BigFix™®

BigFix® Firewall Deployment Guide

BigFix, Inc.
Emeryville, CA

Last Modified: 9/6/07

Version 2.0

BigFix, Inc.
1480 64th Street Suite 200
Emeryville, CA 94608-2017

Contents

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 Wizard**: 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
Bold Sans	A bold sans-serif font is used for chapter headers.
Bold text	Bold text typically refers to a program interface.
Italics	Italics are used for BigFix document titles.
`Mono-space`	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

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 advantages include:

- **Real-time visibility and control**:
  - Centralized visibility and reporting at up to very large scale with minimal network and client impact
  - Location and network context-sensitive policy enforcement
  - Management of mobile and remote computers over public networks
  - Digitally signed policies and administrative actions
  - Full change audit trail
- **Rapid time-to-manageability**:
  - Very rapid deployment even in large, complex networks
  - Easy to use with short administrator learning curve
  - Instant-on systems management and security solutions with no additional training
  - Comprehensive available policy libraries including tens of thousands of pre-packaged policies for security and configuration issues including patches, vulnerabilities, security compliance, anti-virus management, and network quarantine
  - Flexible and rapid development of customer-created policies
  - Personalized professional services policy delivery for enterprise needs
- **Reduced total cost of ownership**:
  - Unique distributed real-time architecture with lightweight network impact
  - Highly scalable
  - Leverage existing IT infrastructure
  - Unified infrastructure and single console management
  - Multiple configuration and security solutions delivered via single agent
  - Active directory integration available but not required
  - Public key infrastructure (PKI) for strong security built-in
  - Role-based administration with credential authentication
  - Integration with multiple network access control frameworks including Cisco NAC

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 to request the masthead.

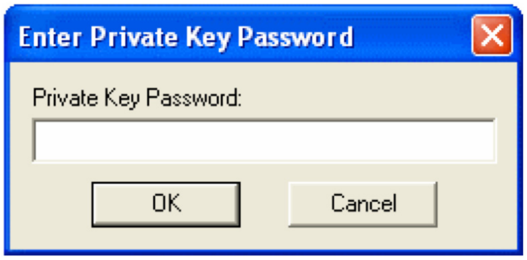
2. Add the BigFix Firewall site:

   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**.

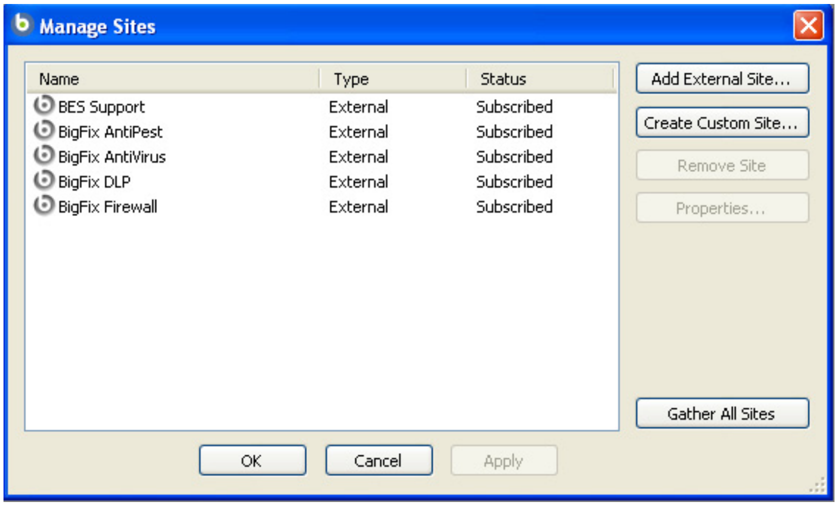


At this point, the BigFix Firewall site will begin the gathering process, in which Fixlets, Tasks, Analyses, etc. are gathered from the central BigFix server.

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.

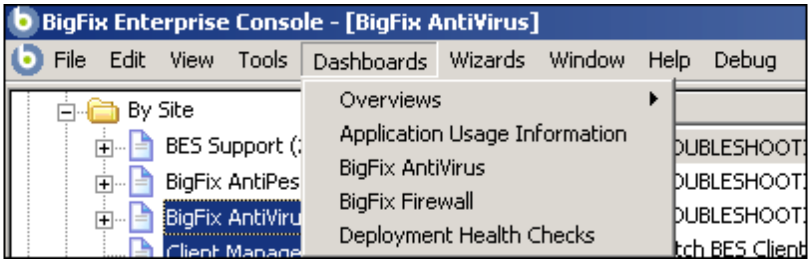


Name	Type	Status
BES Support	External	Subscribed
BigFix AntiPest	External	Subscribed
BigFix AntiVirus	External	Subscribed
BigFix DLP	External	Subscribed
BigFix Firewall	External	Subscribed

Accessing the BigFix Firewall Dashboard

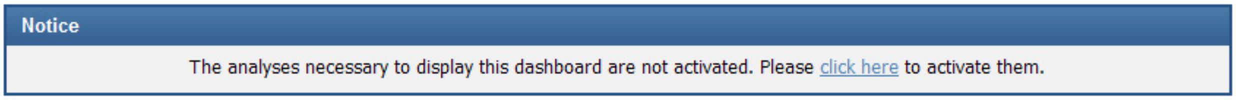
BigFix Firewall provides a dashboard view with overview statistics and charts that enable administrators to gauge the current status of their system and to track statistics as BigFix Firewall enforces Firewall policies throughout the network. In addition, you can use the Dashboard as a central point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

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



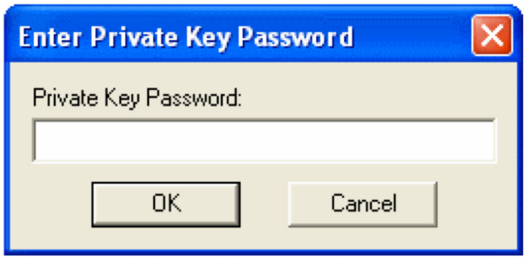
Launching the Dashboard

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


Notice

The analyses necessary to display this dashboard are not activated. Please click here to activate them.

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

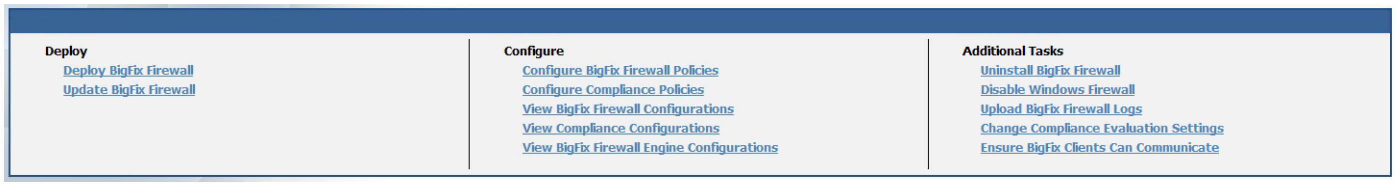


After activation, you might also see a notice to install Office Web Components. If necessary, install Office Web Components following the instructions in the linked Knowledge Base Article.

