BigFix® AntiPest Deployment Guide

BigFix, Inc.
Emeryville, CA

Last Modified: 8/9/07

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 AntiPest. 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 AntiPest.
- **Quick Start**: This section provides brief instructions for deploying and using BigFix AntiPest.
- **Using BigFix AntiPest**: This section provides instructions for performing the most common tasks with BigFix AntiPest.
- **Troubleshooting**: This section provides troubleshooting tips.
- **Frequently Asked Questions**: This section provides answers for frequently asked questions about BigFix AntiPest.

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 AntiPest, Version 2.0 and later.

Introduction

BigFix AntiPest helps to reduce IT break-fix costs and to protect computers and their sensitive information from spyware and other software pests. BigFix AntiPest utilizes the scalability, real-time speed, and control provided by the BigFix platform.

Increasingly often, distributed and porous enterprise networks make it difficult for IT managers to ensure the health and security of their organizations' desktop, laptop and server computers. The growing number of remote and mobile computers connecting in from public or foreign networks increases the likelihood that enterprise computers will be compromised by malicious software. Employees, contractors, suppliers and partners routinely access corporate data via remote networks, VPNs, or wireless connections, often unwittingly providing entry points for security threats to enterprise resources.

Spyware and other software pests can threaten business continuity; require time-consuming remediation, lower employee productivity, and compromise sensitive corporate and customer data. There are already tens of thousands of programs available and circulating on the internet that can steal data and give attackers access to computers. Microsoft estimates that unwanted, malicious programs are responsible for 50 percent of all PC crashes.

By using BigFix AntiPest to address the challenges posed by spyware and other pests, IT organizations benefit by:

- **Gaining enterprise-class, anti-spyware management—**Gain control, scheduling, and reporting for pest detection and remediation.
- **Gaining rapid roll out capabilities—**Achieve rapid deployment and simplified ongoing administrative maintenance.
- **Leveraging existing agent and infrastructure—**Avoid or eliminate redundant software pest detection and removal management infrastructure.
- **Getting a lower total cost of ownership—**Reduce training overhead and achieve lower total cost of ownership.

BigFix advantages include:

- Real-time visibility and control:
  - Centralized visibility and reporting at up to very large scale with minimal network and client impact
  - New malware infections and removals reported immediately to central server to allow for reporting and notifications in real-time
  - Detection and remediation is independent of network connectivity
  - 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 AntiPest.

Beginning Setup

This procedure assumes that you already have installed BigFix.

1. Obtain a masthead for the BigFix AntiPest site.

   Email licensing@bigfix.com to request the masthead.

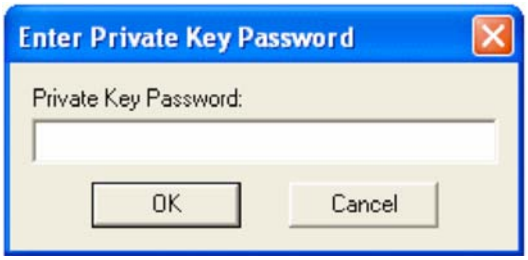
2. Add the BigFix AntiPest site:

   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**.

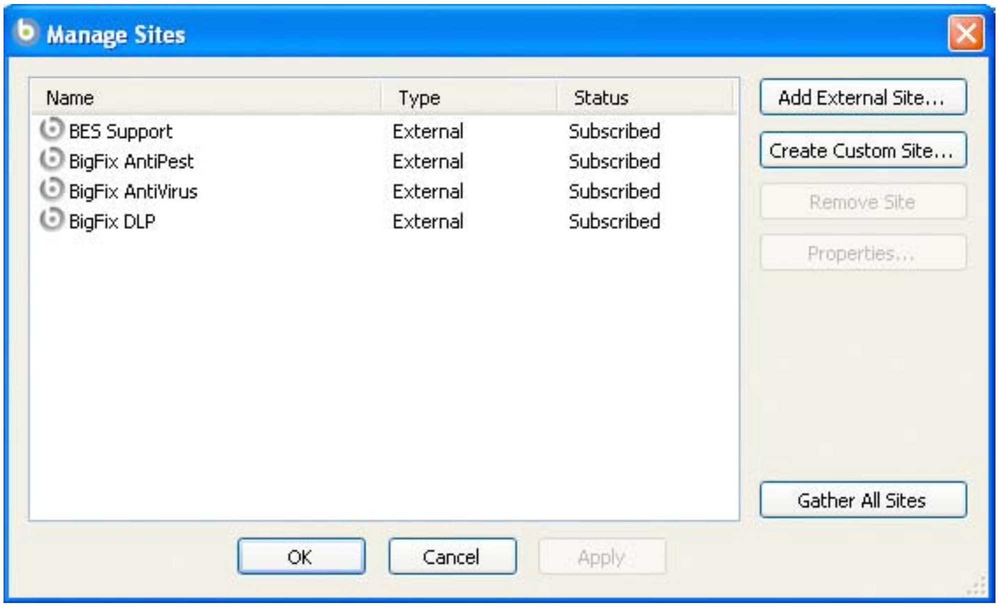


At this point, the BigFix AntiPest site will begin the gathering process, in which Fixlets, Tasks, Analyses, etc. are gathered from the central BigFix server.

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 AntiPest entry in the **Dashboards** menu and your Navigation Bar. The site will show as **Subscribed** in the **Manage Sites** dialog.

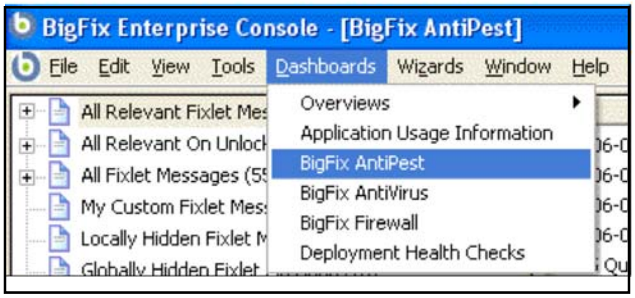


Name	Type	Status
BES Support	External	Subscribed
BigFix AntiPest	External	Subscribed
BigFix AntiVirus	External	Subscribed
BigFix DLP	External	Subscribed

Accessing the BigFix AntiPest Dashboard

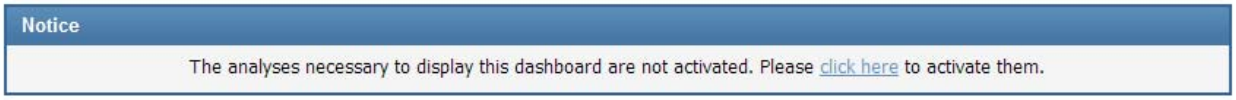
BigFix AntiPest provides a dashboard view with overview statistics and charts that enable you to gauge the current health of your system and to track progress as BigFix AntiPest enforces anti-pest compliance and pushes updates throughout the network. In addition, you can use the Dashboard as a central point to manage important tasks such as deployment, updates, and scanning.

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



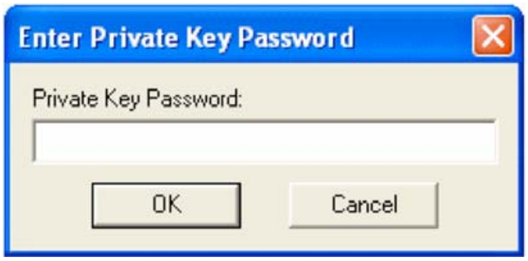
Launching the Dashboard

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.

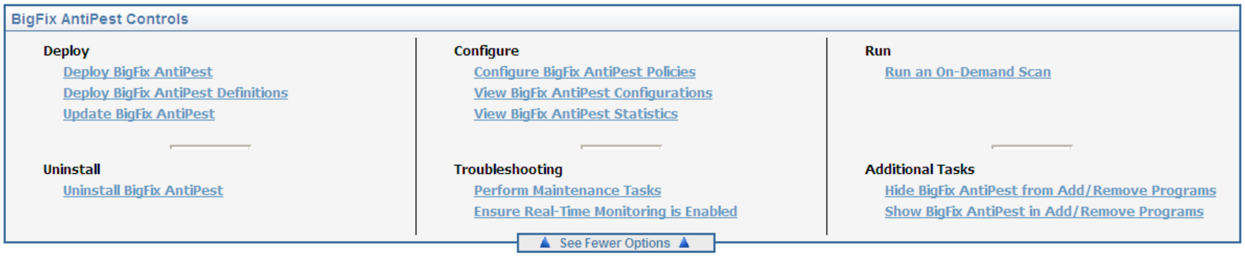


After activation, you might also see a notice to install Office Web Components. If necessary, install Office Web Components following the instructions in the linked Knowledge Base Article.

