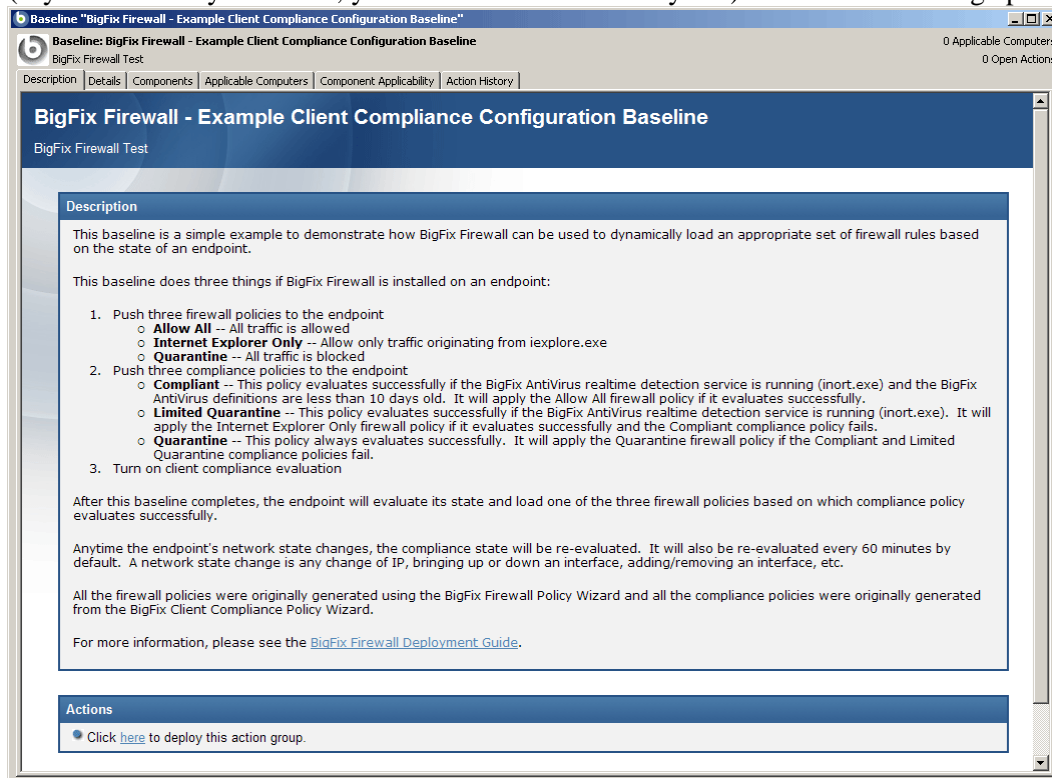
- Using the baseline Action, target machines on which you would like to enforce dynamic firewall policies. This Action will deploy BigFix Firewall, your firewall policies, your compliance policies, and turn on client compliance evaluation.

## Using the Example Client Compliance Configuration Baseline

A baseline is included with the BigFix Firewall site. It provides an example configuration with three firewall policies and three corresponding compliance policies. After you deploy it to a client the policies will appear in the wizards.

Follow these steps to run the baseline:

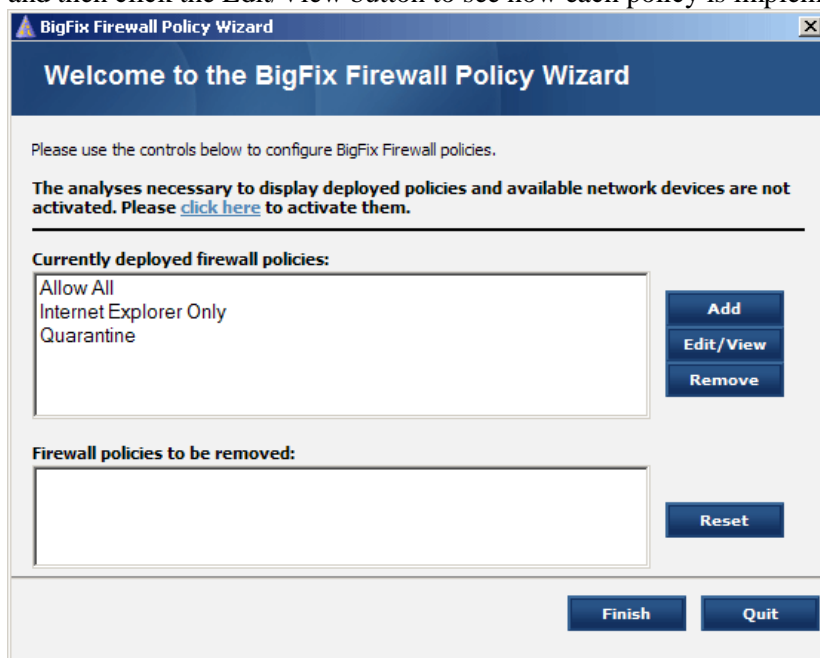
- Click the Baselines tab in the Console and select the Example client compliance configuration baseline (if you have many baselines, you can filter them down by site). The baseline dialog opens.