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

Understanding the BigFix Firewall Dashboard Controls

At the top of the Dashboard, you see the BigFix Firewall Controls:


Deploy
- Deploy BigFix Firewall
- Update BigFix Firewall

Configure
- Configure BigFix Firewall Policies
- Configure Compliance Policies
- View BigFix Firewall Configurations
- View Compliance Configurations
- View BigFix Firewall Engine Configurations

Additional Tasks
- Uninstall BigFix Firewall
- Disable Windows Firewall
- Upload BigFix Firewall Logs
- Change Compliance Evaluation Settings
- Ensure BigFix Clients Can Communicate

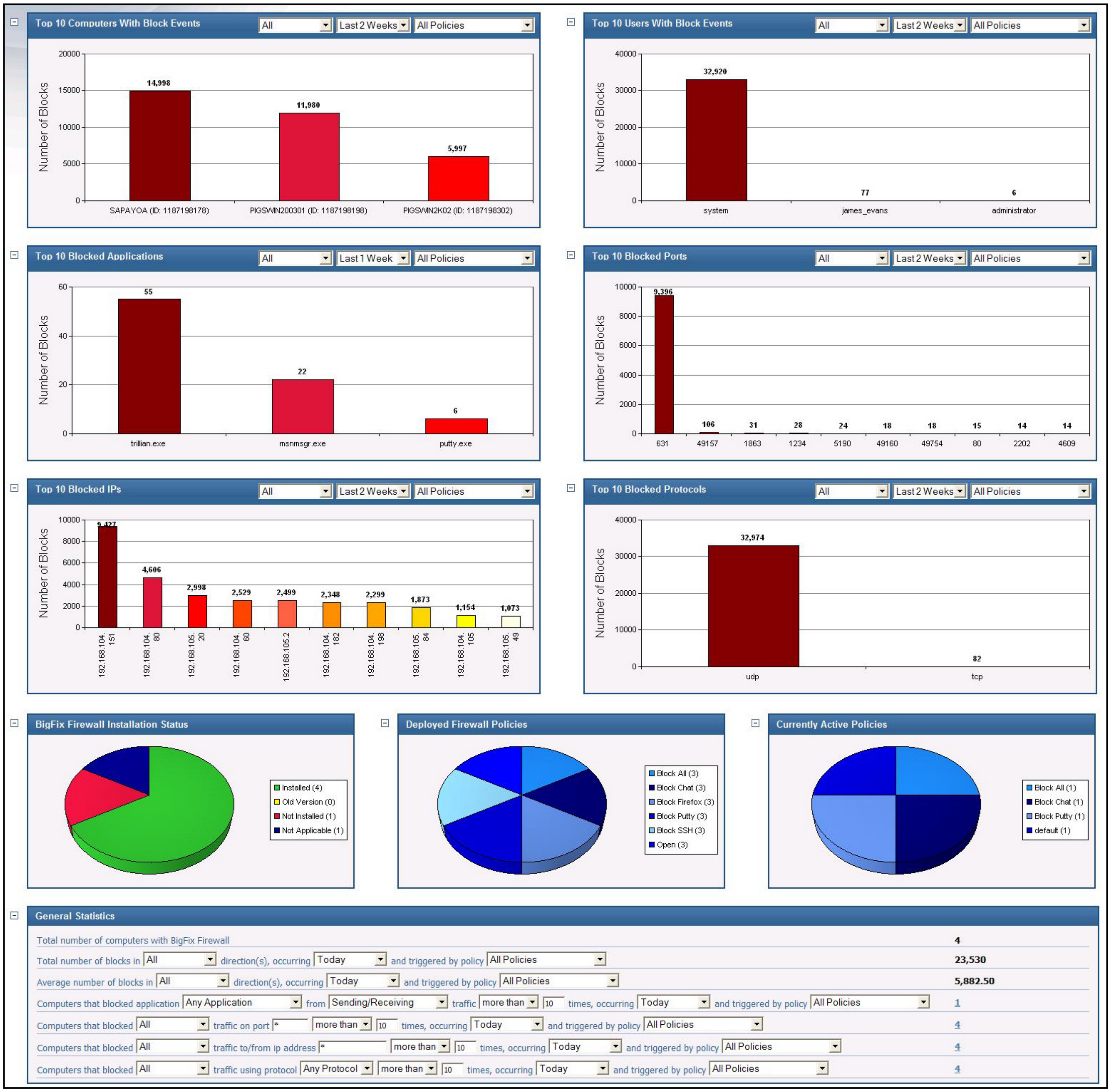
The controls that BigFix Firewall provides are:

- **Deploy**: Use the controls in this section to deploy or update BigFix Firewall.
  - Deploy BigFix Firewall

  - Update BigFix Firewall
- **Configure**: Use the controls in this section to configure BigFix Firewall or to view your existing configurations.
  - Configure BigFix Firewall Policies
  - Configure Compliance Policies
  - View BigFix Firewall Configurations
  - View Compliance Configurations
  - View BigFix Firewall Engine Configurations
- **Additional Tasks**: Use these controls to enable or disable client compliance evaluation and client controls.
  - Uninstall BigFix Firewall
  - Disable Windows Firewall
  - Upload BigFix Firewall Logs
  - Change Compliance Evaluation Settings
  - Ensure BigFix Clients Can Communicate

Reading the Dashboard's Overview Statistics and Charts

Below the controls, you see reports on your deployment of BigFix Firewall in chart and text format.