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

Understanding the BigFix AntiPest Dashboard Controls

At the top of the Dashboard, you see the **BigFix AntiPest Controls**:


BigFix AntiPest Controls
Deploy
Deploy BigFix AntiPest
Deploy BigFix AntiPest Definitions
Update BigFix AntiPest
Uninstall
Uninstall BigFix AntiPest
Configure
Configure BigFix AntiPest Policies
View BigFix AntiPest Configurations
View BigFix AntiPest Statistics
Troubleshooting
Perform Maintenance Tasks
Ensure Real-Time Monitoring is Enabled
Run
Run an On-Demand Scan
Additional Tasks
Hide BigFix AntiPest from Add/Remove Programs
Show BigFix AntiPest in Add/Remove Programs
See Fewer Options

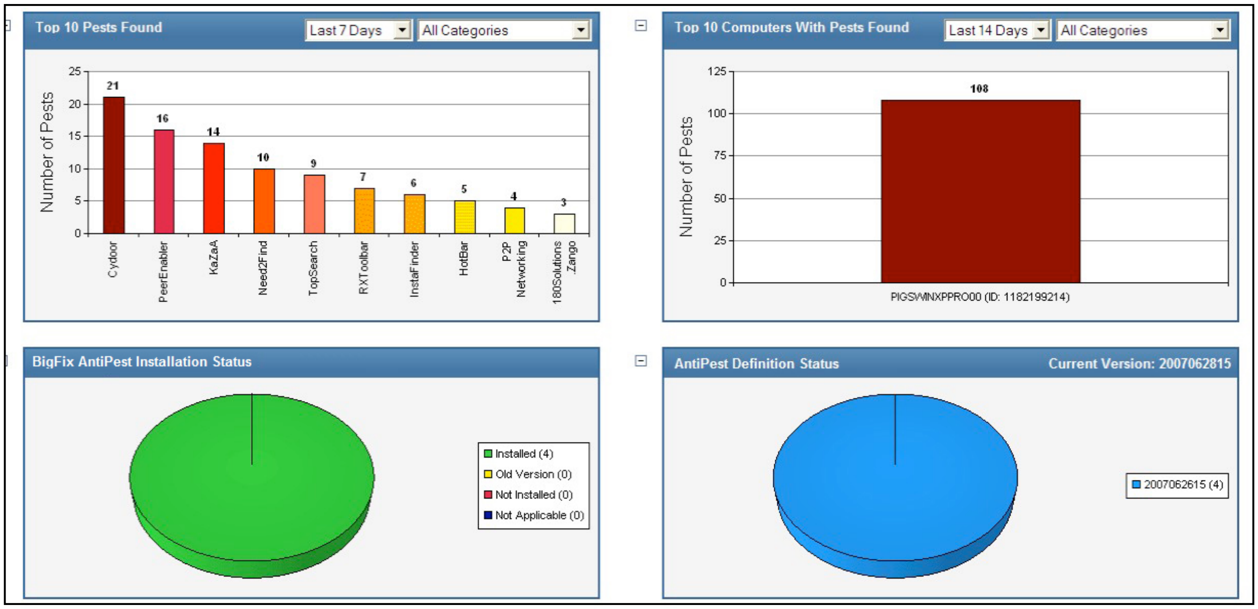
The controls that BigFix AntiPest provides are:

- **Deploy**: Use the controls in this section to deploy BigFix AntiPest, update BigFix AntiPest, or update BigFix AntiPest definitions.
  - Deploy BigFix AntiPest
  - Update BigFix AntiPest Definitions
  - Update BigFix AntiPest
- **Uninstall**: Use the control in this section to uninstall BigFix AntiPest.
  - Uninstall BigFix AntiPest
- **Configure**: Use the controls in this section to configure AntiPest, or to view your existing configurations or statistics.
  - Configure BigFix AntiPest Policies
  - View BigFix AntiPest Configurations
  - View BigFix AntiPest Statistics
- **Troubleshooting**: Use the controls in this section if you have problems with your deployment of BigFix AntiPest.
  - Perform Maintenance Tasks
    - Unquarantine the pests quarantined by the most recent scan
    - Unquarantine all quarantined pests
    - Remove quarantined pests
    - Reset statistics information
  - Ensure Real-Time Monitoring is Enabled

- **Run**: Use this control to run an on-demand scan.
  - Run an On-Demand Scan
- **Additional Tasks**: Use these controls to show or hide BigFix AntiPest in Add/Remove Programs.
  - Hide BigFix AntiPest from Add/Remove Programs
  - Show BigFix AntiPest in Add/Remove Programs

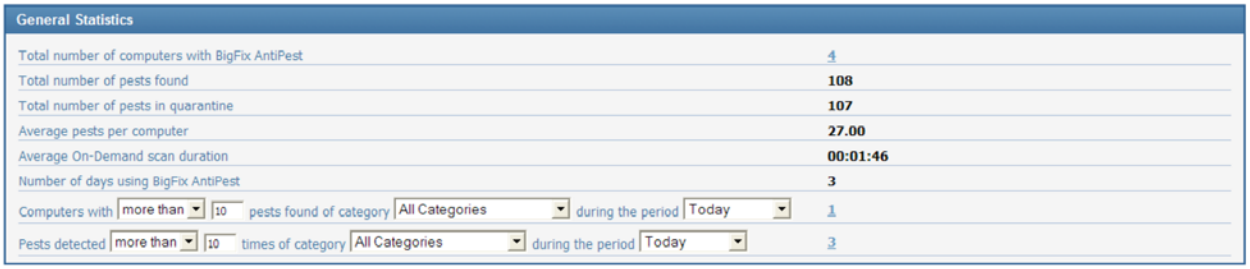
Reading the Dashboard's Overview Statistics and Charts

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



BigFix AntiPest provides charts illustrating:

- **Top 10 Pests Found**: This is a bar chart displaying the top 10 pests in your deployment, and on how many computers each is found.
- **Top 10 Computers with Pests Found**: This is a bar chart displaying how many pests are found on the top 10 computers with pests.
- **AntiPest Installation Status**: This is a pie chart displaying which computers have the current version of BigFix AntiPest installed, not installed, or have an old version installed.
- **AntiPest Definition Status**: This is a pie chart displaying which computers have which version of AntiPest definitions installed.



General Statistics

Total number of computers with BigFix AntiPest	4
Total number of pests found	108
Total number of pests in quarantine	107
Average pests per computer	27.00
Average On-Demand scan duration	00:01:46
Number of days using BigFix AntiPest	3
Computers with [more than] [10] pests found of category [All Categories] during the period [Today]	1
Pests detected [more than] [10] times of category [All Categories] during the period [Today]	3

The statistics you can gather on your deployment include:

- Total number of computers with BigFix AntiPest

- Total number of pests found
- Total number of pests in quarantine
- Average number of pests per computer
- Average On-Demand scan duration
- Number of days using BigFix AntiPest
- Computers with <less than, more than, exactly> <number> pests found of category <categories> during the period <Today, Last 7 Days, Last 14 Days, Last 30 Days, Last 60 Days, All>
- Pests detected <less than, more than, exactly> <number> times of category <categories> during the period <Today, Last 7 Days, Last 14 Days, Last 30 Days, Last 60 Days, All>

Tip: You can use the **Maintenance Tasks** Task to reset statistics.

Tip: You can use the drop-down menus in the title bars to filter graphs by pest category or by detection time.