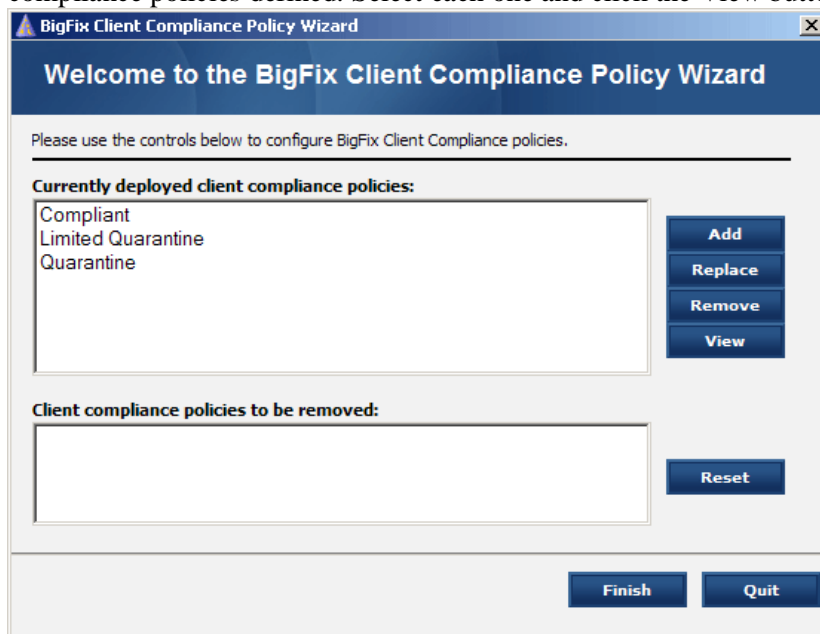
- Click the Action link to deploy the action group.

## SETTING POLICIES USING THE BIGFIX FIREWALL WIZARDS

3. Select the BigFix Firewall Policy Wizard from the Wizards menu. Note that there are now three new firewall policies available. These represent three different levels of firewall security. Select each one and then click the Edit/View button to see how each policy is implemented.



4. Select the BigFix Compliance Policy Wizard from Wizards menu. Note that there are three new compliance policies defined. Select each one and click the View button to see how it is implemented.



By studying these examples, you can see how to establish firewall and zone rules and then combine them with Client compliance to create a highly-granular security policy.

## Performing Additional Tasks

---

There are a number of additional tasks available from the BigFix Firewall Dashboard:

### Uploading BigFix Firewall Logs

Use this Task if you want to instruct a machine to upload its Firewall logs to the BigFix server. After the log files have been uploaded, you will find them in the following path: <server installation directory>\UploadManagerFiles\BufferDir\sha1\<last 2 digits of client ID>\<client ID>.

Note that Firewall logs can become very large and, therefore you should not apply this action as a policy or to a large number of machines. If you do, you risk impacting you network and/or BigFix Server.

### Changing Compliance Evaluation Settings

BigFix Firewall can be configured to load different firewall policies based on the results of evaluating client compliance documents. Typically the evaluation happens on every network state change and on a specified interval. The default interval is 60 minutes.

Use this Task to request an immediate compliance evaluation, change the periodic evaluation interval, or enable/disable client compliance evaluation.

### Ensuring BigFix Clients Can Communicate

By default, BigFix Firewall will insert firewall rules to allow inbound UDP and outbound TCP on the BigFix port (typically port 52311) for the application BESClient.exe. BigFix Firewall will also insert rules to allow inbound and outbound ICMP so that the BigFix Client can perform automatic relay selection and calculate the 'Distance to BES Relay' property.

In addition, BigFix Firewall will insert rules to allow outbound UDP on port 53 for BESClient.exe to resolve hostnames for BigFix Relays and/or Servers. Finally, BigFix Firewall will insert a rule to allow inbound TCP and outbound TCP and UDP on the BigFix port for the application BESRelay.exe.

Computers relevant for this Fixlet message have overridden the default behavior and may load firewall policies that block the BigFix client from communicating normally. It is recommended that you issue a policy action using this Fixlet to ensure the BigFix client can always communicate successfully.