General Statistics

Total number of computers with BigFix Firewall **4**

Total number of blocks in All direction(s), occurring Today and triggered by policy All Policies **23,530**

Average number of blocks in All direction(s), occurring Today and triggered by policy All Policies **5,882.50**

Computers that blocked application Any Application from Sending/Receiving traffic more than 10 times, occurring Today and triggered by policy All Policies 1

Computers that blocked All traffic on port * more than 10 times, occurring Today and triggered by policy All Policies 4

Computers that blocked All traffic to/from ip address * more than 10 times, occurring Today and triggered by policy All Policies 4

Computers that blocked All traffic using protocol Any Protocol more than 10 times, occurring Today and triggered by policy All Policies 4

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.
- **Deployed Firewall Policies**: A pie chart showing on how many machines each policy is deployed.
- **Currently Active Policies**: A pie chart showing which policies are currently active.
- **General Statistics**: The statistics you can gather on your deployment include:
    - Total number of computers with BigFix Firewall
    - Total number of blocks in <All, Inbound, Outbound> direction(s), occurring <Today, Last 1 Week, Last 2 Weeks> and triggered by policy <*policy*, All Policies>
    - Average number of blocks in <All, Inbound, Outbound> direction(s), occurring <Today, Last 1 Week, Last 2 Weeks> and triggered by policy <*policy*, All Policies>
    - Computers that blocked <application, Any Application> from <Sending/Receiving, Receiving, Sending> traffic <less than, more than, exactly> <*number*> times, occurring <Today, Last 1 Week, Last 2 Weeks> and triggered by policy <*policy*, All Policies>
    - Computers that blocked <All, Inbound, Outbound> traffic on port <*number*> <less than, more than, exactly> <*number*> times, occurring <Today, Last 1 Week, Last 2 Weeks> and triggered by policy <*policy*, All Policies>
    - Computers that blocked <All, Inbound, Outbound> traffic to/from IP address <*address*> <less than, more than, exactly> <*number*> times, occurring <Today, Last 1 Week, Last 2 Weeks> and triggered by policy <*policy*, All Policies>
    - Computers that blocked <All, Inbound, Outbound> traffic to/from IP address <*address*> <less than, more than, exactly> <*number*> times, occurring <Today, Last 1 Week, Last 2 Weeks> and triggered by policy <*policy*, All Policies>

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

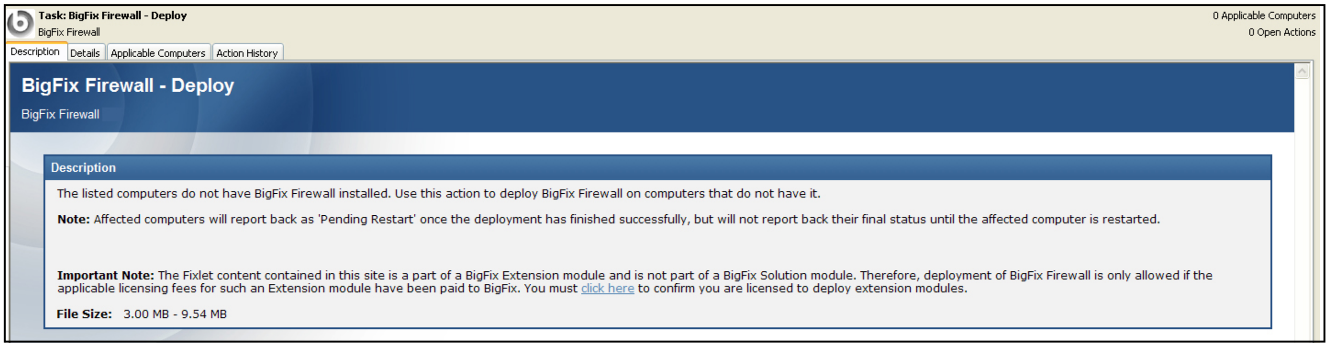
Using BigFix Firewall

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.



The listed computers do not have BigFix Firewall installed. Use this action to deploy BigFix Firewall on computers that do not have it.

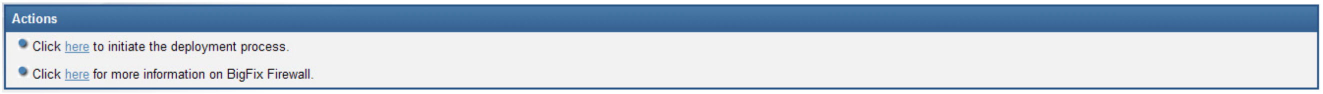
Note: Affected computers will report back as 'Pending Restart' once the deployment has finished successfully, but will not report back their final status until the affected computer is restarted.

Important Note: The Fixlet content contained in this site is a part of a BigFix Extension module and is not part of a BigFix Solution module. Therefore, deployment of BigFix Firewall is only allowed if the applicable licensing fees for such an Extension module have been paid to BigFix. You must click here to confirm you are licensed to deploy extension modules.

File Size: 3.00 MB - 9.54 MB

2. Click the **click here** link located in the **Description** section to accept the extension license.

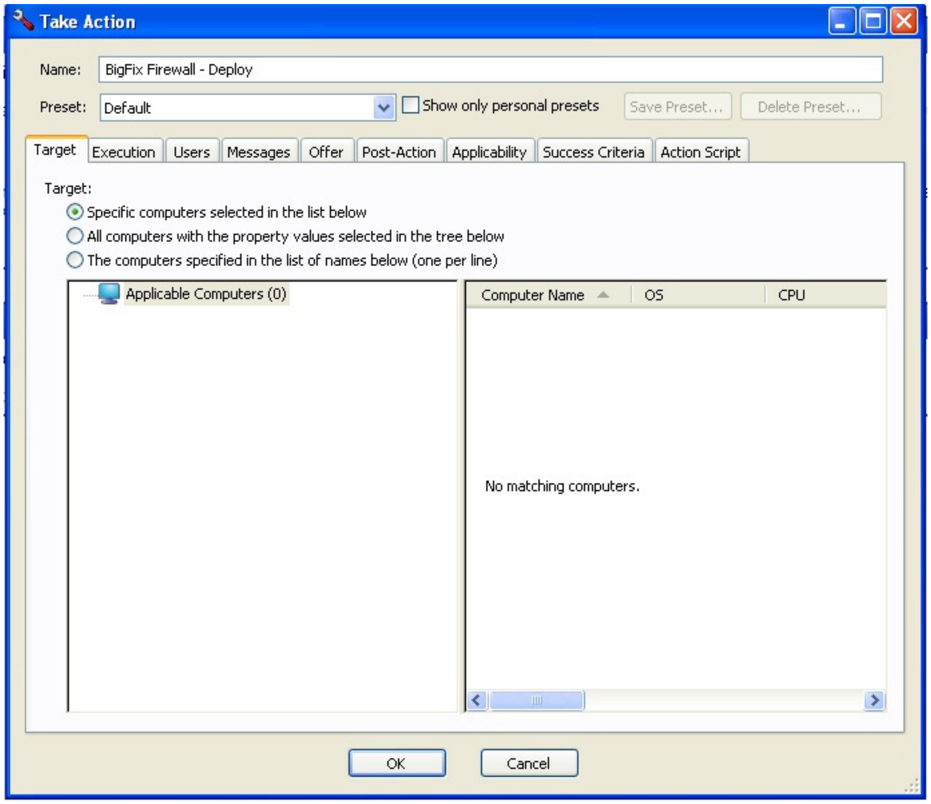
   Links will appear in the **Actions** section.