Using BigFix AntiPest

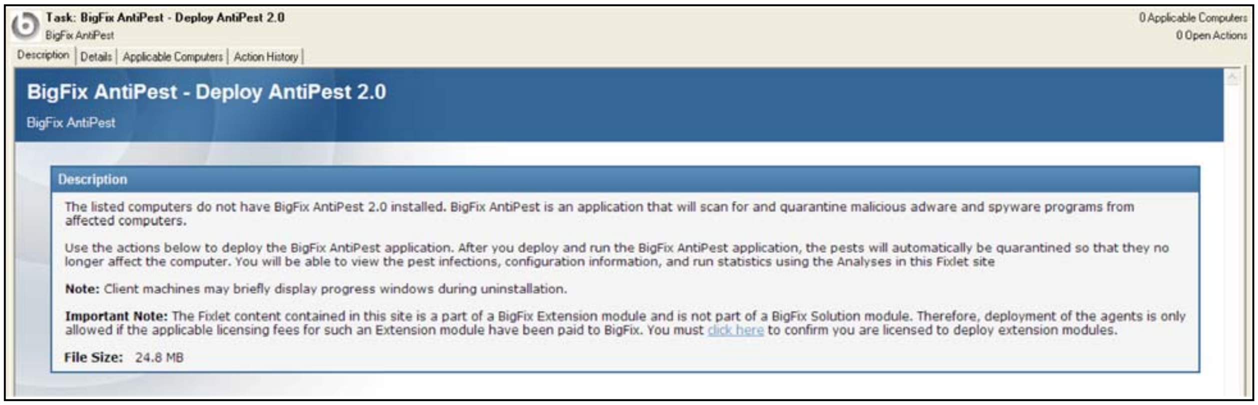
This section provides instructions for performing the most common tasks with BigFix AntiPest.

Deploying BigFix AntiPest

To deploy BigFix AntiPest:

1. From the Dashboard, click the **Deploy BigFix AntiPest** link in the Dashboard controls.

   The **Deploy BigFix AntiPest** Task will open.



BigFix AntiPest - Deploy AntiPest 2.0

BigFix AntiPest

Description

The listed computers do not have BigFix AntiPest 2.0 installed. BigFix AntiPest is an application that will scan for and quarantine malicious adware and spyware programs from affected computers.

Use the actions below to deploy the BigFix AntiPest application. After you deploy and run the BigFix AntiPest application, the pests will automatically be quarantined so that they no longer affect the computer. You will be able to view the pest infections, configuration information, and run statistics using the Analyses in this Fixlet site

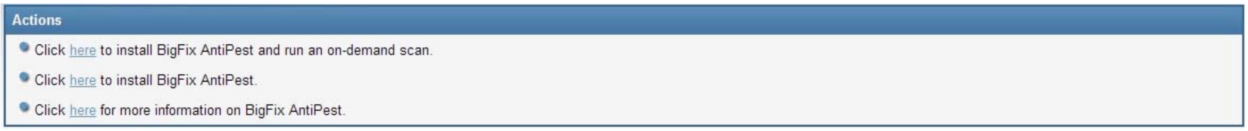
Note: Client machines may briefly display progress windows during uninstallation.

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 the agents 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: 24.8 MB

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

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

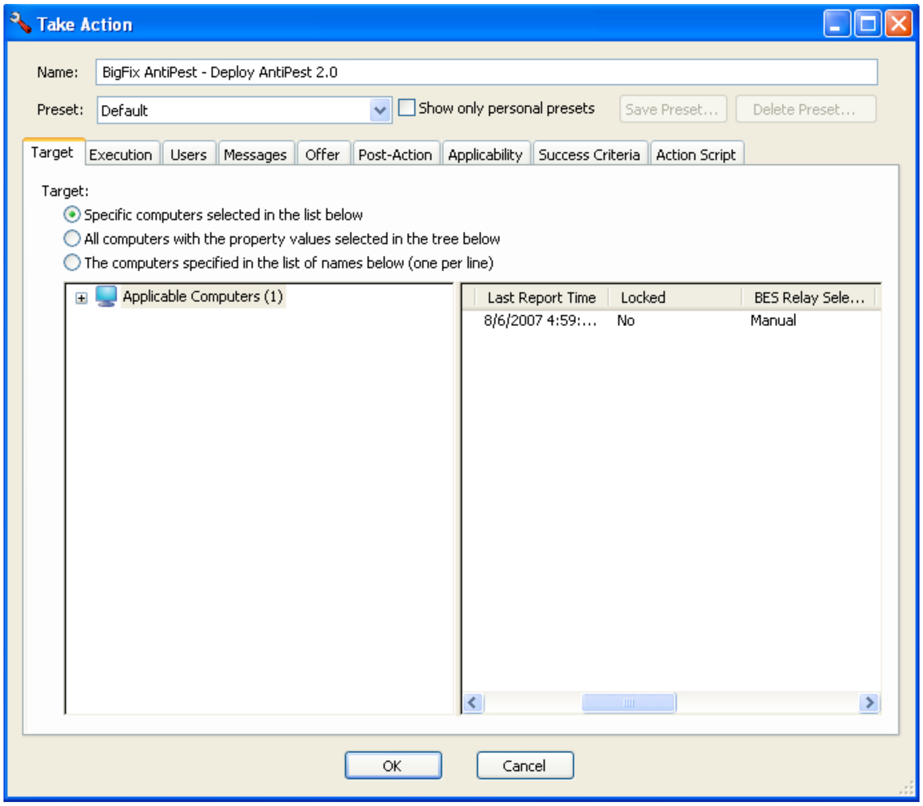


Actions

- Click here to install BigFix AntiPest and run an on-demand scan.
- Click here to install BigFix AntiPest.
- Click here for more information on BigFix AntiPest.

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

   The **Take Action** dialog box opens.


Take Action
Name: BigFix AntiPest - Deploy AntiPest 2.0
Preset: Default
□ Show only personal presets
Save Preset...
Delete Preset...
Target
Execution
Users
Messages
Offer
Post-Action
Applicability
Success Criteria
Action Script
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 (1)
OK
Cancel

Last Report Time	Locked	BES Relay Sele...
8/6/2007 4:59:...	No	Manual

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

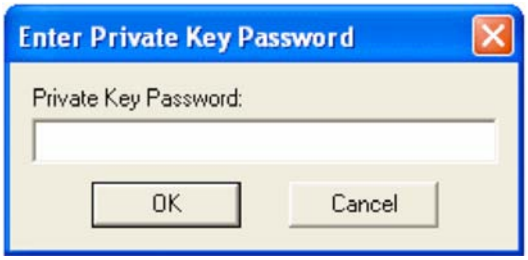
   a. Select the computer(s) to which you would like to deploy BigFix AntiPest.

   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.

Verifying Deployment

BigFix AntiPest installs by default at C:\Program Files\BigFix AntiPest:

- The DAT subfolder contains the Definitions for the Pests and the Quarantine folder contains quarantined pests.
- If BigFix AntiPest is correctly installed, you will see the BigFixAntiPest.exe (AntiPest executable) file in the "BigFix AntiPest" folder. The file properties will provide version information.

- In a default configuration, you will see BigFix AntiPest in Add or Remove Programs.

There are two other files you will normally see in the "BigFix AntiPest" folder: PestCurrent.txt and PestHistorical.txt. These files contain information about found pests.

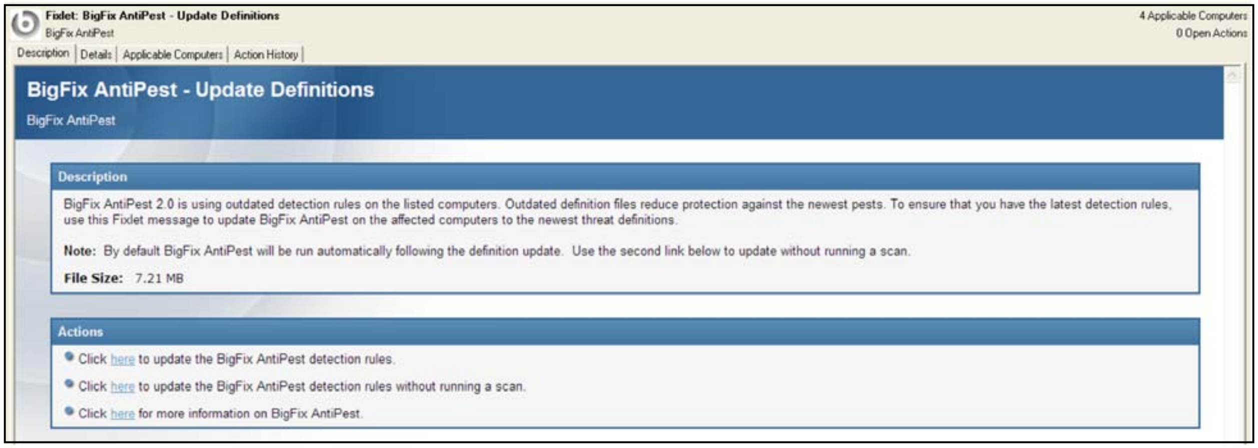
Updating Definitions

Outdated definition files reduce protection against the newest pests. To ensure you have the latest detection rules for your deployment, regularly update your AntiPest Definitions.