For more information on BigFix network traffic, see: <http://support.bigfix.com/bes/misc/networktraffic.html>

### Disabling Windows Firewall

Use this Task to turn off Windows Firewall. It is recommended that you take this as a policy action, targeted at all machines with BigFix Firewall installed. Multiple firewalls installed and active on a machine can lead to unexpected behavior.



## ADVANCED SETTINGS

## Advanced Settings

---

There is usually no need to override the default settings for network traffic, but in certain circumstances the following advanced settings are available to be set under the registry key “HKLM\Software\BigFix\Firewall”:

Value Name	Default Value	Description
BESICMPOpen	1	If set to 0, a rule will not be added to always allow ICMP traffic necessary for BigFix Client communication. Anything other than 0 is treated as 1.
BESPortOpen	1	If set to 0, a rule will not be added to always allow TCP/UDP traffic on the BigFix Port (default 52311) necessary for BigFix Client communication. Anything other than 0 is treated as 1.
DNSOpen	1	If set to 0, a rule will not be added to always allow traffic on the DNS port (53) necessary for DNS resolution. Anything other than 0 is treated as 1.
LogPreventAndAllow	0	If set to 1, BigFix Firewall will log all traffic, including allowed packets. The default (0) is to only log blocked traffic. Anything other than 1 is treated as 0. WARNING: This setting will likely result in very large log files and should not be left on for extended periods.
NetBIOSOpen	0	If set to 1, a rule will be added to always allow NetBIOS traffic (UDP port 137). Anything other than 1 is treated as 0.

## FIREWALL RULE SORTING

## Firewall Rule Sorting

---

Firewall rules are sorted using the following steps. Note that some functionality listed below is not exposed through the Firewall Policy Wizard interface.

1. Rules are divided into 5 groups: `PRIOR_HIGH` (preferred), `PRIOR_HIGH`, `PRIOR_NORMAL`, `PRIOR_LOW` (preferred), `PRIOR_LOW`.
2. Rules are sorted by application in the sequence of label, group, and then All Applications (\*). Order within labels is determined alphabetically as is order within groups.
3. Rules are sorted by transport object in the following order:
  - a. Protocol—in the sequence of `PROT_TCP`, `PROT_UDP`, `PROT_TCP_UDP`, `PROT_ICMP`, `PROT_OTHER`, and `PROT_ALL` (\*).
  - b. Direction—in the sequence of `DIR_IN`, `DIR_OUT`, `DIR_IN_OUT`.
  - c. Ports or ICMP codes—port intervals that are subsets of another interval have higher priority. For all other intervals the order is determined by the order in which the rules are listed. Local ports are sorted before remote ports. ICMP codes are sorted such that `ICMP_ALL` will be last. For all other ICMP codes the order is determined by the order in which the rules are listed. If protocol is `PROT_OTHER`, the same logic is applied as for ports.
4. Rules are sorted by remote IP address. Addresses that are subsets of another set of addresses have higher priority. In all other cases the order is determined by the order in which the rules are listed.
5. Rules are sorted by time of day. An interval that is a subset of another interval has higher priority. For all other time of day rules the order is determined by the order in which the rules are listed.
6. If two otherwise exactly the same rules are present, except that one is Prevent and the other is Allow, Prevent takes precedence.
7. If rules remain tied after the sorting steps above, the order they appear in the rule list will determine precedence

## Frequently Asked Questions

---

### General Questions

#### **Can I get a centralized view and control of my Firewall efforts?**

Yes. You can centrally manage (control and report) up to 250,000 endpoints with a single BigFix Server. Centralized reporting at larger scale is fully supported with multiple BigFix servers.

#### **In what environments can BigFix Firewall be installed?**

BigFix Firewall supports 32-bit Microsoft Windows 2000, Server 2003, XP, Vista, and Server 2008.

#### **Does BigFix Firewall support multi-site, cross-domain deployment?**

Yes.

#### **What type of Firewall configuration reporting does BigFix Firewall provide?**

BigFix Firewall provides Dashboard views showing where it is deployed, what policies are in place and a variety of other information via the control Dashboard and BigFix Web Reports.

#### **How do I get logs to my archive / SIM?**

You can use the Upload Logs task to send logs periodically to the BigFix server. Once the files are on the server they can be parsed easily for entry into a SIM, or moved off the server to another location for further processing or storage.