- Click here to initiate the deployment process.
- Click here for more information on BigFix Firewall.

3. Click the appropriate **here** link located in the **Actions** section.

   The **Take Action** dialog box opens.



Name: BigFix Firewall - Deploy

Preset: Default

☐ Show only personal presets

Target:

● Specific computers selected in the list below

○ All computers with the property values selected in the tree below

○ The computers specified in the list of names below (one per line)

Applicable Computers (0)

No matching computers.

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

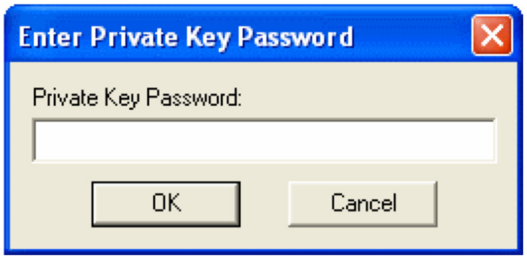
   a. Select the computer(s) to which you would like to deploy BigFix Firewall.

   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, in which you can 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.

USING 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

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.

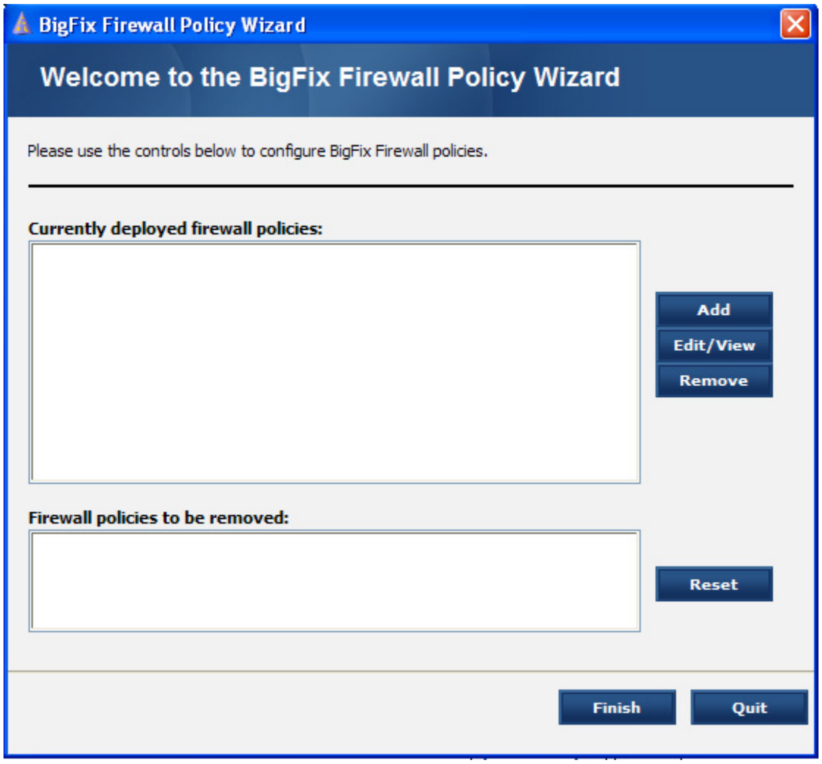
Configuring Firewall Policies

Use the BigFix Firewall Policy Wizard to create firewall policies, and then apply these policies using the generated task.

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.



BigFix Firewall Policy Wizard

Welcome to the BigFix Firewall Policy Wizard

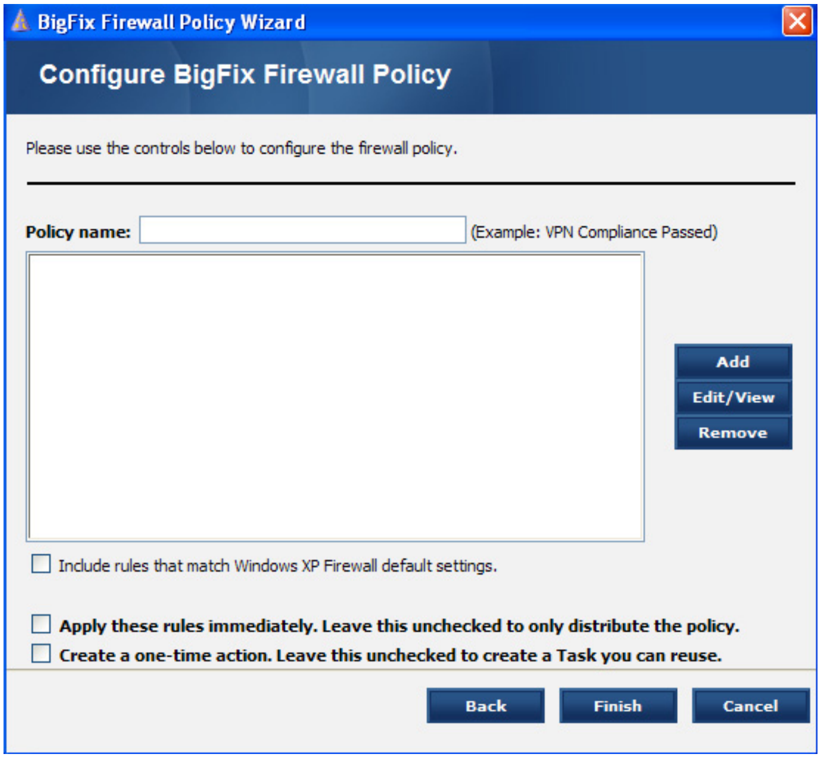
Please use the controls below to configure BigFix Firewall policies.

Currently deployed firewall policies:

Firewall policies to be removed:

2. To add a new policy, click the **Add** button.

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



Configure BigFix Firewall Policy

Please use the controls below to configure the firewall policy.

