BigFix® AntiVirus 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

CONTENTS II

PREFACE 3

AUDIENCE 3
ORGANIZATION OF THIS GUIDE 3
CONVENTIONS USED IN THIS GUIDE 3
VERSIONS 3

INTRODUCTION 4

QUICK-START 6

BEGINNING SETUP 6
ACCESSING THE BIGFIX ANTIVIRUS DASHBOARD 7
Launching the Dashboard 7
Understanding the BigFix AntiVirus Dashboard Controls 8
Reading the Dashboard's Overview Statistics and Charts 9

USING BIGFIX ANTIVIRUS 11

DEPLOYING BIGFIX ANTIVIRUS 11
UPDATING DEFINITIONS 13
USING THE BIGFIX ANTIVIRUS WIZARD 14
Configuring On-Demand Scanning Policies 14
Configuring Real-Time Detection Options 20
RUNNING AN ON-DEMAND SCAN 26
RUNNING SCHEDULED VIRUS SCANS 27
RUNNING REAL-TIME PROTECTION 27
UPDATING BIGFIX ANTIVIRUS 28

FREQUENTLY ASKED QUESTIONS 29

GENERAL QUESTIONS 29
REPORTING 31

ACKNOWLEDGEMENTS AND NOTICES 32

Preface

Audience

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

Organization of this Guide

This guide is composed of four major sections:

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

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 AntiVirus, Version 2.0 and later.

Introduction

BigFix AntiVirus enables you to maintain virus defense on all your managed computers, whether they are in or out of the enterprise network. It features include the ability to deploy antivirus software to network endpoints, continuously monitor endpoints in real-time, run both on-demand and scheduled reports, update virus signature files, and assess network health and track the progress of your efforts by using dashboard overviews. In addition, BigFix provides for easy removal of other antivirus products.

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

- **Rapid response to emergency threats**—BigFix leverages a network of rapid response centers that monitor and respond to threats 24 x 7.
- **Antivirus policy enforcement**—BigFix endpoint agents ensure the antivirus client is installed and running on desktops, laptops, and servers, as well as remote and mobile computers, thereby closing the 5-15% gap in antivirus coverage common to antivirus deployments.
- **Rapid distribution of definition updates**—Reliable and rapid distribution capabilities, including the ability to verify receipt of definition updates.
- **Centralized reporting across multiple platforms**—Comprehensive, accurate, and consolidated real-time reporting of antivirus status in environments with multiple platforms and a distributed network.
- **Closed-loop feedback**—Real-time status from each endpoint, enabling IT personnel to ensure successful delivery of updates within a few minutes without adversely affecting the network.

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 AntiVirus.

Beginning Setup

This procedure assumes that you already have installed BigFix.

1. Obtain a masthead for the BigFix AntiVirus site.

   Email licensing@bigfix.com to request the masthead.

2. Add the BigFix AntiVirus 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**.

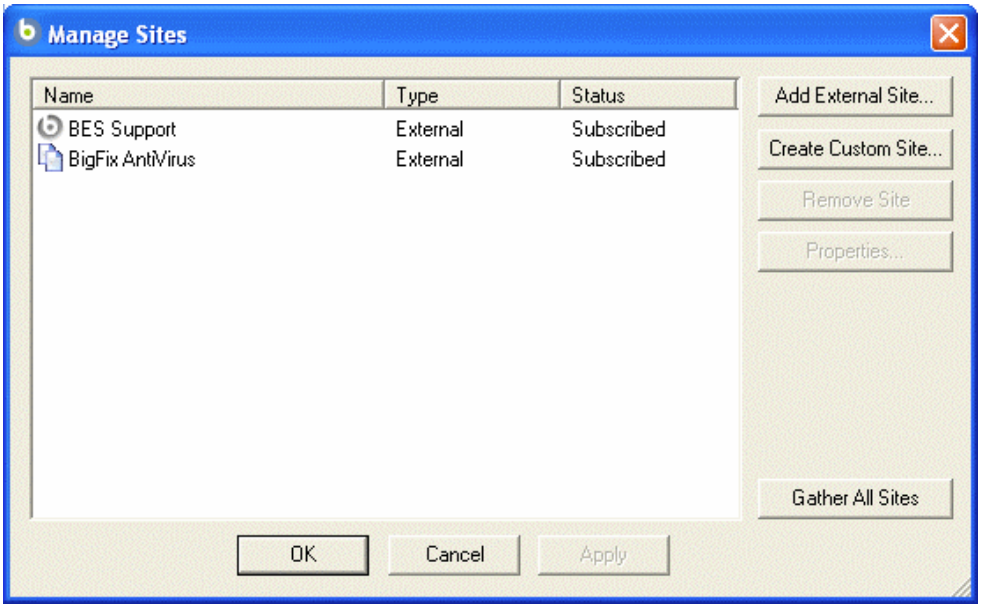
   c. Enter your Private Key Password and click **OK**.

   At this point, the BigFix AntiVirus 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.

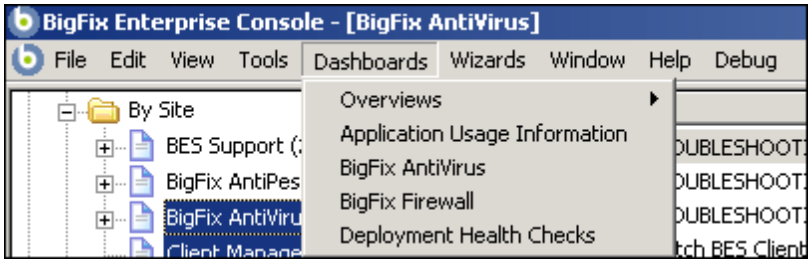
   You will see a new BigFix AntiVirus entry in the **Dashboards** menu and your Navigation Bar. The site will show as **Subscribed** in the **Manage Sites** dialog.



Accessing the BigFix AntiVirus Dashboard

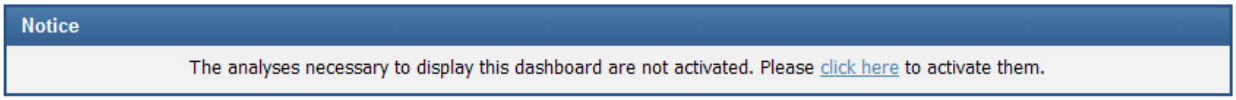
BigFix AntiVirus provides a dashboard view with overview statistics and charts that enable administrators to gauge the current health of their system and to track progress as BigFix AntiVirus enforces antivirus compliance and pushes updates throughout the network. In addition, you can use the Dashboard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

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



Launching the Dashboard

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



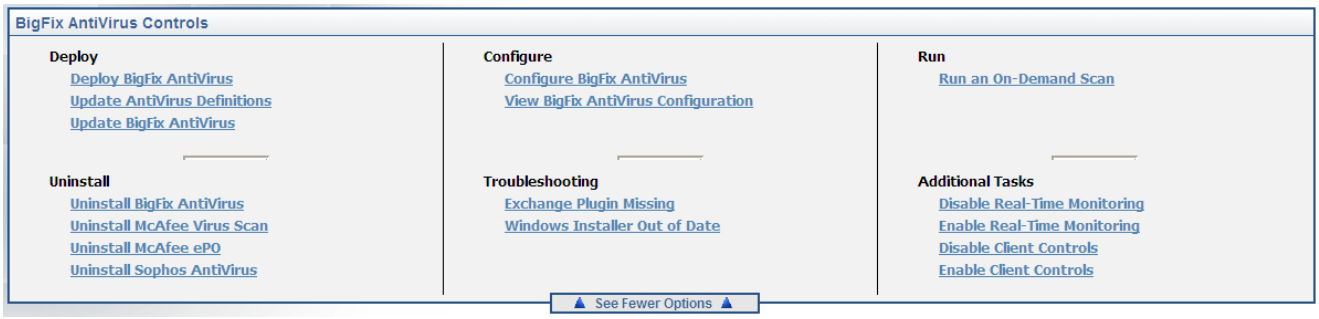
1. Click the **click here** link.
2. Enter your private key password when prompted and click **OK**.