To update definitions:

1. Click the **Deploy AntiPest Definitions** dashboard link.

   The **BigFix AntiPest – Update Definitions** Fixlet opens.



BigFix AntiPest - Update Definitions

BigFix AntiPest

Description

BigFix AntiPest 2.0 is using outdated detection rules on the listed computers. Outdated definition files reduce protection against the newest pests. To ensure that you have the latest detection rules, use this Fixlet message to update BigFix AntiPest on the affected computers to the newest threat definitions.

Note: By default BigFix AntiPest will be run automatically following the definition update. Use the second link below to update without running a scan.

File Size: 7.21 MB

Actions

- Click here to update the BigFix AntiPest detection rules.
- Click here to update the BigFix AntiPest detection rules without running a scan.
- Click here for more information on BigFix AntiPest.

2. From this page:

   a. Choose whether you want to:

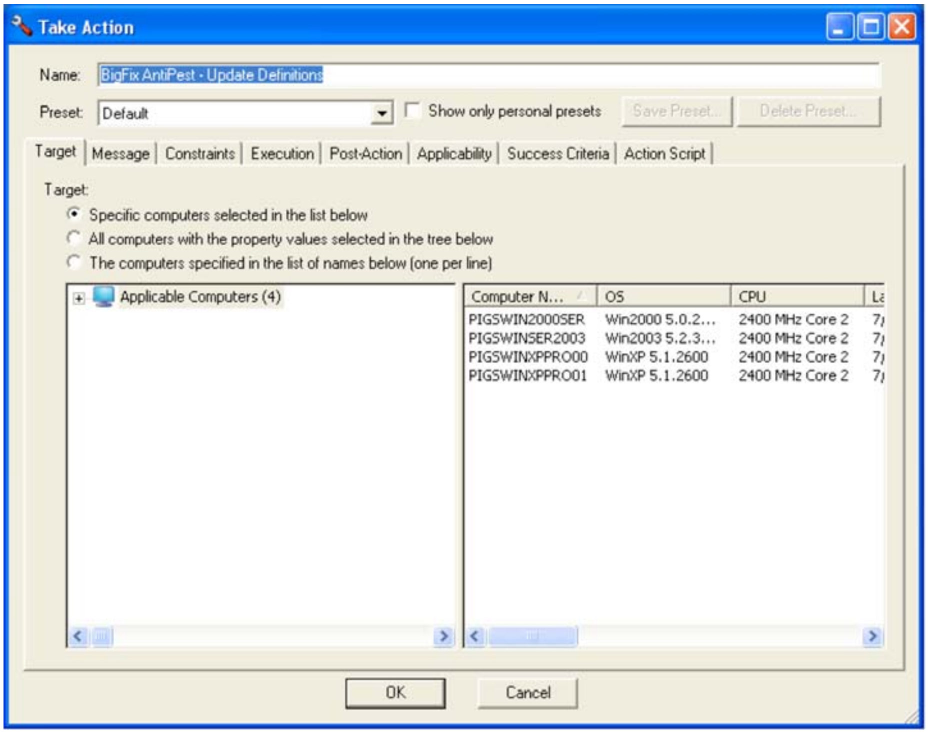
      o Update BigFix AntiPest detection rules.

      o Update BigFix AntiPest detection rules without running a scan.

   b. Click the appropriate link.

Note: You can also choose a link to obtain more information on BigFix AntiPest. This link takes you to the support page at: http://support.bigfix.com/bes/sites/antipest.html.

The **Take Action** dialog box opens.



Name: BigFix AntiPest - Update Definitions

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)

Computer N...	OS	CPU	La
PIGSWIN2000SER	Win2000 5.0.2...	2400 MHz Core 2	7/
PIGSWINSER2003	Win2003 5.2.3...	2400 MHz Core 2	7/
PIGSWINXPPRO00	WinXP 5.1.2600	2400 MHz Core 2	7/
PIGSWINXPPRO01	WinXP 5.1.2600	2400 MHz Core 2	7/

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

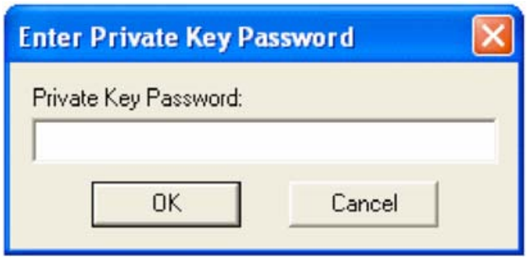
   a. Select the computer(s) to which you would like to update your definitions.

   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.

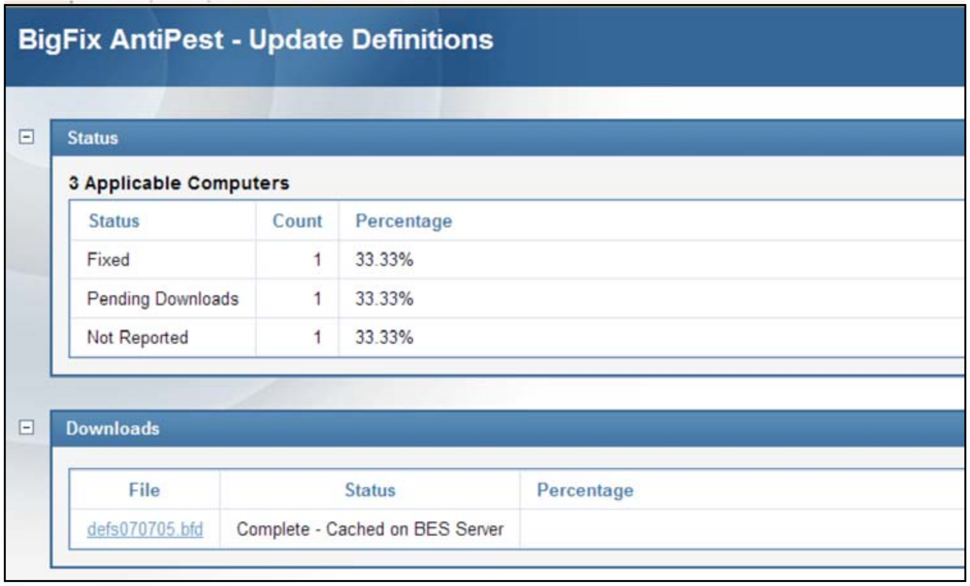
   d. You will be prompted for you private key password.



Private Key Password:

4. Enter your **Private Key Password** when prompted.

   An Action window will appear, in which you can track the progress of your deployment.



BigFix AntiPest - Update Definitions

Status

3 Applicable Computers

Status	Count	Percentage
Fixed	1	33.33%
Pending Downloads	1	33.33%
Not Reported	1	33.33%

Downloads

File	Status	Percentage
defs070705.bfd	Complete - Cached on BES Server	

When the update is complete, the Action window will show 100% complete.

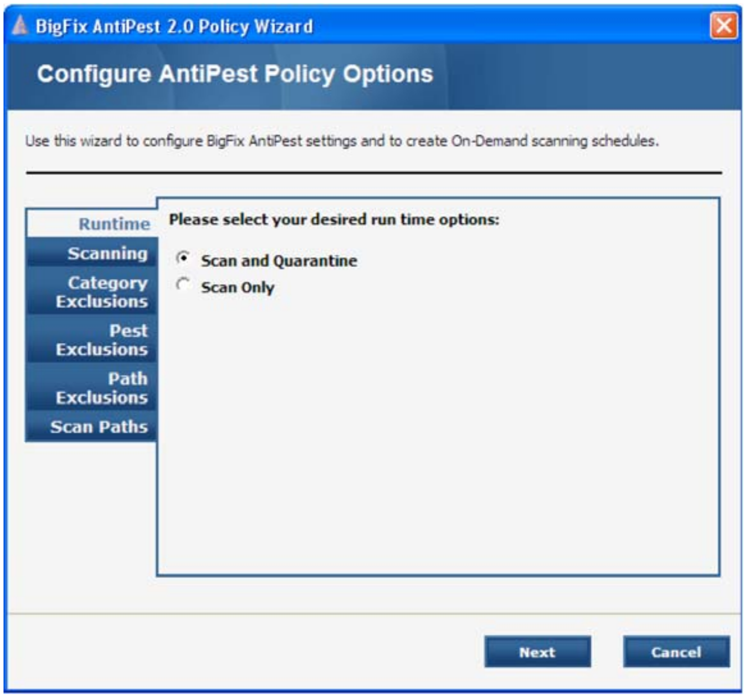
Using the BigFix AntiPest Policy Wizard

BigFix AntiPest provides a Wizard to configure settings and to create customized On-Demand scanning schedules.