Policy name: (Example: VPN Compliance Passed)

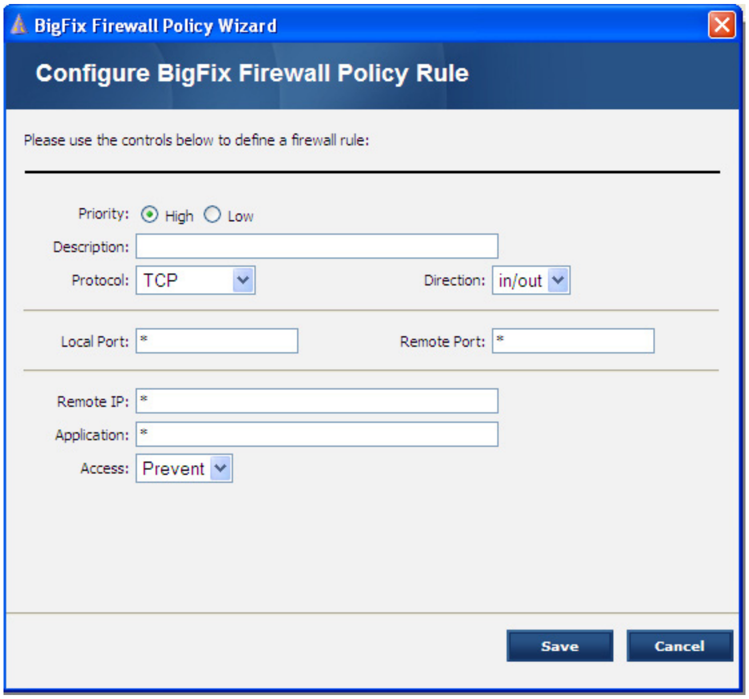
□ Include rules that match Windows XP Firewall default settings.

□ **Apply these rules immediately. Leave this unchecked to only distribute the policy.**

□ **Create a one-time action. Leave this unchecked to create a Task you can reuse.**

3. Name your policy, and then click the **Add** button to create a Firewall rule.

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



Configure BigFix Firewall Policy Rule

Please use the controls below to define a firewall rule:

Priority: ● High ○ Low

Description:

Protocol: TCP Direction: in/out

Local Port: * Remote Port: *

Remote IP: *

Application: *

Access: Prevent

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

   a. Choose the **Priority** for your rule.

   b. Enter a **Description** for your rule.

c. Choose the **Protocol** for which it applies: TCP, UDP, or Both.

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 this rule **Allows** or **Prevents** traffic matching the criteria specified in steps c-e.

g. Click **Save**.

Add additional rules by repeating Steps 3 and 4.

5. Choose whether you want to:

a. Include rules that match Windows XP Firewall default settings.

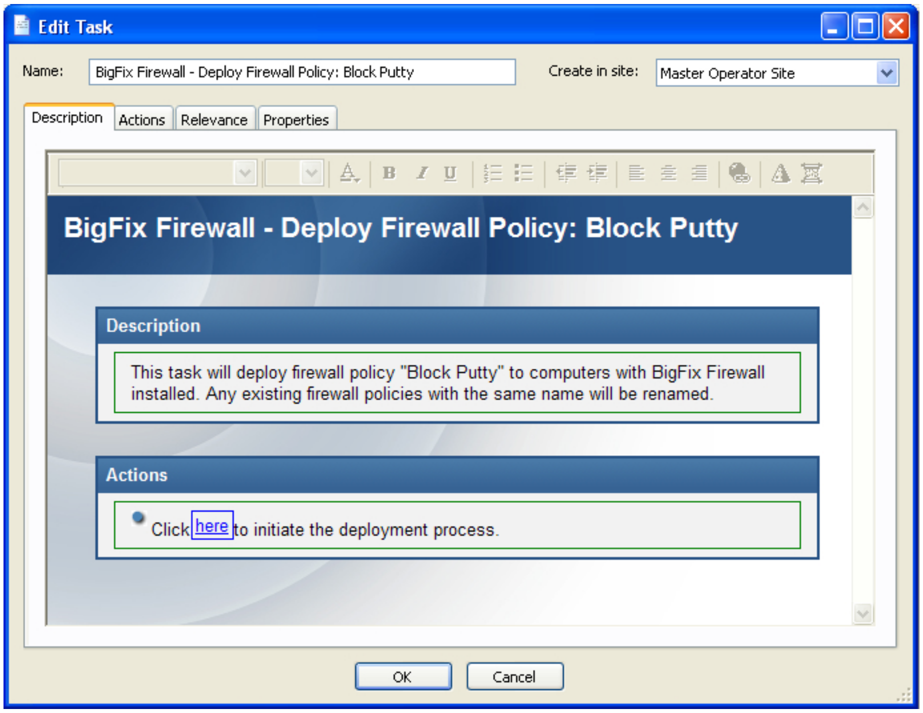
b. Apply these rules immediately. Leave this unchecked to only distribute the policy.

c. Create a one-time action. Leave this unchecked to create a Task you can reuse.

Tip: If you intended to load your policy statically, check the box in step 5b. If you intend to load your policy dynamically, based on client compliance, leave the box in step 5b unchecked.

6. Click **Finish**.

An **Edit Task** window opens.



Edit Task

Name: BigFix Firewall - Deploy Firewall Policy: Block Putty

Create in site: Master Operator Site

BigFix Firewall - Deploy Firewall Policy: Block Putty

Description

This task will deploy firewall policy "Block Putty" to computers with BigFix Firewall installed. Any existing firewall policies with the same name will be renamed.

Actions

Click here to initiate the deployment process.

7. Click **OK**, and then enter your **Private Key Password**.

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 meet your company's security policies, e.g. patches and virus definitions are up-to-date, and a different firewall policy for machines that fail your compliance check.

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 polices 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 a single Boolean value, 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.
- **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 to do not a long time to evaluate.
- Put checks you expect to fail most frequently first.
- If possible, avoid Client Context checks.

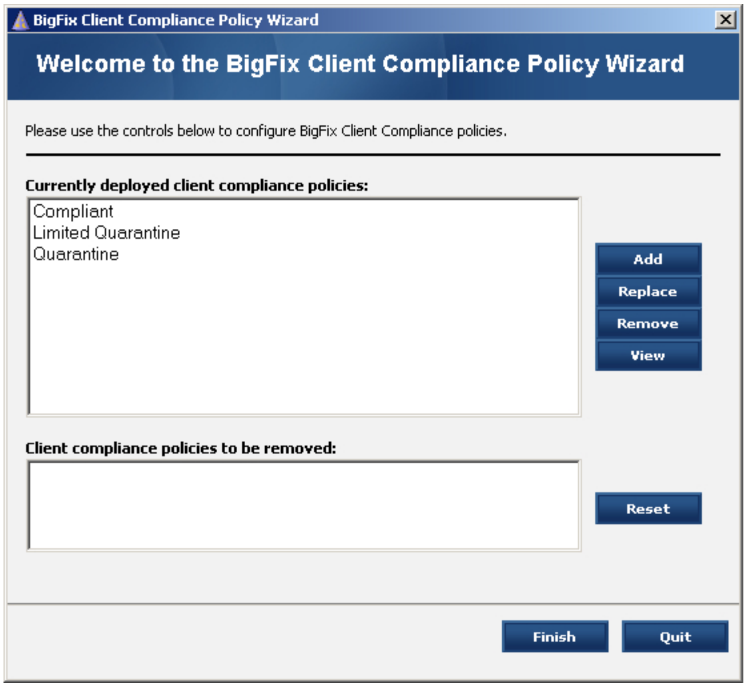
The following is a sample compliance document containing all four types of compliance checks:

```
<?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>
```

To configure a Client Compliance Policy:

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

   The **Client Compliance Policy Wizard** opens.