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

Understanding the BigFix AntiVirus Dashboard Controls

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



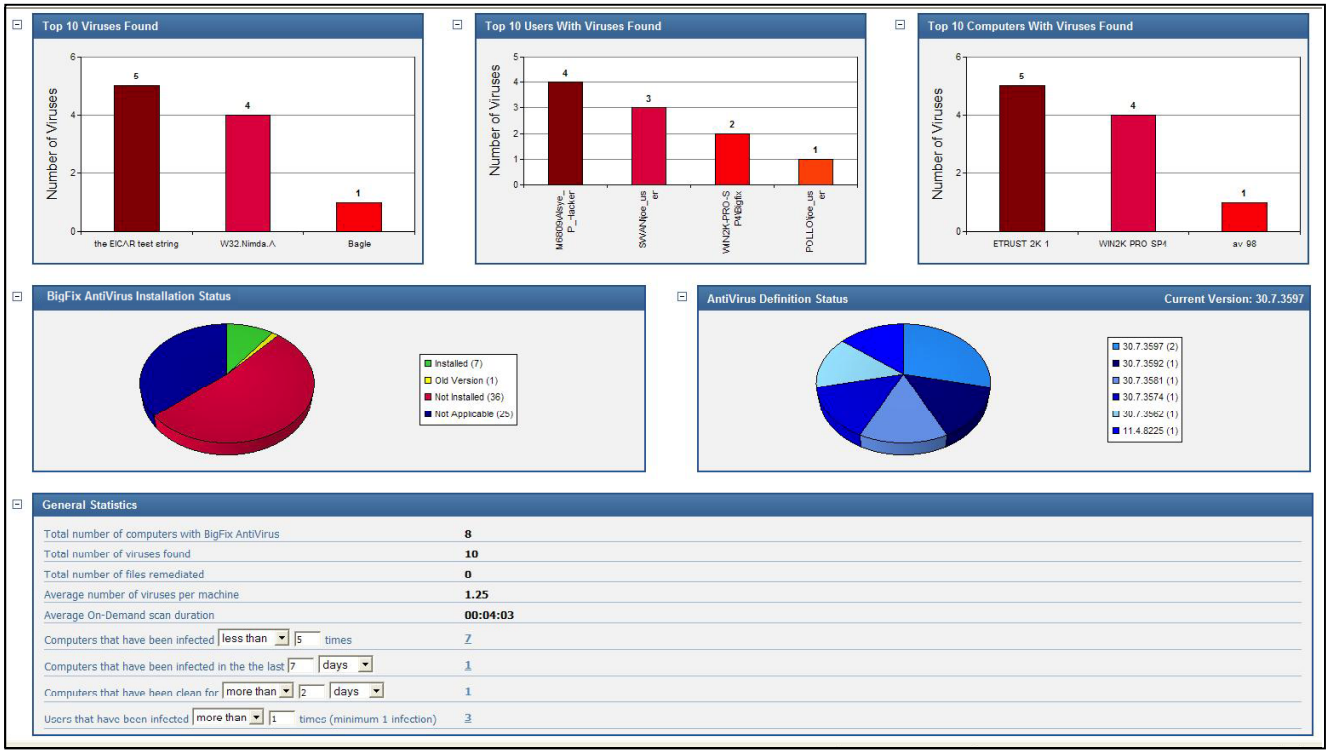
The controls that BigFix AntiVirus provides are:

- **Deploy**: Use the controls in this section to deploy BigFix AntiVirus, update BigFix AntiVirus or update BigFix AntiVirus definitions.
  - Deploy BigFix AntiVirus
  - Update AntiVirus Definitions
  - Update BigFix AntiVirus
- **Uninstall**: Use the controls in this section to uninstall antivirus products on your network, including BigFix AntiVirus.
  - Uninstall BigFix AntiVirus
  - Uninstall <other antivirus product(s) on your network>
- **Configure**: Use the controls in this section to configure BigFix AntiVirus or to view your existing configurations.
  - Configure BigFix AntiVirus
  - View Agent Configuration
- **Troubleshooting**: Use the controls in this section to monitor possible problems with BigFix AntiVirus.
  - Exchange Plugin Missing
  - Windows Installer Out of Date
- **Run**: Use this control to run an on-demand virus scan.
  - Run an On-Demand Scan

- **Additional Tasks**: Use these controls to enable or disable real-time monitoring and client controls. Client controls allow end users to view and change their BigFix AntiVirus configurations.
  - Disable Real-Time Monitoring
  - Enable Real-Time Monitoring
  - Disable Client Controls
  - Enable Client Controls

Reading the Dashboard's Overview Statistics and Charts

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



BigFix AntiVirus provides charts illustrating:

- **Aggregate Infection History**: You can view the history for Last 2 Hours, Last 8 Hours, Last 24 Hours, Last 7 Days, Last 30 Days, Last 26 Weeks, and Last 52 weeks, provided you have been running BigFix AntiVirus for the appropriate amount of time.
- **Top 10 Viruses Found**: This is a bar chart showing the most frequently detected viruses.
- **Top 10 Users With Viruses Found**: This is a bar chart showing the most frequently infected users.
- **Top 10 Computers With Viruses Found**: This is a bar chart showing the most frequently infected computers.
- **AntiVirus Installation Status**: This is a pie chart showing whether computers have the current version of BigFix AntiVirus installed, not installed, or have an old version installed.
- **AntiVirus Definition Status**: This is a pie chart showing which computers have which version of the antivirus definitions installed.

The statistics you can gather on your deployment include:

- Total number of computers with BigFix AntiVirus

- Total number of viruses found
- Total number of files remediated
- Average number of viruses per machine
- Average On-Demand scan duration
- Computers that have been infected <less than, more than, exactly> <number> times
- Computers that have been infected in the last <number> <hours, days, weeks>
- Computers that have been clean for <less than, more than, exactly><number> <hours, days, weeks>
- Users that have been infected <less than, more than, exactly> <number> times (minimum 1 infection)

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.

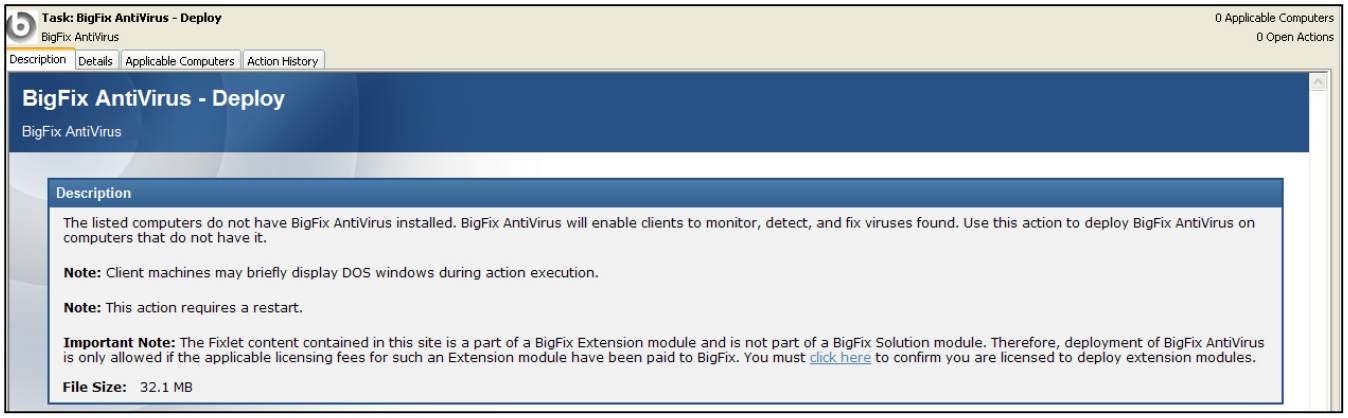
Using BigFix AntiVirus

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

Deploying BigFix AntiVirus

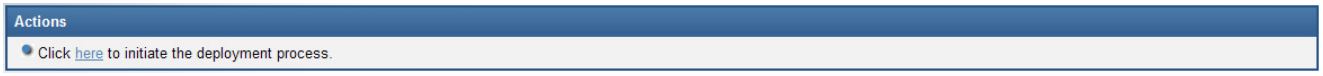
1. From the Dashboard, click on the **Deploy BigFix AntiVirus** link.