#### **How do I apply different firewall policies based on the location of the device?**

BigFix Firewall has extremely granular ability to examine the state and location of a machine. You can easily map different client states and locations to particular firewall policies using the Client Compliance Policy Wizard. See the “Configuring Client Compliance Policies” section of this document for further details.

#### **Can BigFix Firewall create application-specific firewall policies?**

Yes.

#### **Does BigFix Firewall provide buffer overflow and/or HIPS functionality?**

These capabilities are planned for a forthcoming release of BigFix Firewall.

#### **Can I deploy different firewall policies based on role?**

Yes, you can assign as many or as few firewall policies as you like and deploy them based on a variety of criteria including, but not limited to: network location, AD OU membership, operating system, logged-in user, connection type, and more.

#### **Can I rollback a new firewall policy?**

Yes, BigFix Firewall versions all firewall policy changes, allowing for rapid rollback if a policy is found to conflict with the operational environment.

#### **How can I be sure my firewall policy will not cut off BigFix client communication?**

BigFix Firewall has been carefully tested to ensure that client communication will always remain intact, even if a policy has been applied that would normally block BigFix traffic. Regardless what rules are specified, BigFix Firewall will always insert rules with higher priorities that are designed specifically to allow BESClient.exe and

## FREQUENTLY ASKED QUESTIONS

BESRelay.exe to communicate normally. In addition, there is a Fixlet message that can be taken as a policy action to ensure that any machines overriding the default settings allowing BigFix communication will be switched back to the default behavior.

**Can BigFix Firewall block traffic on specific network adapters and/or connection type?**

Yes, it is possible to block traffic on specific network adapters and/or connection types by creating zone rules as part of your firewall policies.

## Reporting

**Can I export report data?**

Yes.

**Does BigFix Firewall provide a dashboard view containing high-level statistics?**

Yes.

## ACKNOWLEDGEMENTS AND NOTICES

## Acknowledgements and Notices

---

We would like to acknowledge the individuals and organizations listed below whose software we have included in unmodified form for use with our proprietary software product. Where applicable, we have included notices applicable to such third parties' software and a link to the URL where you can obtain such third party software.

ALL THIRD PARTY SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, AND ALL WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT, ARE HEREBY DISCLAIMED. FURTHER, BigFix, INC. DOES NOT WARRANT RESULTS OF USE OR FREEDOM FROM BUGS OR UNINTERRUPTED USE OR ACCESS. IN NO EVENT SHALL BigFix, INC. BE LIABLE OR OBLIGATED WITH RESPECT TO ANY THIRD PARTY SOFTWARE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION, PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY, SERVICES OR RIGHTS, INTERRUPTION OF USE, LOSS OR CORRUPTION OF DATA, LOST PROFITS OR BUSINESS INTERRUPTION) HOWEVER CAUSED, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The 'zlib' compression library written by Jean-loup Gailly (jloup@gzip.org) and Mark Adler (madler@alumni.caltech.edu) is included with this product. You can obtain the 'zlib' compression library code at <http://www.gzip.org/zlib/>.

This product uses cryptographic software written by Eric Young (eay@cryptsoft.com). This product uses software written by Tim Hudson (tjh@cryptsoft.com). The following notice applies only to such software, which together comprises the 'openssl' library included with this product. You can obtain the 'openssl' library code at <http://www.openssl.org/>.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

## ACKNOWLEDGEMENTS AND NOTICES

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following notice applies only to the 'gd' library software included with this product. You can obtain the 'gd' library code at <http://www.boutell.com/gd/>.

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdtf.c copyright 1999, 2000, 2001, 2002 John Ellson ([ellson@graphviz.org](mailto:ellson@graphviz.org)).

Portions relating to gdft.c copyright 2001, 2002 John Ellson ([ellson@graphviz.org](mailto:ellson@graphviz.org)).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file libjpeg-license.txt for more information.

See also libfreetype-license.txt, libpng-license.txt, zlib-license.txt, and libjpeg-license.txt, all of which are open source licenses compatible with free commercial and noncommercial use, in some cases with minor documentation requirements.

Portions relating to WBMP copyright 2000, 2001, 2002, 2003 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in this version of gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

The PNG Reference Library, 'libpng' is included with this product. You can obtain the libpng code at <http://www.libpng.org/pub/png/libpng.html>.

## ACKNOWLEDGEMENTS AND NOTICES

The following notice applies only to FreeType Project software included with this product. You can obtain the FreeType Project code at <http://www.freetype.org/>.

Portions of this software are copyright © 1996-2002 The FreeType Project ([www.freetype.org](http://www.freetype.org)). All rights reserved.