BigFix Client Compliance Policy Wizard

Welcome to the BigFix Client Compliance Policy Wizard

Please use the controls below to configure BigFix Client Compliance policies.

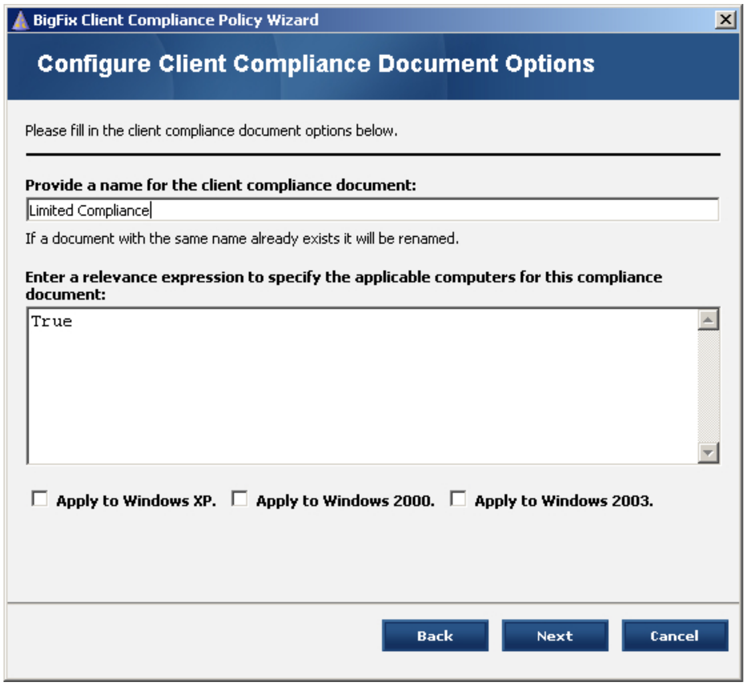
Currently deployed client compliance policies:

Compliant
Limited Quarantine
Quarantine

Client compliance policies to be removed:

2. Click the **Add** button.

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



BigFix Client Compliance Policy Wizard

Configure Client Compliance Document Options

Please fill in the client compliance document options below.

Provide a name for the client compliance document:

Limited Compliance

If a document with the same name already exists it will be renamed.

Enter a relevance expression to specify the applicable computers for this compliance document:

```
True
```

☐ Apply to Windows XP. ☐ Apply to Windows 2000. ☐ Apply to Windows 2003.

3. In this window:

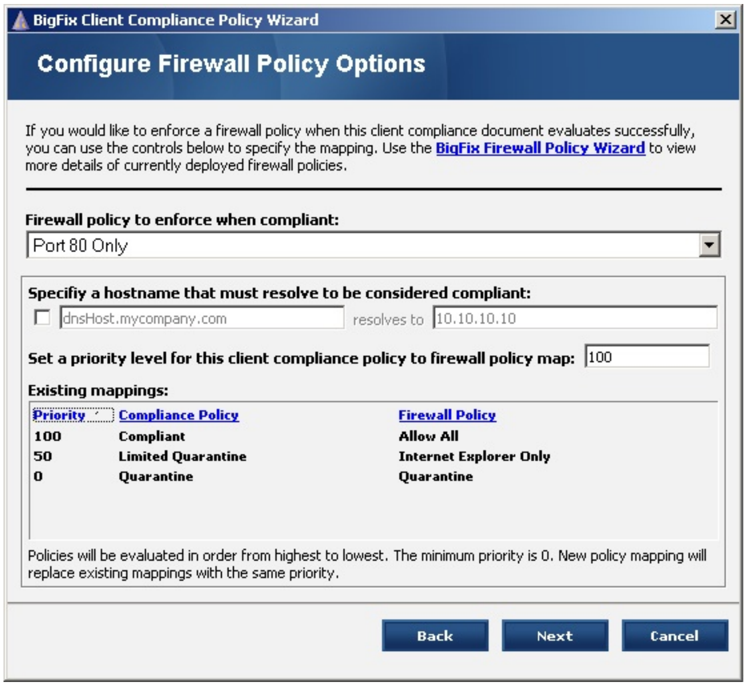
   a. Name your Client Compliance Document.

   b. Enter a relevance expression to specify the applicable computers for this document.

   c. Check the WinXP, Win2K, and/or Win2003 button if appropriate. The default is to apply it to all three operating systems.

d. Click **Next**.

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



BigFix Client Compliance Policy Wizard

Configure Firewall Policy Options

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.

Firewall policy to enforce when compliant:

Port 80 Only

Specifiy a hostname that must resolve to be considered compliant:

□ dnsHost.mycompany.com resolves to 10.10.10.10

Set a priority level for this client compliance policy to firewall policy map: 100

Existing mappings:

Priority	Compliance Policy	Firewall Policy
100	Compliant	Allow All
50	Limited Quarantine	Internet Explorer Only
0	Quarantine	Quarantine

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.

4. In this window:

   a. Choose which Firewall policy to enforce when compliant.

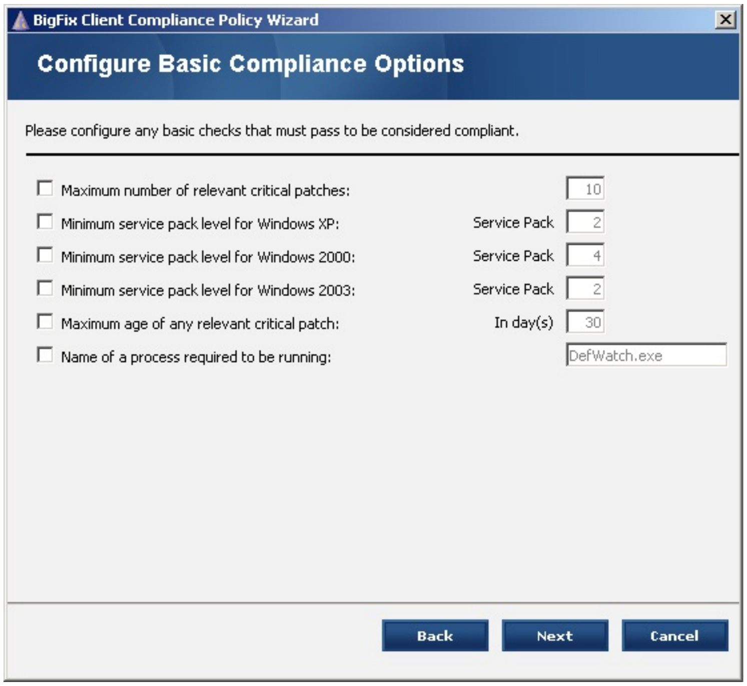
   b. If you want, specify a hostname that must resolve to be compliant.