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



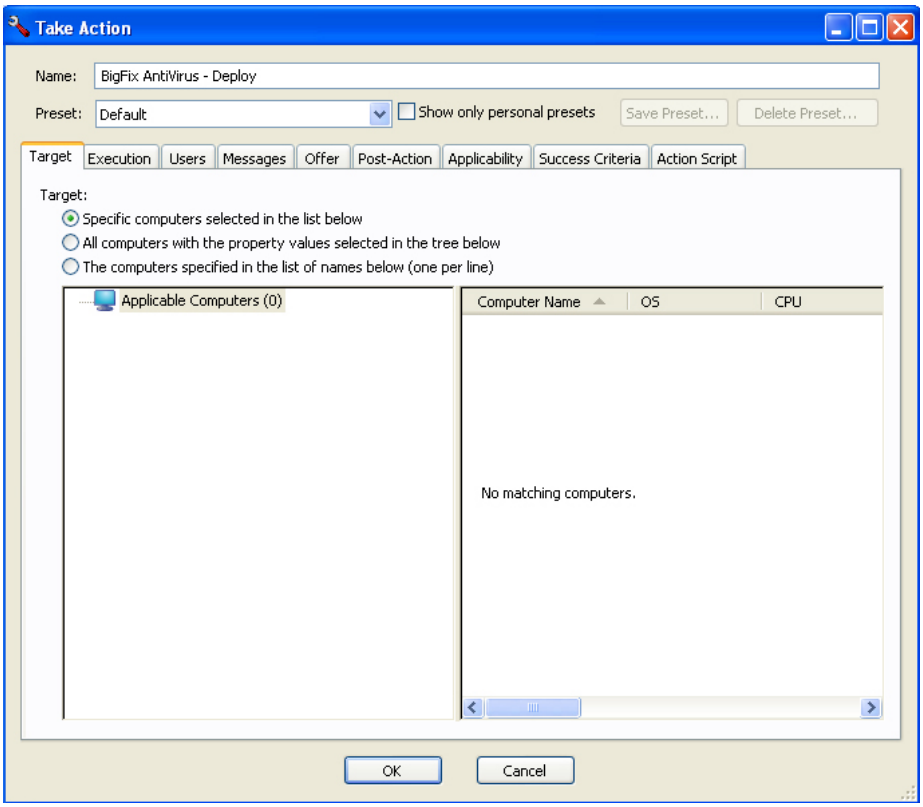
2. Click the **click here** link located in the **Description** section to accept the extension license.

   A link will appear in the **Actions** section.



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

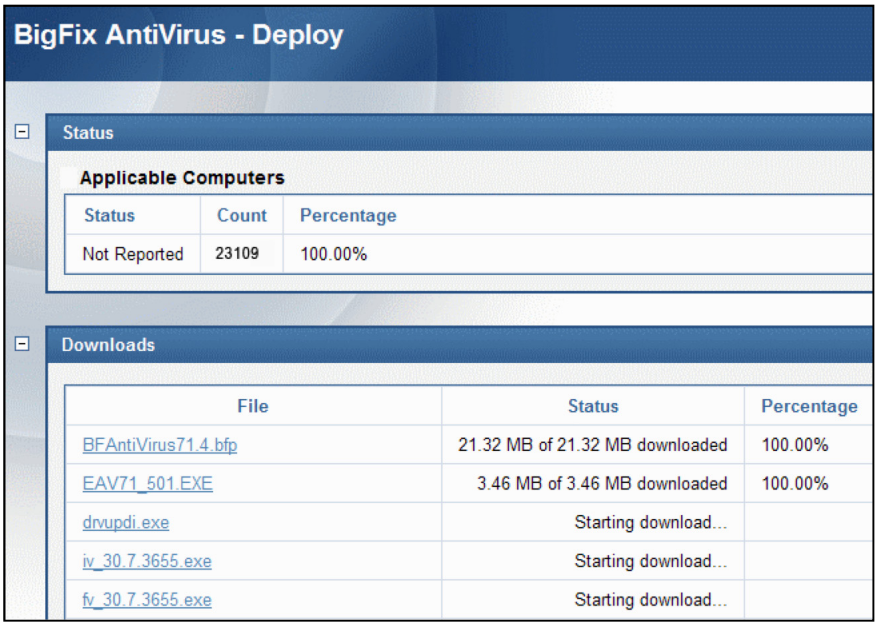
   The **Take Action** dialog box opens.



4. In the **Take Action** dialog box:
   a. Select the computer(s) to which you would like to deploy BigFix AntiVirus.
   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.

Status	Count	Percentage
Pending Restart	23109	100.00%

For more information about restarting computers using the BigFix Console, consult the *Console Operators Guide*.

After restarting, the deployment will be complete.

Status	Count	Percentage
Completed	23109	100.00%

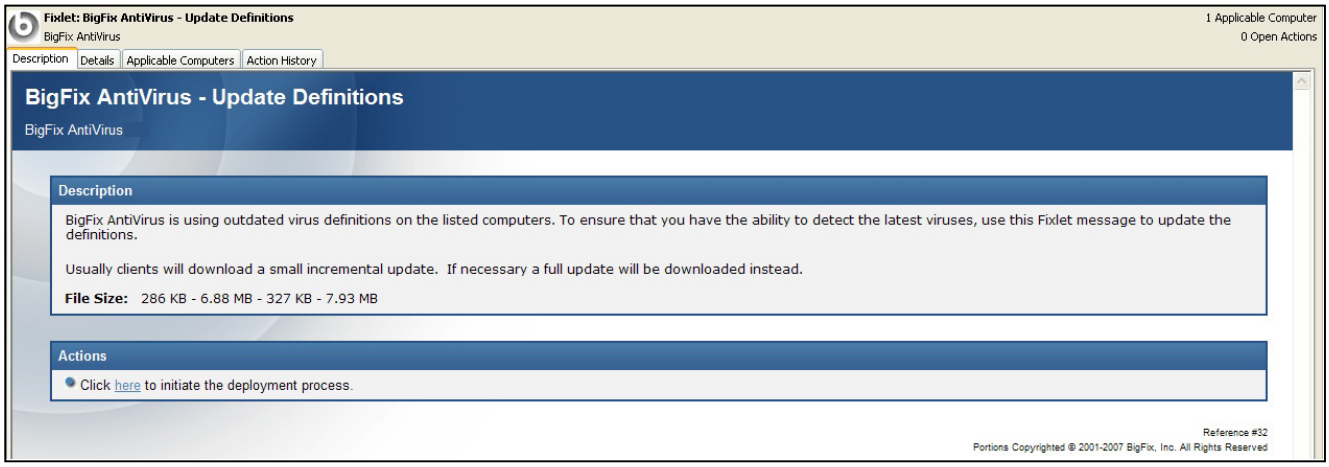
You will be ready to run on-demand or scheduled virus scans, update virus definition files, and view metrics about the health of your network.

Updating Definitions

Virus definitions are updated every weekday, and it is recommended that you perform a quick manual test for each definition before widely deploying BigFix AntiVirus. Although it is recommended that you perform a manual test for each definition, you can use the action regenerator at http://support.bigfix.com/bes/misc/actionregenerator.html to auto-update your virus definitions.

1. From the Dashboard, click the **Update AntiVirus Definitions** link.

   The **BigFix AntiVirus—Update Definitions** Fixlet window opens.



2. Click the **here** link 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 virus definitions.

   b. Set any desired constraints and other options.

   c. Click **OK** when you are finished, and then enter your **Private Key Password**.

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

Using the BigFix AntiVirus Wizard

You can configure both On-Demand and Real-Time scanning policies for BigFix AntiVirus using a Wizard. In addition, you can create a Task to apply the settings so that you can repeat the configuration without going through the wizard, or you can apply the settings immediately.

BigFix AntiVirus offers two scan modes:

- **Secure** is the default normal scan mode, and review is the debug mode to figure out why something might not have been caught by the scanner.
- The **Heuristic Scanner** engine scans files for viruses whose signatures have not yet been isolated and documented.

Use the **Scan Alternate Data** Streams option to search for virus content in alternate data streams on NTFS and resources on HFS+ file systems.

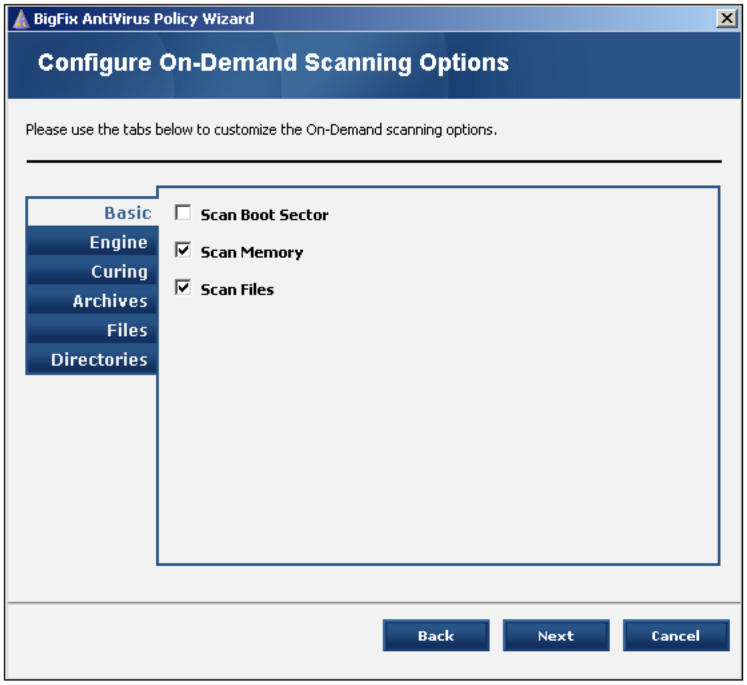
Configuring On-Demand Scanning Policies

To configure on-demand scanning policies:

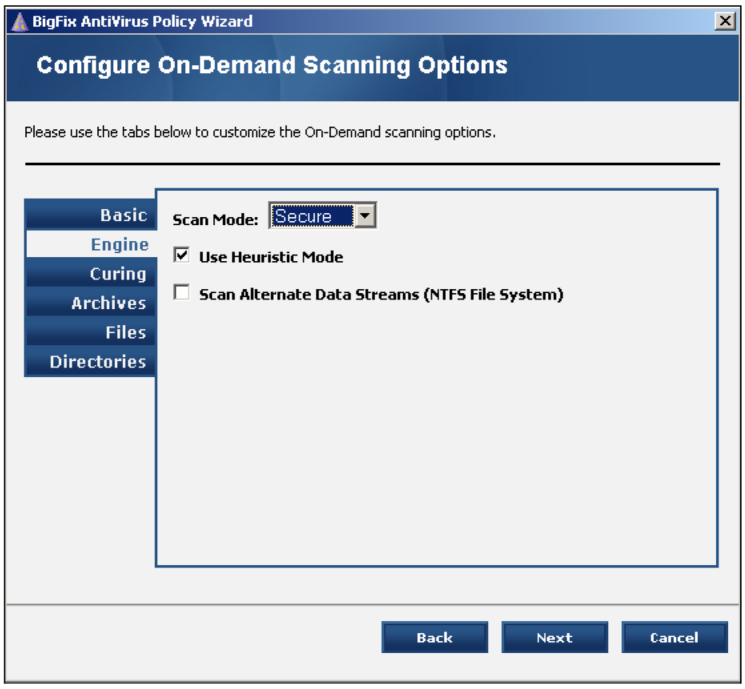
1. From the Dashboard, click the **Configure BigFix AntiVirus** link or select **Wizards > BigFix AntiVirus Policy Wizard**.

   The **BigFix AntiVirus Policy Wizard** opens.

2. To configure On-Demand scanning policies, click the **On-Demand** button.
3. On the **Basic** tab, choose whether to scan the boot sector, memory, and/or files.



4. On the **Engine** tab:

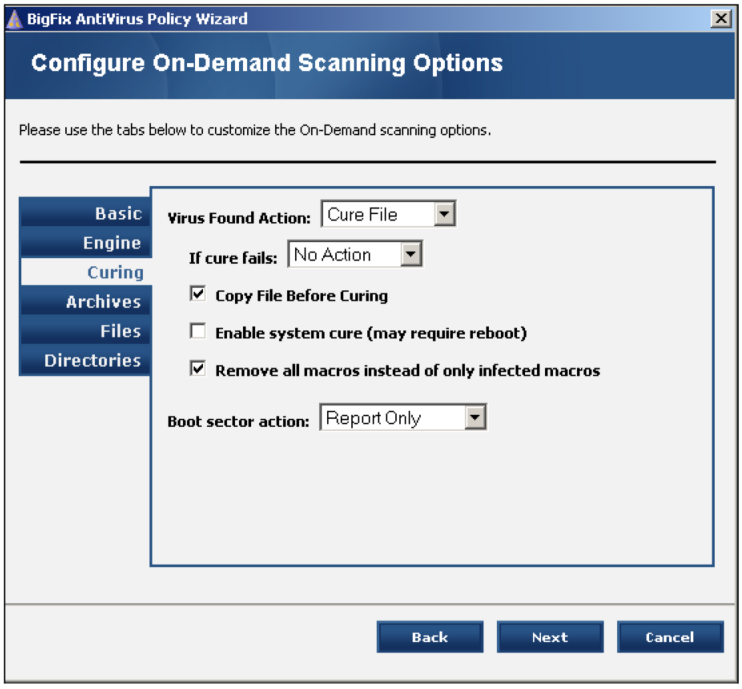


a. Choose whether to scan in Secure or Reviewer mode.

b. Choose whether to use Heuristic mode.

c. Choose whether to scan alternate data streams (for an NTFS Files system).

5. On the **Curing** tab:



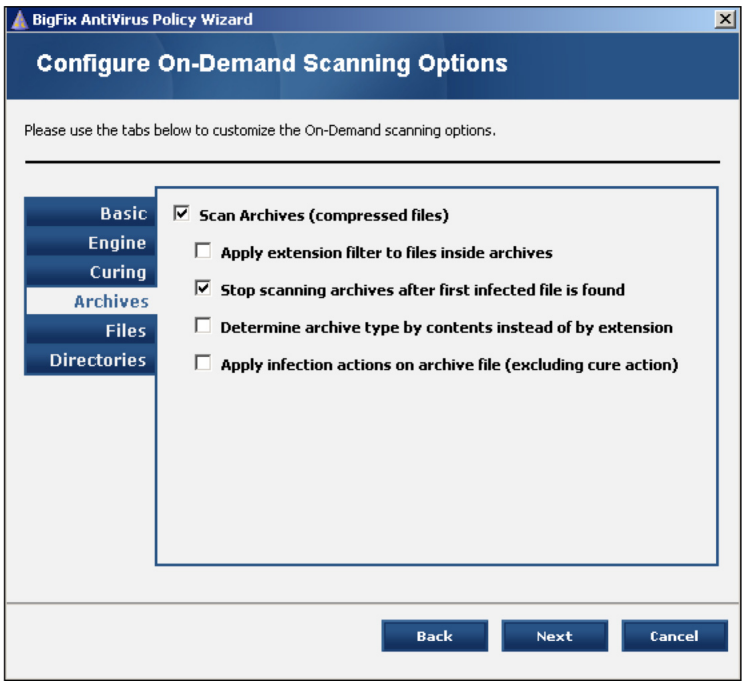
a. For **Virus Found Action**, choose Report Only, Cure File, Rename File, Delete File, or Move File.

b. For **If cure fails**, choose No Action, Rename File, or Move File.

c. Choose whether to copy file before curing, enable system cure, and/or remove all macros instead of only infected macros.

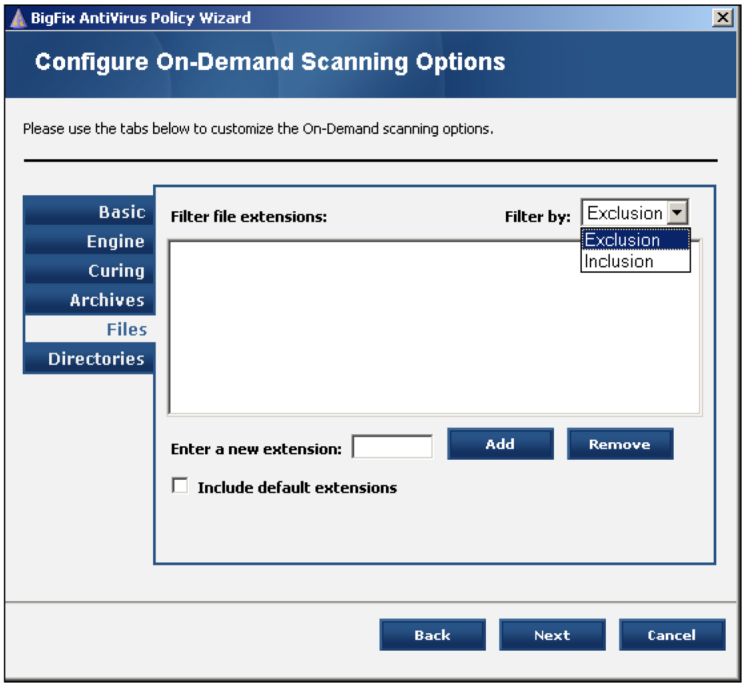
d. For **Boot Section Action**, choose Report Only or Cure Boot Sector.