To use this wizard:

1. From the Dashboard, click the **Configure BigFix AntiPest Policies** link or select **BigFix AntiPest 2.0 Policy Wizard** from the Wizards menu.

   The **BigFix AntiPest 2.0 Policy** Wizard opens on the Runtime tab.



BigFix AntiPest 2.0 Policy Wizard

Configure AntiPest Policy Options

Use this wizard to configure BigFix AntiPest settings and to create On-Demand scanning schedules.

Please select your desired run time options:

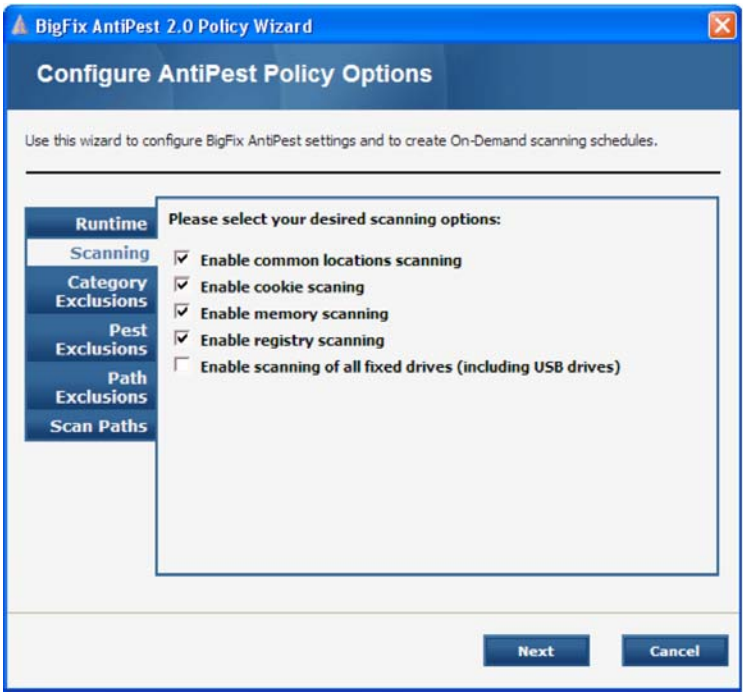
● Scan and Quarantine
○ Scan Only

2. On the first page of the wizard:

a. Select whether you want to scan and quarantine, or scan only.

b. Click the **Scanning** tab.

Tip: It is recommended that initially you configure a scan-only task. Based on the results of the scan, you should use the Wizard to configure any exclusions necessary in your environment. After you have tested your exclusions, use the Wizard to create scan and quarantine configurations that meet your requirements.



BigFix AntiPest 2.0 Policy Wizard

Configure AntiPest Policy Options

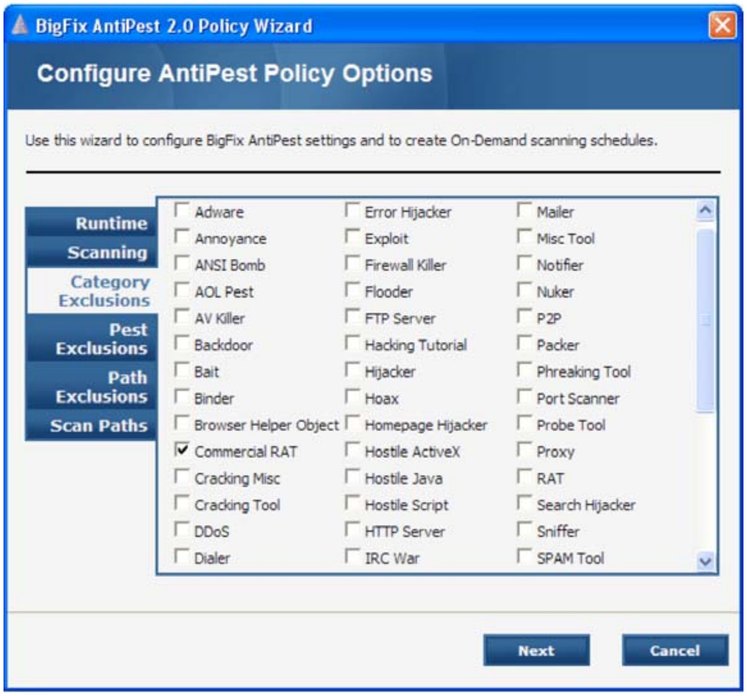
Use this wizard to configure BigFix AntiPest settings and to create On-Demand scanning schedules.

Please select your desired scanning options:

☑ Enable common locations scanning
☑ Enable cookie scaning
☑ Enable memory scanning
☑ Enable registry scanning
☐ Enable scanning of all fixed drives (including USB drives)

3. Select the scanning options that are best for your deployment. The default selects all options except for scanning of all fixed drives, including USB drives.

   Click the **Category Exclusions** tab.



BigFix AntiPest 2.0 Policy Wizard

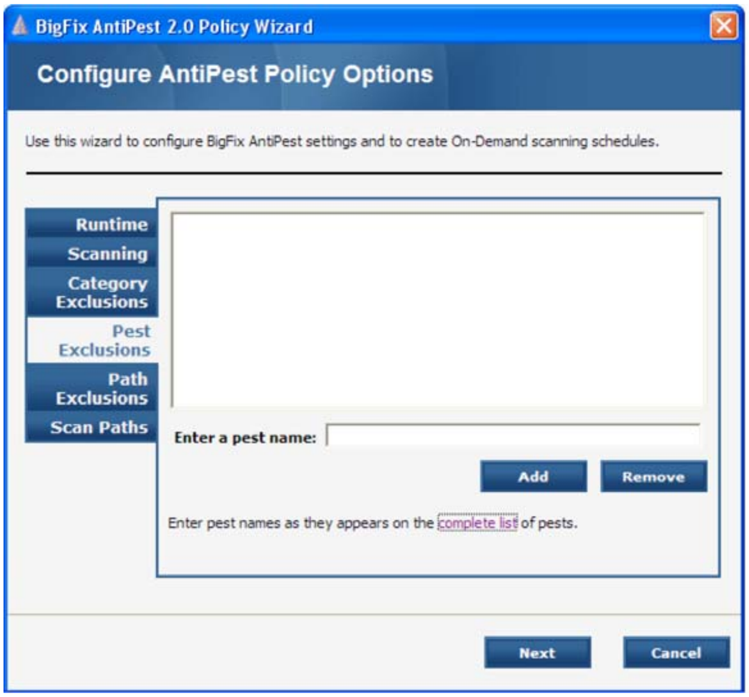
Configure AntiPest Policy Options

Use this wizard to configure BigFix AntiPest settings and to create On-Demand scanning schedules.

□ Adware
□ Annoyance
□ ANSI Bomb
□ AOL Pest
□ AV Killer
□ Backdoor
□ Bait
□ Binder
□ Browser Helper Object
☑ Commercial RAT
□ Cracking Misc
□ Cracking Tool
□ DDoS
□ Dialer
□ Error Hijacker
□ Exploit
□ Firewall Killer
□ Flooder
□ FTP Server
□ Hacking Tutorial
□ Hijacker
□ Hoax
□ Homepage Hijacker
□ Hostile ActiveX
□ Hostile Java
□ Hostile Script
□ HTTP Server
□ IRC War
□ Mailer
□ Misc Tool
□ Notifier
□ Nuker
□ P2P
□ Packer
□ Phreaking Tool
□ Port Scanner
□ Probe Tool
□ Proxy
□ RAT
□ Search Hijacker
□ Sniffer
□ SPAM Tool

4. Select any potential pest categories that you wish to exclude from scans. By default, BigFix AntiPest excludes Commercial RAT files, which include remote access products like VNC and DameWare™.

   Click the **Pest Exclusions** tab.