The following notice applies only to the H3 Library software included with this product. You can obtain the H3 Library code at <http://software.bigfix.com/download/bes/misc/bigfixh3modifications.zip>.

Copyright © 1998, Silicon Graphics, Inc. -- ALL RIGHTS RESERVED

Permission is granted to copy, modify, use and distribute this software and accompanying documentation free of charge provided (i) you include the entirety of this reservation of rights notice in all such copies, (ii) you comply with any additional or different obligations and/or use restrictions specified by any third party owner or supplier of the software and accompanying documentation in other notices that may be included with the software, (iii) you do not charge any fee for the use or redistribution of the software or accompanying documentation, or modified versions thereof. Contact [sitemgr@sgi.com](mailto:sitemgr@sgi.com) for information on licensing this software for commercial use. Contact [munzner@cs.stanford.edu](mailto:munzner@cs.stanford.edu) for technical questions.

SILICON GRAPHICS DISCLAIMS ALL WARRANTIES WITH RESPECT TO THIS SOFTWARE, EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. SILICON GRAPHICS SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST REVENUES, LOST PROFITS, OR LOSS OF PROSPECTIVE ECONOMIC ADVANTAGE, RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the Government is subject to restrictions as set forth in FAR 52.227.19(c)(2) or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and/or in similar or successor clauses in the FAR, or the DOD or NASA FAR Supplement. Unpublished - rights reserved under the Copyright Laws of United States. Contractor/manufacturer is Silicon Graphics, Inc., 2011 N. Shoreline Blvd. Mountain View, CA 94039-7311.

This software includes portions of geomview/OOGL. Copyright (c) 1992 The Geometry Center; University of Minnesota, 1300 South Second Street; Minneapolis, MN 55454, USA

geomview/OOGL is free software; you can redistribute it and/or modify it only under the terms given in the file COPYING, which you should have received along with this file. This and other related software may be obtained via anonymous ftp from [geom.umn.edu](http://geom.umn.edu); email: [software@geom.umn.edu](mailto:software@geom.umn.edu).

The incorporated portions of geomview/OOGL have been modified by Silicon Graphics, Inc. in 1998 for the purpose of the creation of this software.

Original Geometry Center Copyright Notice: Copyright (c) 1993

The National Science and Technology Research Center for Computation and Visualization of Geometric Structures (The Geometry Center): University of Minnesota, 1300 South Second Street Minneapolis, MN 55454 USA email: [software@geom.umn.edu](mailto:software@geom.umn.edu)

This software is copyrighted as noted above. It is free software and may be obtained via anonymous ftp from [geom.umn.edu](http://geom.umn.edu). It may be freely copied, modified, and redistributed under the following conditions:

1. All copyright notices must remain intact in all files.

## ACKNOWLEDGEMENTS AND NOTICES

2. A copy of this file (COPYING) must be distributed along with any copies which you redistribute; this includes copies which you have modified, or copies of programs or other software products which include this software.
3. If you modify this software, you must include a notice giving the name of the person performing the modification, the date of modification, and the reason for such modification.
4. When distributing modified versions of this software, or other software products which include this software, you must provide notice that the original source code may be obtained as noted above.
5. There is no warranty or other guarantee of fitness for this software, it is provided solely "as is". Bug reports or fixes may be sent to the email address above; the authors may or may not act on them as they desire.

If you use an image produced by this software in a publication or presentation, we request that you credit the Geometry Center with a notice such as the following: Figures 1, 2, and 5-300 were generated with software written at the Geometry Center, University of Minnesota.



ACKNOWLEDGEMENTS AND NOTICES

---

**About BigFix, Inc.**

Founded in 1997, BigFix is the category leader in security configuration management software, services, and solutions for real-time visibility and control of computers across the distributed enterprise. BigFix solutions are proven in production at more than 500 companies, government agencies and public sector institutions worldwide and currently manage over 5,000,000 desktop and mobile clients, workstations, and servers. The company has received numerous awards and industry recognitions, including the 2005 Codie Award for "Best Security Product" and the SC Magazine "Product of the Year" recognition in 2004 and eWeek's "Analyst's Choice" award in 2006. For more information, visit [www.bigfix.com](http://www.bigfix.com).

BigFix, Inc.  
1480 64<sup>th</sup> Street Suite 200  
Emeryville, California 94608  
[t] 510 652-6700  
[f] 510 652-6742  
[e] [info@bigfix.com](mailto:info@bigfix.com)  
[e] [sales@bigfix.com](mailto:sales@bigfix.com)

© 2008 BigFix® and the BigFix logo are registered trademarks of BigFix, Inc. All other trademarks are the property of their respective owners.