6. On the **Archives** tab, choose whether to scan archives.

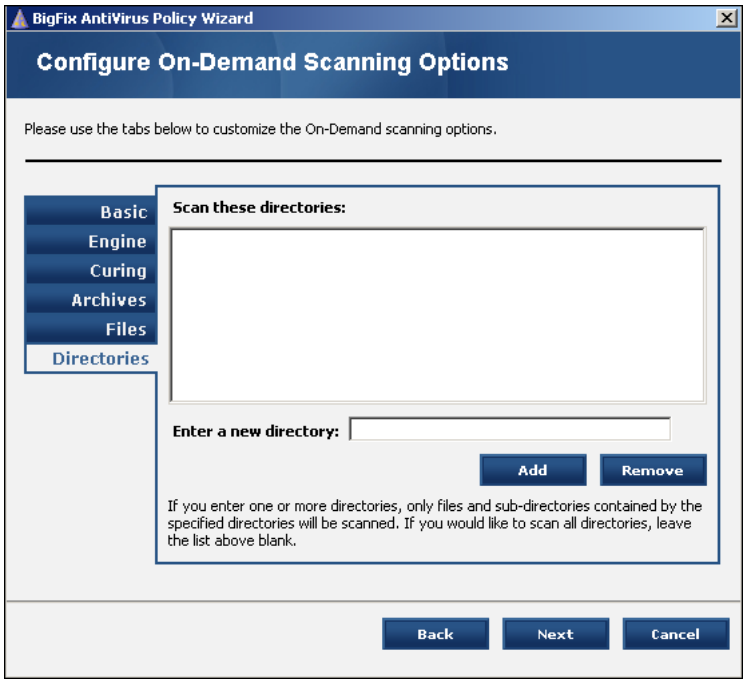


If you choose to scan archives, you can also choose whether to apply extension filters to files inside archives, stop scanning archives after the first infected file is found, determine archive type by contents instead of by extension, and/or apply infection actions on archive files (excluding the cure action).

7. On the **Files** tab, choose any file types you want to filter, either by exclusion or inclusion.



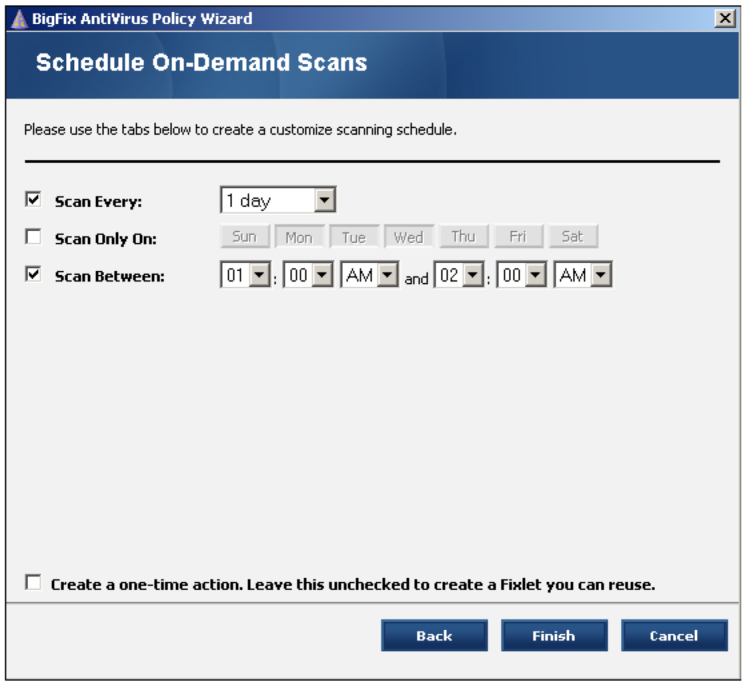
8. On the **Directories** tab, specify specific directories to scan.



If you want to scan all directories, leave this list blank.

9. Click **Next**.

The **Schedule On-Demand Scans** window opens.



10. 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.

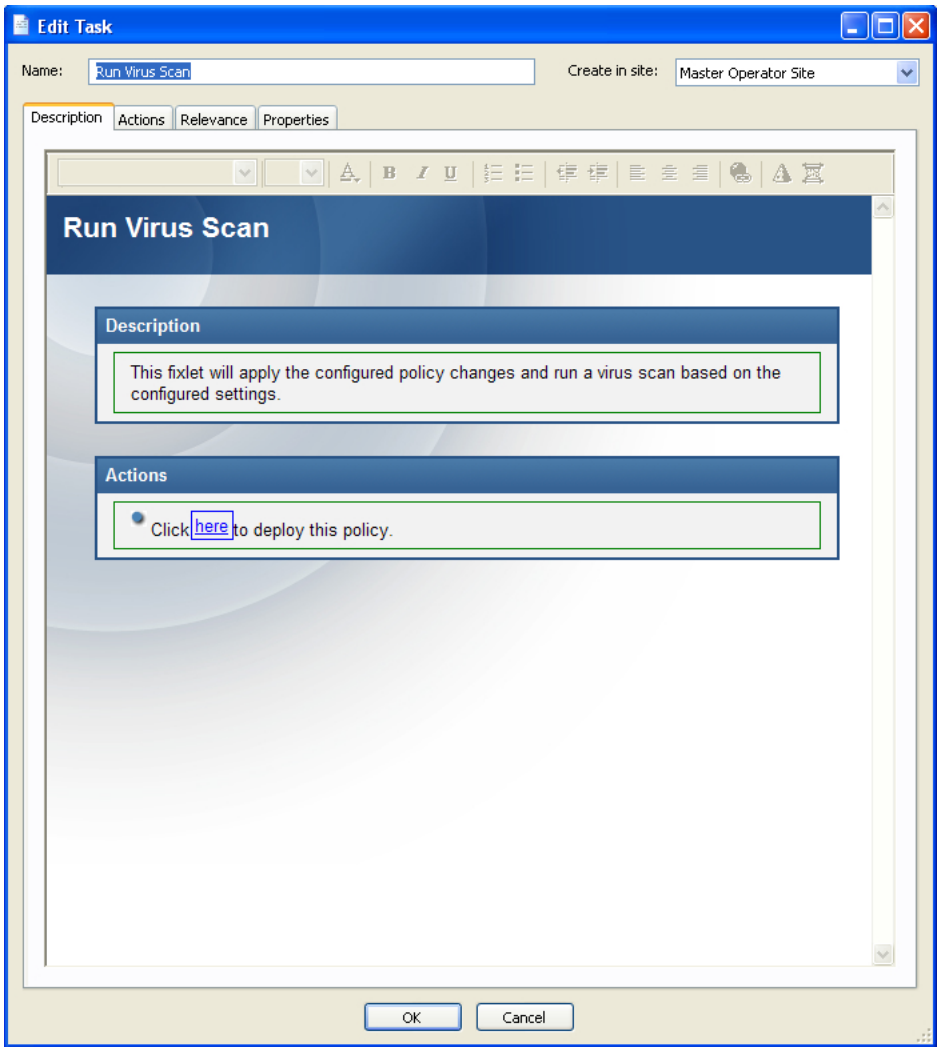
c. Select the time at which to scan

d. Leave the last check box unchecked to create a reusable Fixlet, or check the box to create a one-time action.

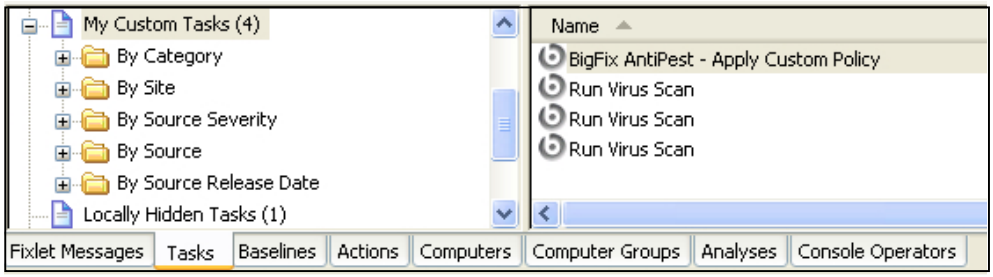
e. Click **Finish**.

If you selected a one-time action in step 10d, 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.



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.