BigFix AntiPest 2.0 Policy Wizard

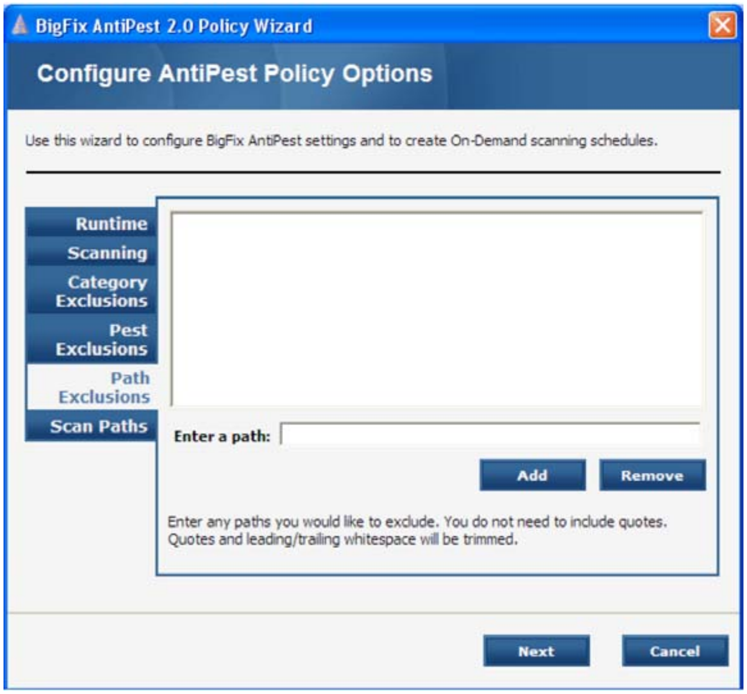
Configure AntiPest Policy Options

Use this wizard to configure BigFix AntiPest settings and to create On-Demand scanning schedules.

Enter pest names as they appears on the complete list of pests.

5. Enter by name any pests you wish to exclude from your scan.

   Click the **Path Exclusions** tab.

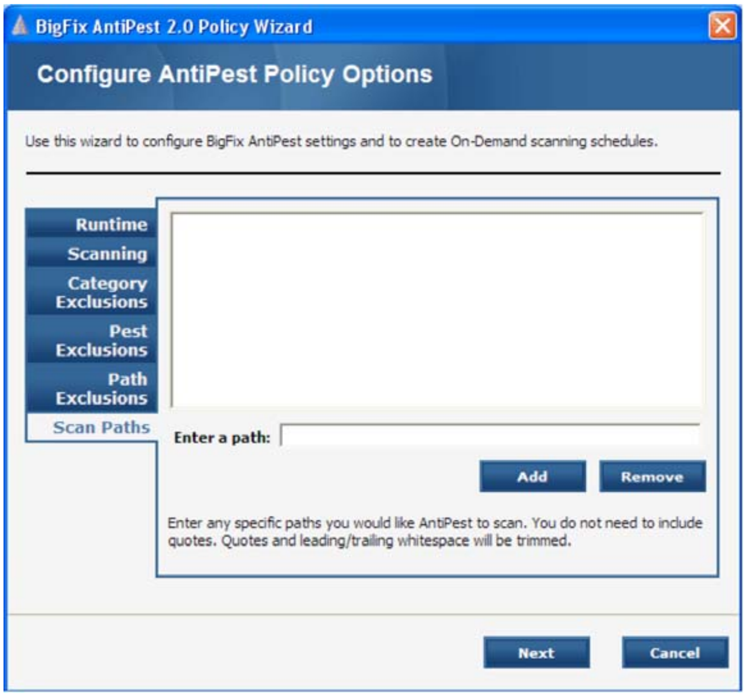


Use this wizard to configure BigFix AntiPest settings and to create On-Demand scanning schedules.

Enter any paths you would like to exclude. You do not need to include quotes. Quotes and leading/trailing whitespace will be trimmed.

6. Enter any paths you wish to exclude from your scan.

   Click the **Scan Paths** tab.



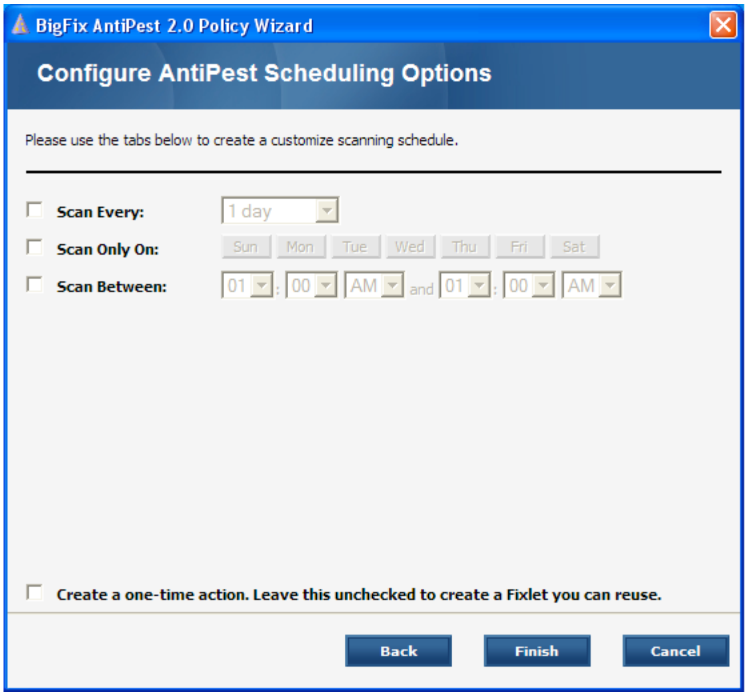
Use this wizard to configure BigFix AntiPest settings and to create On-Demand scanning schedules.

Enter any specific paths you would like AntiPest to scan. You do not need to include quotes. Quotes and leading/trailing whitespace will be trimmed.

7. Enter any specific paths you want BigFix AntiPest to scan.

   Click **Next**.

   The **Configure AntiPest Scheduling Options** window appears.



BigFix AntiPest 2.0 Policy Wizard

Configure AntiPest Scheduling Options

Please use the tabs below to create a customize scanning schedule.

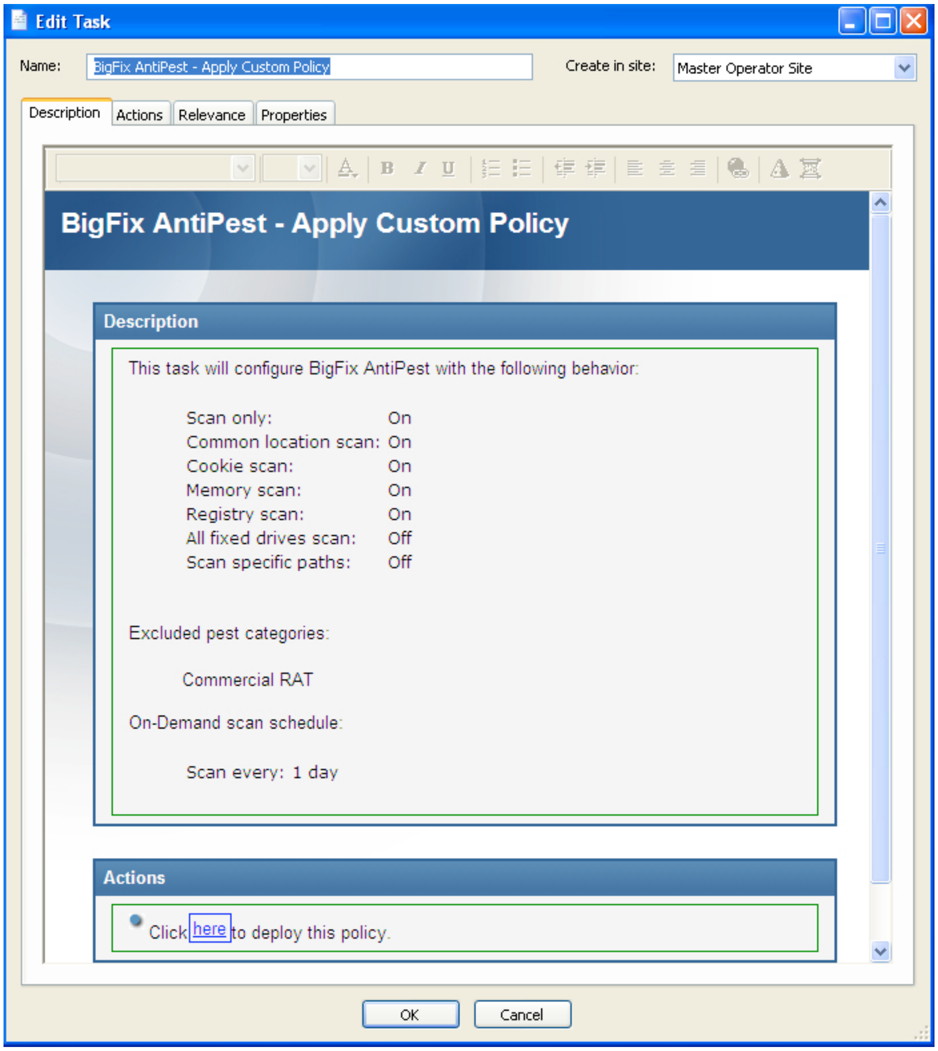
- □ Scan Every: 1 day
- □ Scan Only On: Sun Mon Tue Wed Thu Fri Sat
- □ Scan Between: 01 : 00 AM and 01 : 00 AM