   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.

Note: Firewall policies will not appear in the drop-down list until the policy has been deployed to at least one client.



BigFix Client Compliance Policy Wizard

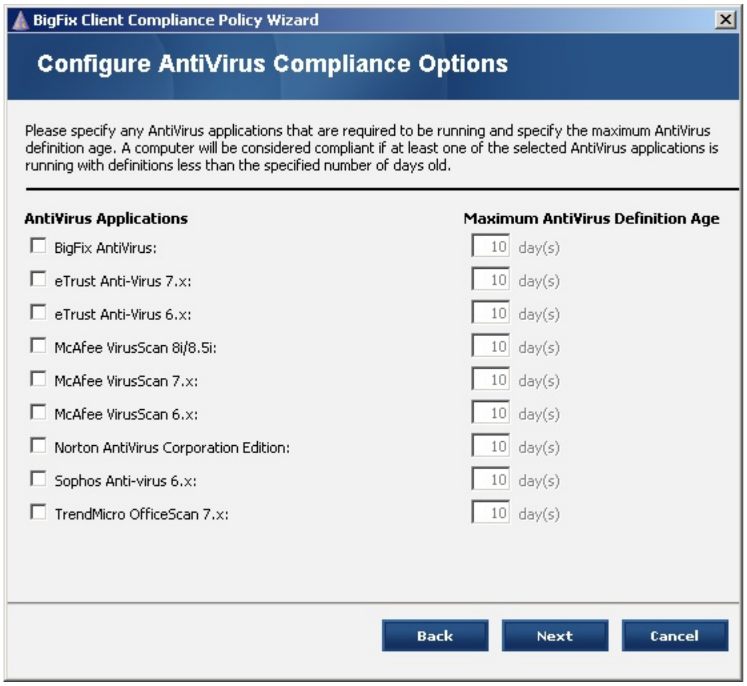
Configure Basic Compliance Options

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 XP:	Service Pack	2
□ Minimum service pack level for Windows 2000:	Service Pack	4
□ Minimum service pack level for Windows 2003:	Service Pack	2
□ Maximum age of any relevant critical patch:	In day(s)	30
□ Name of a process required to be running:		DefWatch.exe

5. 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

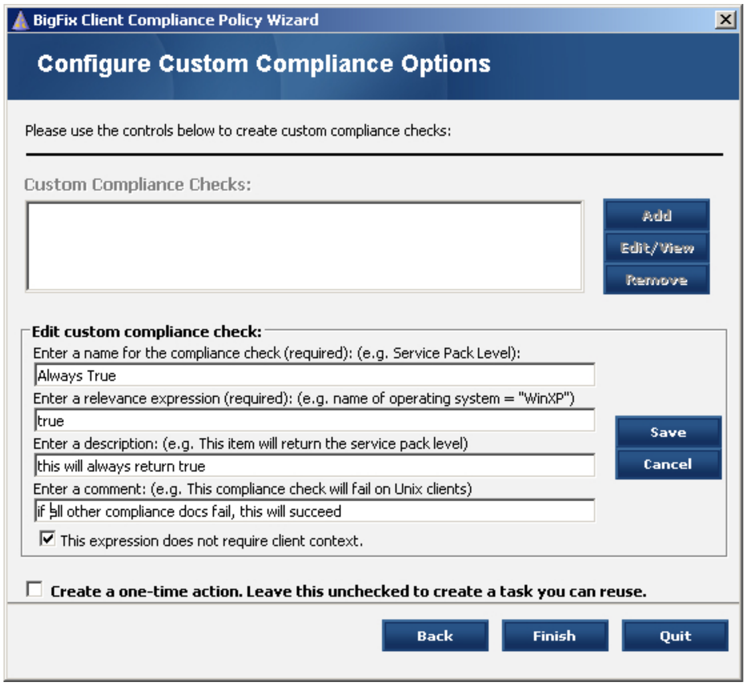
Configure AntiVirus Compliance Options

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	Maximum AntiVirus Definition Age
□ BigFix AntiVirus:	10 day(s)
□ eTrust Anti-Virus 7.x:	10 day(s)
□ eTrust Anti-Virus 6.x:	10 day(s)
□ McAfee VirusScan 8i/8.5i:	10 day(s)
□ McAfee VirusScan 7.x:	10 day(s)
□ McAfee VirusScan 6.x:	10 day(s)
□ Norton AntiVirus Corporation Edition:	10 day(s)
□ Sophos Anti-virus 6.x:	10 day(s)
□ TrendMicro OfficeScan 7.x:	10 day(s)

6. 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.



Configure Custom Compliance Options

Please use the controls below to create custom compliance checks:

Custom Compliance Checks:

Edit custom compliance check:

Enter a name for the compliance check (required): (e.g. Service Pack Level): Always True

Enter a relevance expression (required): (e.g. name of operating system = "WinXP"): true

Enter a description: (e.g. This item will return the service pack level): this will always return true

Enter a comment: (e.g. This compliance check will fail on Unix clients): if all other compliance docs fail, this will succeed

☑ This expression does not require client context.

☐ **Create a one-time action. Leave this unchecked to create a task you can reuse.**