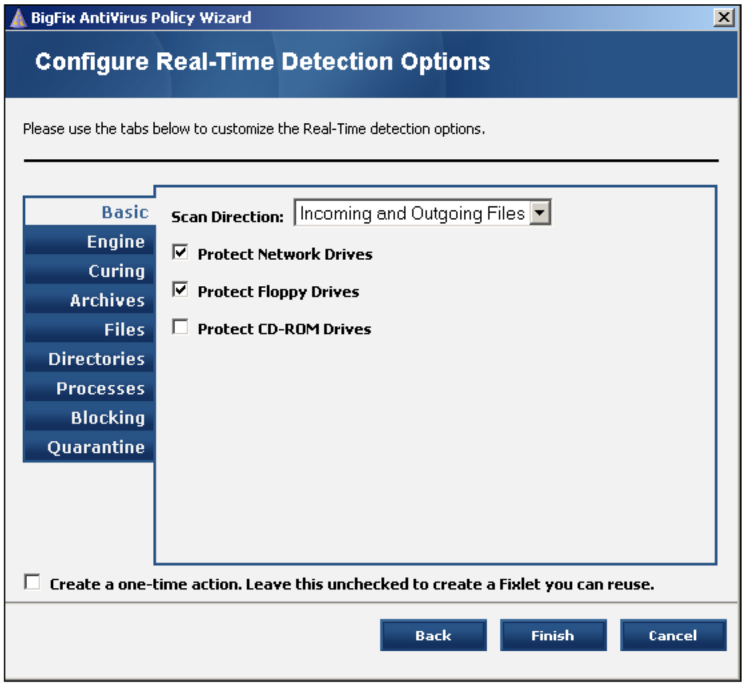
Configuring Real-Time Detection Options

To configure real-time detection options:

1. From the Dashboard, click the **Configure BigFix AntiVirus** link.

   The **BigFix AntiVirus Policy Wizard** opens.

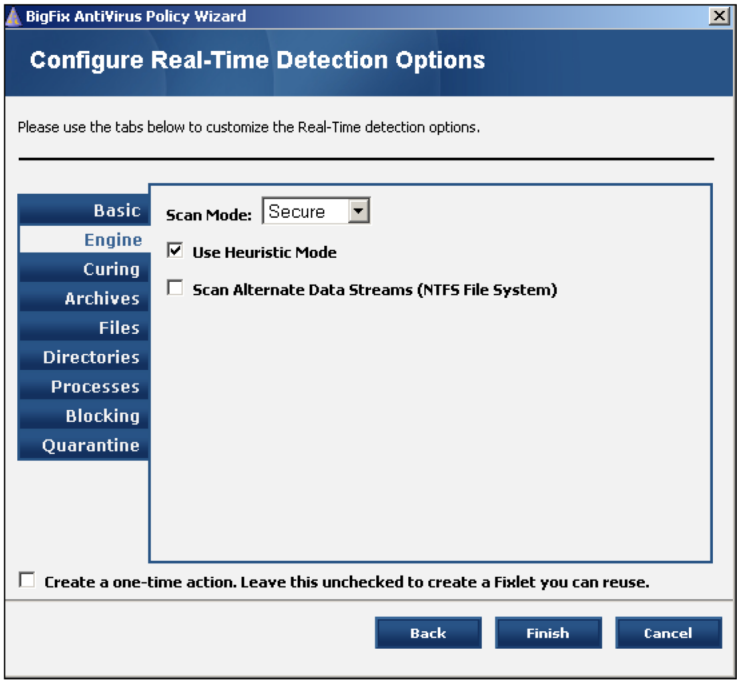
2. To configure Real-Time scanning policies, click the **Real-Time** button.
3. On the **Basic** tab:



a. Choose whether to scan incoming files, incoming and outgoing files, or no files.

b. Choose whether to protect network drives, floppy drives, and/or CD-ROM drives.

4. On the **Engine** tab:

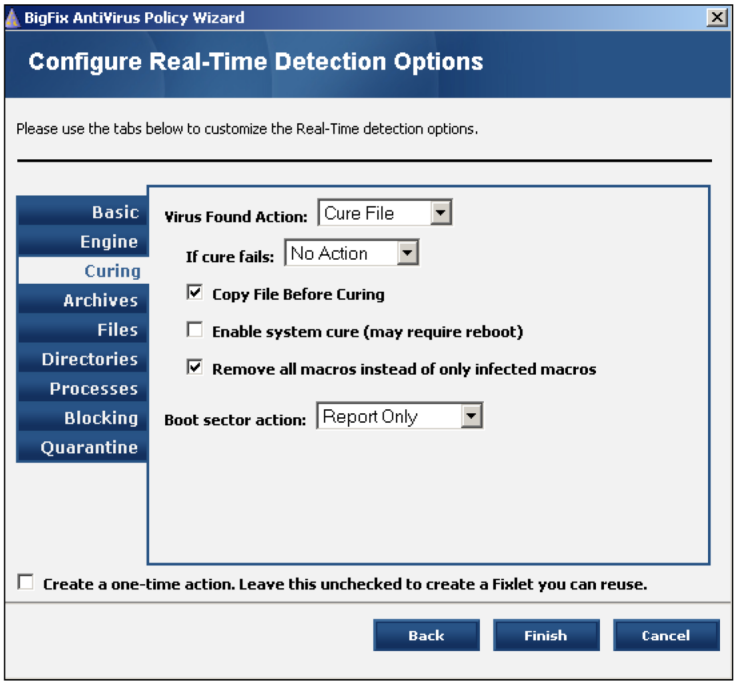


a. Choose whether to scan in Secure or Reviewer mode.

b. Choose whether or not to use Heuristic mode.

c. Choose whether to scan alternate data streams (for an NTFS Files system).

5. On the **Curing** tab:



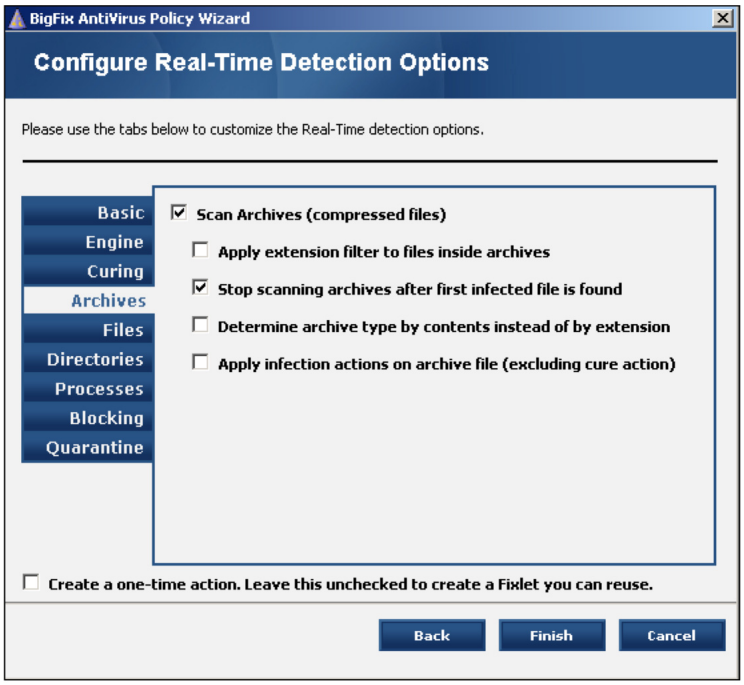
a. For **Virus Found Action**, choose Report Only, Cure File, Rename File, Delete File or Move File.

b. For **If cure fails**, choose No Action, Rename File, or Move File.

c. Choose whether to copy file before curing, enable system cure, and/or remove all macros instead of only infected macros.

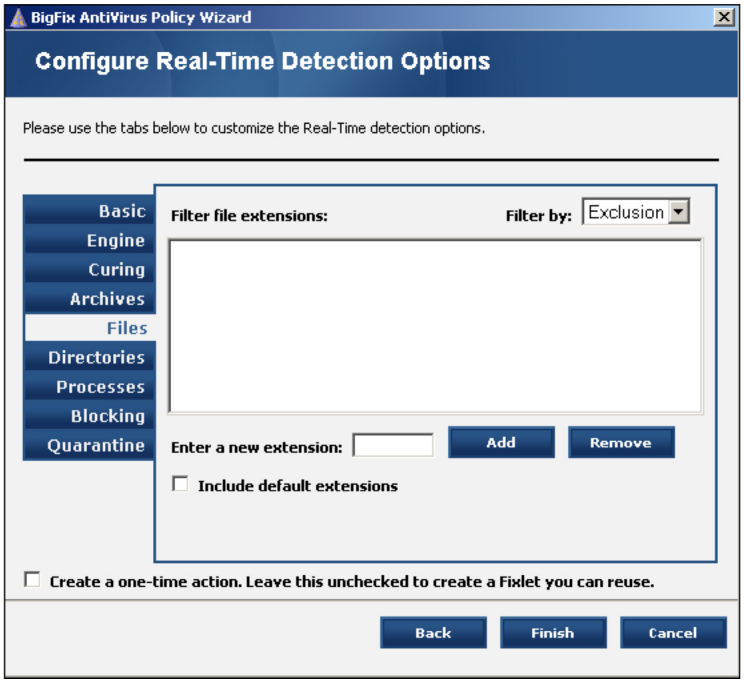
d. For **Boot Section Action**, choose Report Only or Cure Boot Sector.