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

8. Use this window to create a customized scanning schedule:
   a. Select your scanning interval. Options range from every 15 minutes to every 30 days.
   b. Select the day or days you wish to scan
   c. Select the time at which to scan.
   d. Leave the last check box unchecked to create a reusable Fixlet, or check the box to create a one-time action.
   e. Click **Finish**.

If you selected a one-time action in step 8d, 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, you will be taken to an **Edit Task** dialog box, in which you can edit descriptions and other parameters of the task.



Edit Task
Name: BigFix AntiPest - Apply Custom Policy
Create in site: Master Operator Site
Description
Actions
Relevance
Properties
OK
Cancel

BigFix AntiPest - Apply Custom Policy

Description

This task will configure BigFix AntiPest with the following behavior:

```
Scan only:             On
Common location scan:  On
Cookie scan:           On
Memory scan:           On
Registry scan:         On
All fixed drives scan: Off
Scan specific paths:   Off
```

Excluded pest categories:

Commercial RAT

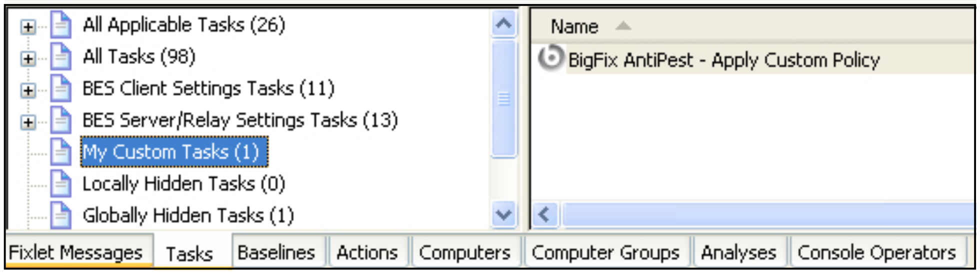
On-Demand scan schedule:

Scan every: 1 day

Actions

- Click here to deploy this policy.

Once you are satisfied, save your task by clicking **OK** and providing your private key password. You will then have a task you can use at any time to apply your custom settings. You will find the task under the **My Custom Tasks** filter on the **Tasks** tab.



All Applicable Tasks (26)
All Tasks (98)
BES Client Settings Tasks (11)
BES Server/Relay Settings Tasks (13)
My Custom Tasks (1)
Locally Hidden Tasks (0)
Globally Hidden Tasks (1)
Name
BigFix AntiPest - Apply Custom Policy
Fixlet Messages
Tasks
Baselines
Actions
Computers
Computer Groups
Analyses
Console Operators

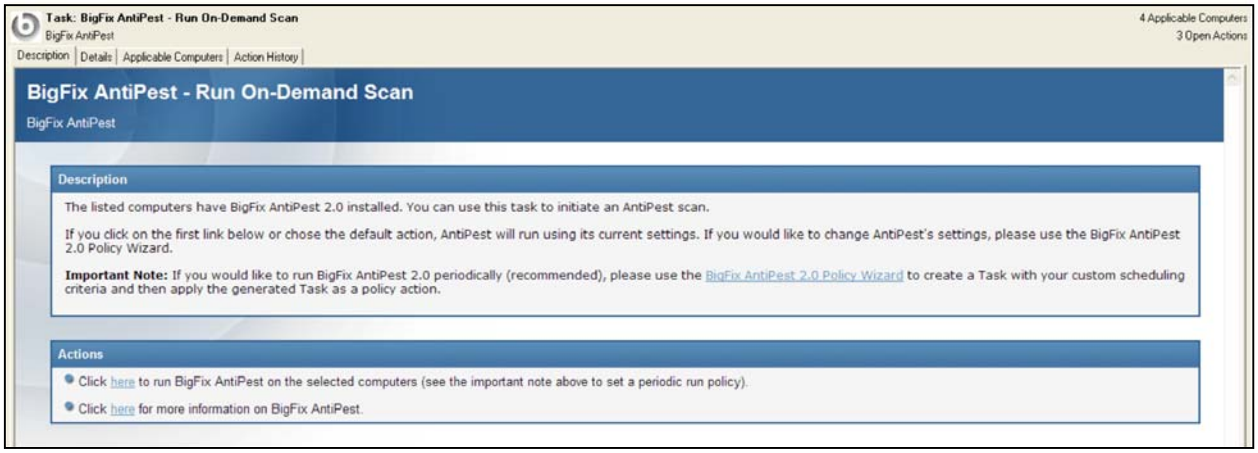
Running an On-Demand Scan

Use the **Run an On-Demand Scan** Task to run a one-time scan using AntiPest's current settings. If you want to change the scan settings or configure recurring scans, use the BigFix AntiPest 2.0 Policy Wizard.

To run an on-demand scan:

1. Click the **Run > Run an On-Demand Scan** link.

The **BigFix AntiPest - Run On-Demand Scan Task** opens.



Task: BigFix AntiPest - Run On-Demand Scan
BigFix AntiPest
4 Applicable Computers
3 Open Actions
Description | Details | Applicable Computers | Action History

BigFix AntiPest - Run On-Demand Scan

BigFix AntiPest

Description

The listed computers have BigFix AntiPest 2.0 installed. You can use this task to initiate an AntiPest scan.

If you click on the first link below or chose the default action, AntiPest will run using its current settings. If you would like to change AntiPest's settings, please use the BigFix AntiPest 2.0 Policy Wizard.

Important Note: If you would like to run BigFix AntiPest 2.0 periodically (recommended), please use the BigFix AntiPest 2.0 Policy Wizard to create a Task with your custom scheduling criteria and then apply the generated Task as a policy action.

Actions

- Click here to run BigFix AntiPest on the selected computers (see the important note above to set a periodic run policy).
- Click here for more information on BigFix AntiPest.

2. Click the **here** link at the bottom to run an On-Demand scan.

   The **Take Action** dialog box opens.

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

   a. Select the computer(s) to which you would like to run an on-demand scan.

   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.

4. Enter your **Private Key Password** when prompted.

   An Action window will appear, in which you can track the progress of your on-demand scan.

   When the scan is finished, the Action window will show 100% complete.

Running Scheduled Scans

Scans can be on-demand or can be scheduled to run at periodic intervals beginning on a user-specified date and time. To run a scheduled scan, use the Wizard to generate a scheduled Task, then apply the Task.

Running Real-Time Protection

There is no configuration necessary to run real-time protection. However, it is important to note that pests are not removed by the real-time component. They are simply blocked. You must run the on-demand component periodically to remove any spyware. In addition, the real-time component does not detect cookie pests.

Manually Running BigFix AntiPest

You can run BigFix AntiPest by double-clicking on the BigFixAntiPest.exe executable. This method will run a silent scan and the results will automatically be picked up by the BigFix Agent the next time it sends a report to the server.

You can override the default configuration by calling BigFixAntiPest.exe with any of the following command options:

`/scanonly`	-scan only, no quarantine
`/rq`	-remove all quarantine
`/uqall`	-unquarantine all quarantined
`/uqlast`	-unquarantine last quarantined
`/cs`	-cookie scan
`/ms`	-memory scan
`/rs`	-registry scan
`/cls`	-common location scan
`/alld`	-all fixed drive scan
`/fldr`	-folder scan (quoted paths must be supplied after the command)

BigFix AntiPest can be removed the same way you uninstall normal Windows applications. Go to **Control Panel > Add/Remove Programs**, select **BigFix AntiPest**, and select **Remove**.