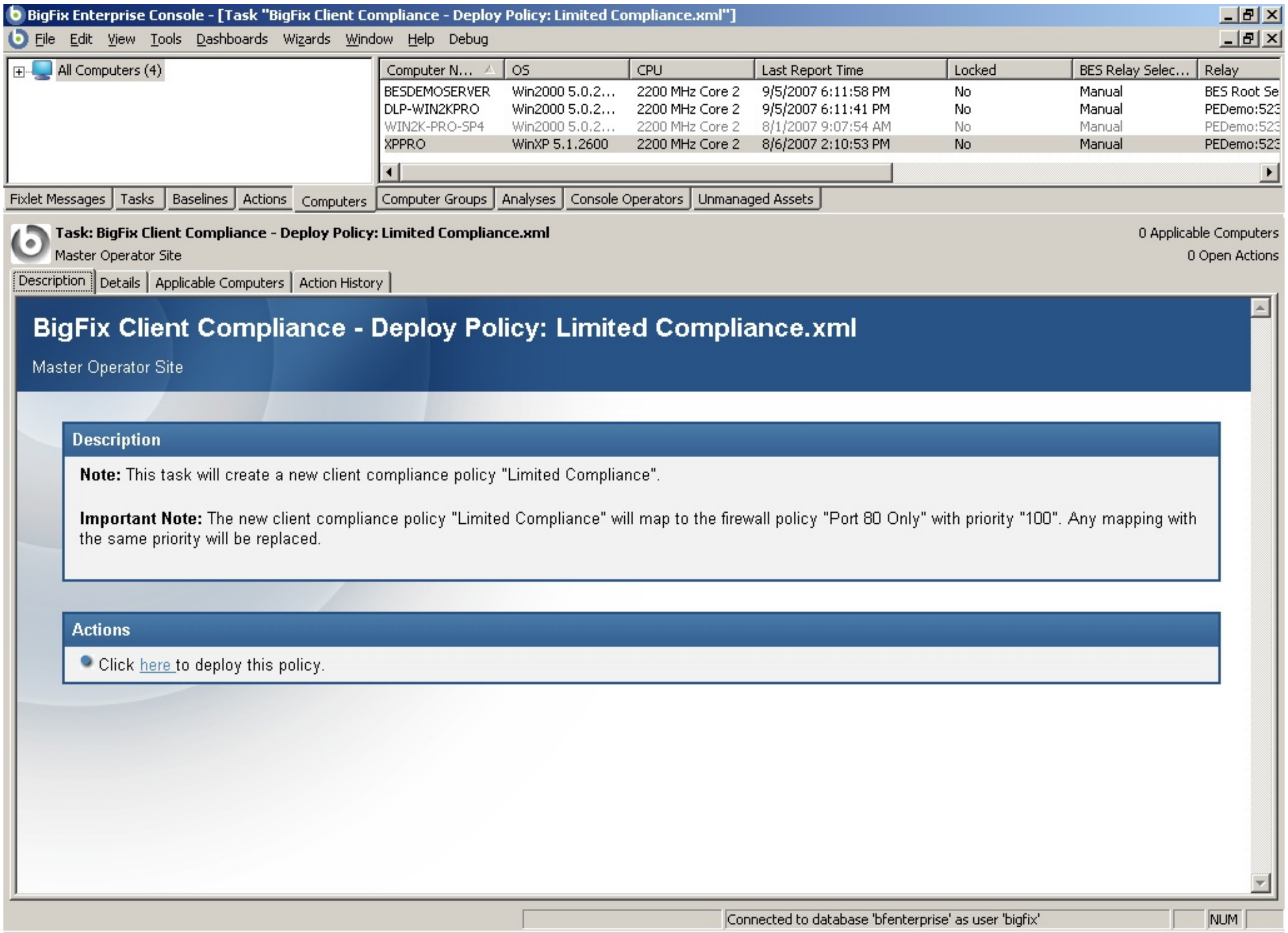
7. In this window:
   a. Add, edit, or remove any custom compliance checks you want.
   b. Leave the last check box unchecked to create a reusable Task, or check the box to create a one-time Action.
   c. Click **Finish**.

   If you selected a one-time action in step 7b, you will be taken to a **Take Action** dialog box, in which you can target any machines to which to apply your policy and choose other deployment options.

   If you did not select a one-time action in step 7b, you will be taken to an **Edit Task** dialog box, in which you can edit descriptions and other parameters of the task.

8. Click **OK**, and then enter your **Private Key Password**.

   If you did not select a one-time action, the **Deploy Policy Task** opens.


BigFix Enterprise Console - [Task "BigFix Client Compliance - Deploy Policy: Limited Compliance.xml"]
File Edit View Tools Dashboards Wizards Window Help Debug
All Computers (4)
Fixlet Messages Tasks Baselines Actions Computers Computer Groups Analyses Console Operators Unmanaged Assets
Description Details Applicable Computers Action History
NUM

Computer N...	OS	CPU	Last Report Time	Locked	BES Relay Selec...	Relay
BESDEMOSERVER	Win2000 5.0.2...	2200 MHz Core 2	9/5/2007 6:11:58 PM	No	Manual	BES Root Se
DLP-WIN2KPRO	Win2000 5.0.2...	2200 MHz Core 2	9/5/2007 6:11:41 PM	No	Manual	PEDemo:523
WIN2K-PRO-SP4	Win2000 5.0.2...	2200 MHz Core 2	8/1/2007 9:07:54 AM	No	Manual	PEDemo:523
XPPRO	WinXP 5.1.2600	2200 MHz Core 2	8/6/2007 2:10:53 PM	No	Manual	PEDemo:523

Task: BigFix Client Compliance - Deploy Policy: Limited Compliance.xml
Master Operator Site

0 Applicable Computers
0 Open Actions

BigFix Client Compliance - Deploy Policy: Limited Compliance.xml

Master Operator Site

Description

Note: This task will create a new client compliance policy "Limited Compliance".

Important Note: The new client compliance policy "Limited Compliance" will map to the firewall policy "Port 80 Only" with priority "100". Any mapping with the same priority will be replaced.

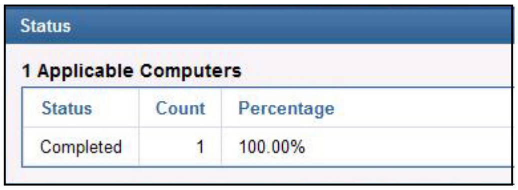
Actions

- Click here to deploy this policy.

Connected to database 'bfenterprise' as user 'bigfix'

9. Click the **here** link to deploy the policy.

   After the policy has deployed, the status will show 100% complete.



Status

1 Applicable Computers

Status	Count	Percentage
Completed	1	100.00%

Enabling Client Compliance

Once you have created your Firewall and Client Compliance policies, you are ready to turn on client compliance evaluation.

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'd 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.
9. 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.

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

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 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, 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.

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 200,000 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 Microsoft Windows 2000, Server 2003, and XP.

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 won’t 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 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 crafting custom XML firewall policies. BigFix professional services are available to assist in crafting these policies. Specific support using the Firewall Policy Wizard is planned for a forthcoming release.

Reporting

Can I export report data?

Yes.

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

Yes.

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/.

ACKNOWLEDGEMENTS AND NOTICES

documentation, or modified versions thereof. Contact sitemgr@sgi.com for information on licensing this software for commercial use. Contact 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; email: 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

This software is copyrighted as noted above. It is free software and may be obtained via anonymous ftp from 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.

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.

BigFix, Inc.
1480 64th Street Suite 200
Emeryville, California 94608
[t] 510 652-6700
[f] 510 652-6742
[e] info@bigfix.com
[e] sales@bigfix.com