6. On the **Archives** tab, choose whether to scan archives.

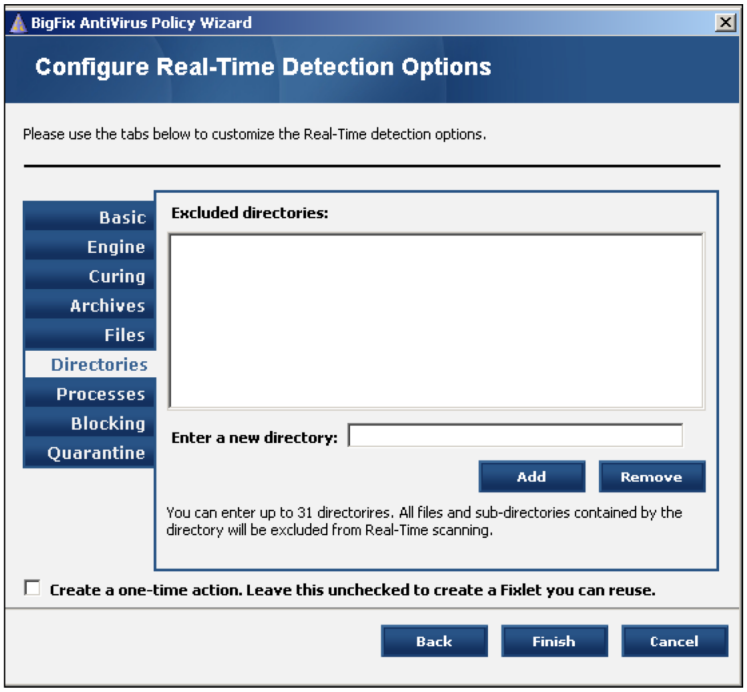


If you choose to scan archives, you can also choose whether to apply extension filters to files inside archives, stop scanning archives after the first infected file is found, determine archive type by contents instead of by extension, and/or apply infection actions on archive files (excluding cure action).

7. On the **Files** tab, choose any file types you want to filter, either by exclusion or inclusion.

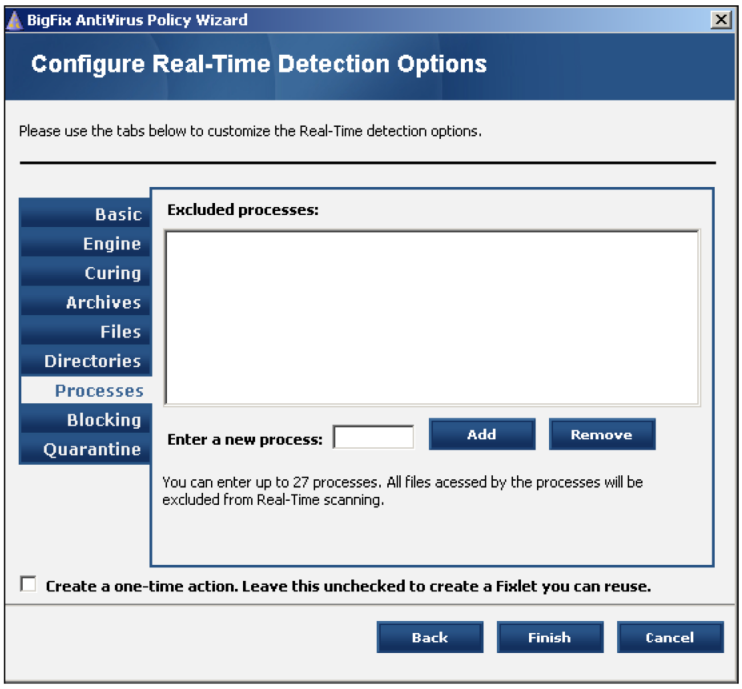


8. On the **Directories** tab, specify specific directories to scan.

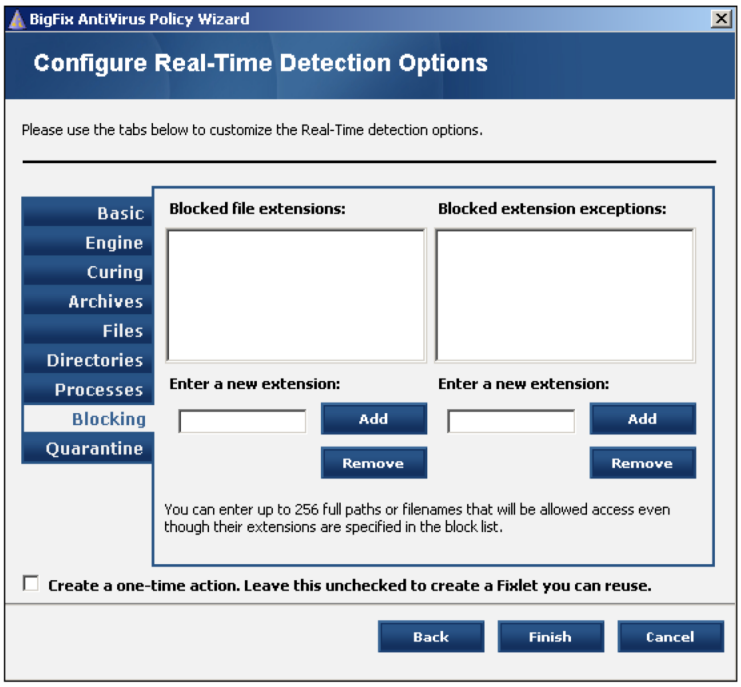


If you want to scan all directories, leave this list blank.

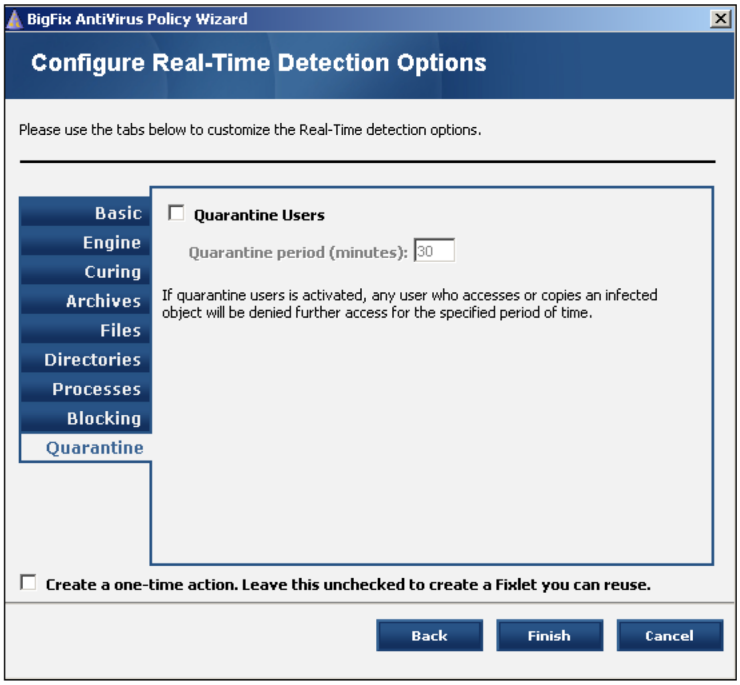
9. On the **Processes** tab, enter up to 27 processes to exclude from Real-Time scanning.



10. On the **Blocking** tab, enter up to 256 full paths or filenames that will be allowed access even though their extensions are specified in the block list.