You can see (or change) the settings that control the behavior of BigFix AntiPest by looking at "HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\AntiPest". You will see settings and statistics stored here.

Updating BigFix AntiPest

BigFix provides a Fixlet to update BigFix AntiPest.

You should check the Update BigFix AntiPest 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 AntiPest** link.

   The **BigFix AntiPest—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 AntiPest.

   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.

Troubleshooting

If there is a problem with BigFix AntiPest, try the following troubleshooting tips.

General Troubleshooting

If BigFix AntiPest fails to install, follow the same troubleshooting procedures that you would use to troubleshoot BigFix Client failures. You can find these procedures in the Administrator's Guide.

- There are several knowledge base articles about troubleshooting installation errors at: http://support.bigfix.com.
- If BigFix AntiPest fails to run properly or anything related to the BigFixAntiPest.exe file is not working properly, try to run it manually and see if there are any errors. If nothing appears to happen, enable the debug log and look at the log output for clues to the problem.
- BigFix AntiPest relies on the BigFix Client to manage it properly. If the BigFix Client is not properly working or reporting, then BigFix AntiPest will not work properly.
- For these types of issues, first troubleshoot the BigFix Client problem. After the BigFix Client problem is resolved, see if BigFix AntiPest is functioning properly. You can find information about troubleshooting the BigFix Client in the Administrator's Guide.

Logging

The BigFix Agent manages BigFix AntiPest. All activities the BigFix Agent does relating to BigFix AntiPest will be noted in the normal agent log. The default location for this log is:

C:\Program Files\BigFix Enterprise\BES Client__BESData__Global\Logs

An optional debug log can be enabled for troubleshooting purposes by changing the value "LogFilePath" at "HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\AntiPest\Logging". If this value contains a path to a valid log file, when running, BigFix AntiPest will write a log file that provides verbose run information and error information.

Frequently Asked Questions

Can I get a centralized view and control of my spyware detection and remediation?

Yes. You can centrally manage up to 200,000 endpoints with a single BigFix server and BigFix AntiPest. Centralized reporting at larger scale is fully supported with multiple BigFix servers.

What kinds of malware does BigFix AntiPest detect and remove?

Some examples of malware that BigFix AntiPest detects and removes include:

- Spyware that "phones home" information about you, your computer, and your surfing habits
- Adware that displays unwanted advertising and can slow your PC to a crawl
- Key loggers that can record every keystroke you make, then steal your passwords and other personal data
- Browser hijackers that change your home page and search results
- Remote Access Trojans (RATs) that allow an attacker to remotely control your computer

You can see a complete list of the malware BigFix AntiPest detects and removes here: http://www.ca.com/us/securityadvisor/pest/browse.aspx.

In what environments can BigFix AntiPest be installed?

BigFix AntiPest supports Windows 2000, Server 2003, and XP.

What kinds of spyware scanning options are available?

BigFix provides scanning options for the following:

- **Files and folders**: Scans files and folders for pests.
- **Cookies**: Scans for any cookie shared among two or more sites for the purpose of tracking a user's browsing history.
- **Windows registry**: Scans Windows registry for known pest keys and values.
- **Memory**: Scans running processes for pests by scanning the virtual memory and physical files of the running processes and loaded modules (DLLs)
- **Common locations**: Scans common locations for pests. Common locations include: the startup folder, desktop folder, program folder, cookies folder, program files folder, system folder, Windows folder, profiles folder, etc. The list of folders is determined based on the available definition files. Any location where pests are known to reside is considered a common location.
- **All fixed drives**: Scan all fixed drives on the machine.
- **Real-time**: BigFix AntiPest provides real-time blocking of spyware.

Does BigFix AntiPest support white list or user-defined exclusions?

Yes, white list or user-defined exclusions are supported in BigFix AntiPest.

Can definition updates be controlled and/or downloaded using the management console?

Yes. The BigFix Console is used to manage all aspects of the definition update process.

Are silent/background definition updates supported?

Yes. BigFix AntiPest deploys definitions updates silently in the background without bothering the end-user.

Can updates be scheduled?

Yes. Updates can be scheduled using many different scheduling criteria, such as deploying the updates at a specific time, targeting a specific subset of computers, etc.

Do I need to run on-demand scans? Won't real-time block everything?

AntiPest 2.0 does include a real-time component, but it is still important to run scans.

Real-time will only *block* spyware, it does not remove it. In addition, real-time will find only active spyware, not resident spyware such as tracking cookies, or dormant spyware that is not currently active but may have been installed on a machine when real-time was off or not installed. In fact, real-time scanning specifically excludes cookie scanning. You will want to run periodic scans to do the actual removal of spyware and to clean cookies.

Are automatic definition updates supported?

Yes. You can use a customer-installed configuration option to deliver automatic definition updates. Note that BigFix recommends the industry best practice of testing and authorizing individual updates before they are released for security and change management reasons; however, automated definition updates are supported.

For more information, see http://support.bigfix.com/bes/misc/actionregenerator.html.

How are definition updates handled?

BigFix automatically publishes BigFix AntiPest update definitions to customers in the standard form of a BigFix Fixlet message. Administrators are able to see in real-time which computers require the update, enabling them to use the BigFix platform to distribute the definition update only to those computers requiring it. Because the definition update process utilizes the BigFix platform, there is significant bandwidth savings with local distribution points (relays), agent auto-discovery of closest distribution point, auto-load-balancing, auto-failover, and bandwidth throttling.

Can BigFix update definitions on mobile or remote computers?

Yes. BigFix AntiPest can update computers that are intermittently connected. Computers that have a network connection can receive updates immediately; computers that do not have a network connection can receive the update as soon as network connectivity becomes available. BigFix can even manage and update computers securely across public networks.

Does BigFix AntiPest offer bandwidth controls?

Yes. The BigFix AntiPest product uses all of the capabilities of the BigFix platform, which includes sophisticated policy-based bandwidth limitation options.

Does BigFix AntiPest support multi-site deployment?

Yes. BigFix AntiPest provides multi-site deployment. BigFix is typically installed in an enterprise environment spanning geographically distributed sites, including mobile users. The BigFix platform provides various features to make multi-site deployment possible, including a highly scalable distributed real-time architecture. BigFix can integrate with Active Directory group information, but does not require Active Directory.

Does BigFix AntiPest support load balancing?

The BigFix platform provides for automatic load balancing and fail-over. This is done primarily with BigFix Relays. Relays are used as distribution and collection points. BigFix Agents running the AntiPest product are capable of automatically finding the closest available relay for communication and load balancing. Fail-over to alternate relays is automatic and highly configurable.

What type of reporting does BigFix AntiPest provide?

BigFix AntiPest leverages the reporting capabilities of the BigFix platform to deliver real-time visibility into the anti-spyware efforts of the enterprise. Reports are available in the Administrative Console application, as well as a Web-based reporting environment. A partial list of reporting data elements includes:

- # Pests Found (Last Run)
- # Pests Found (Lifetime)
- # Pests in Quarantine
- # Pests Quarantined (Last Run)
- AntiPest Engine Version
- Average Run Time
- BigFix AntiPest Version
- Category Exclusions
- Common Locations Scan
- Cookie Scan
- Definition Version
- Errors (Last Run)
- First Time Run
- Install Date
- Last Definition Update
- Last Run Finish Time
- Last Run Start Time
- Memory Scan
- Number of Times Run
- Path Exclusions
- Pest Exclusions
- Pests Found (Last Run)
- Pests Found (Lifetime)
- Registry Scan
- Remove Quarantined
- Scan Only

BigFix provides comprehensive reporting using the BigFix Console.

BigFix also provides comprehensive reporting using BigFix Web Reports. HTML reporting is fully customizable. For example, you can select specific data elements for the report, filter by a set of attributes, groups of machines, by geographical and physical locations, types of charts, etc.

You can also author custom reports or contract BigFix Professional Services to help author custom reports.

Can I export report data?

Yes. Report data can be exported using the Web Report interface in CSV format. Alternately, BigFix also provides a Database API for direct access to reporting data using 3rd party products via standard SQL. BigFix 7.0 also provides a SOAP interface for querying the database.

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

Yes. BigFix AntiPest provides a dashboard view with overview statistics and charts that enable administrators to gauge the current health of the system (from a spyware perspective), and to track progress as AntiPest eliminates spyware from computers.

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/.

(eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
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)."

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 gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@graphviz.org).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (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.

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). 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 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;

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