11. On the **Quarantine** tab, choose whether to quarantine users and, if so, for how many minutes.

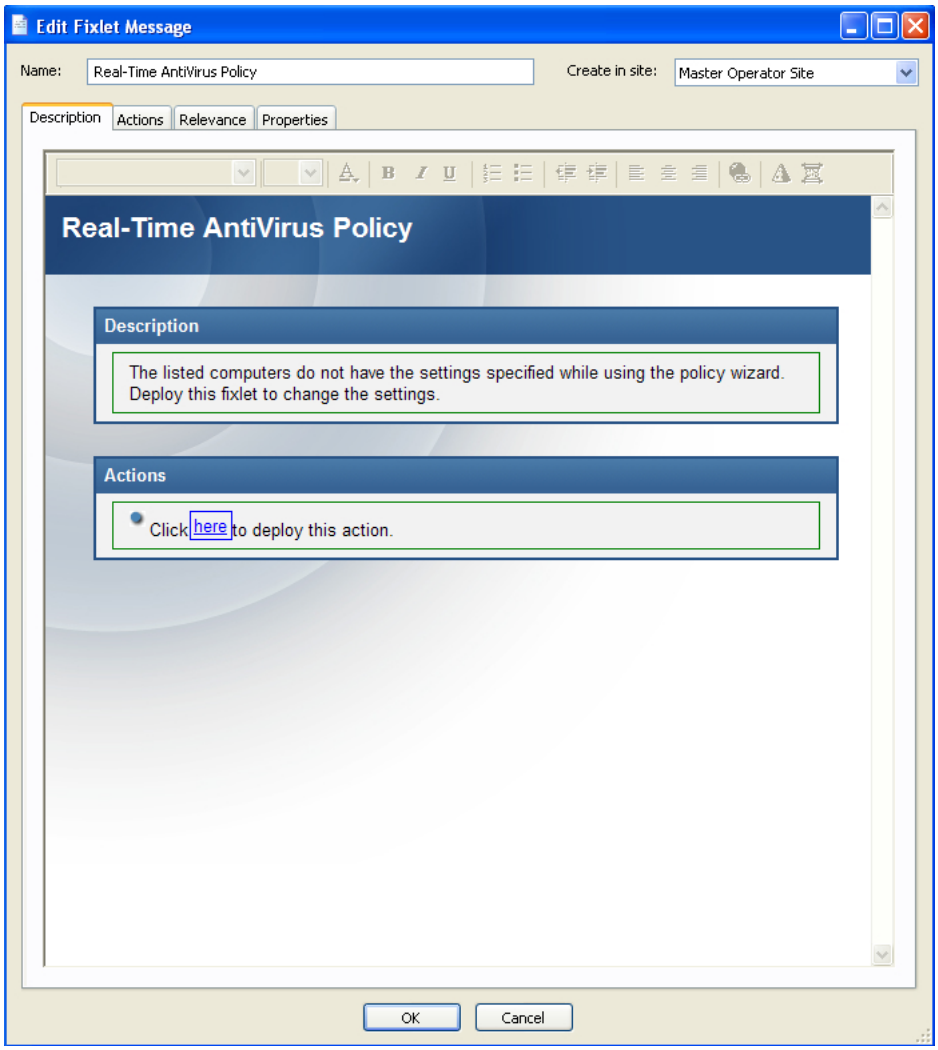


If you choose to quarantine users, any user who accesses or copies an infected object will be denied further access for the specified time.

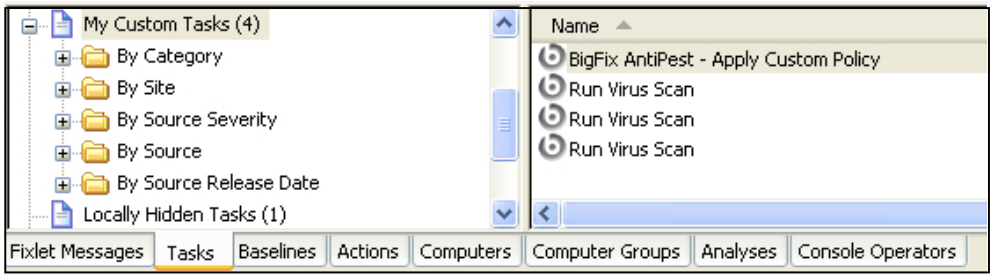
12. Check the box at the bottom of the wizard if you want to create a one-time action.
13. Click **Finish**, and then enter your private key password.

If you selected a one-time action, 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.



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.



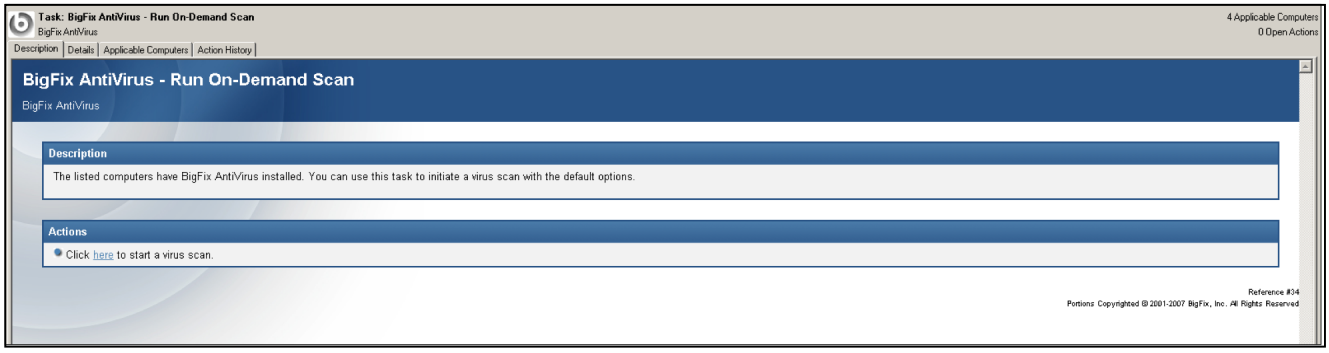
Running an On-Demand Scan

Virus scans can be run on-demand or can be scheduled to run at periodic intervals beginning on a user-specified date and time.

To run an on-demand scan:

1. From the Dashboard, click the **Run an On-Demand Scan** link.

   The **BigFix AntiVirus—Run On-Demand Scan** Task 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 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 Virus Scans

Virus scans can be run 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

Real-time protection is enabled by default. You can toggle real-time protection using tasks linked from the Dashboard.

To disable real-time protection:

1. Click the **Disable Real-Time Monitoring** link under **Additional Tasks**.

   The **BigFix AntiVirus - Disable Real-Time Monitoring** task opens.

2. Click the **here** link 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 disable real-time monitoring.

   b. Set any desired constraints and other options.

c. Click **OK** when you are finished, and then enter your **Private Key Password**.

An Action window opens in which you can track progress.

To enable real-time protection:

1. Click the **Enable Real-Time Monitoring** link under **Additional Tasks**.

   The **BigFix AntiVirus - Enable Real-Time Monitoring** task opens.
2. Click the **here** link 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 enable real-time monitoring.
   b. Set any desired constraints and other options.
   c. Click **OK** when you are finished, and then enter your **Private Key Password**.

   An Action window opens in which you can track progress.

Updating BigFix AntiVirus

BigFix provides a Fixlet to update BigFix AntiVirus.

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

   The **BigFix AntiVirus—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:
   1. Select the computers on which you would like to update BigFix AntiVirus.
   2. Set any desired constraints and other options.
   3. 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.

Frequently Asked Questions

General Questions

Can I get a centralized view and control of my antivirus 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.

Does BigFix AntiVirus use real-time scanning to detect malware?

Yes. BigFix AntiVirus uses real-time scanning to detect and remove viruses. The real-time scanner runs in the background, scanning files as they are executed or read from or written to the disk. Very low endpoint performance impact, and very high client stability and reliability are important considerations when evaluating any anti-malware solution. BigFix AntiVirus detection and remediation technology ensures timely detection and remediation while at the same time delivering high reliability without any impact on the stability of the endpoint operating system.

Does BigFix AntiVirus allow for scheduled / on-demand scans?

Yes. BigFix AntiVirus provides for flexible scheduling options.

What kinds of virus scanning options are available?

BigFix AntiVirus includes a Configuration Wizard that facilitates configuration of options for on-demand scanning as well for real-time scanning. For on-demand scans, the wizard provides flexibility to scan the boot sector, files and folders, memory, and compressed files/archives. Additionally, administrators can enter file extensions to explicitly scan or exclude.

For real-time scanning, the wizard enables administrators to scan floppy, CD-ROM, and network drives, as well as archives. Administrators can also specify whether the scan should include incoming files, outgoing files, or both, as well as select the action to take when a virus is discovered. Additionally, the wizard allows for the exclusion of user-defined processes, directories, and extensions.

How are definition updates handled?

BigFix publishes definition updates to customers as we receive them. Updated definitions are delivered in the standard form of a BigFix Fixlet message. Administrators are then able to see in real-time the computers requiring the update, enabling them to distribute the definition update using the BigFix platform 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.

You can see a complete list of the viruses BigFix AntiVirus fights here: http://www3.ca.com/securityadvisor/virusinfo/.

How often does BigFix publish definition files?

BigFix typically publishes definition files within the same day we receive them, usually once per weekday.

Can definition updates be controlled / downloaded via 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 AntiVirus deploys definition updates silently in the background without bothering the end-user.

Can the updates be scheduled?

Yes. The 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.

Are automatic definition updates supported?

Yes. BigFix AntiVirus using a customer-installed configuration option can deliver automatic definition updates. BigFix recommends the industry best practice of testing and authorizing individual updates before they are released for security and change management reasons, but automated definition updates are supported.

Use the action regenerator at http://support.bigfix.com/bes/misc/actionregenerator.html to auto-update your virus definitions.

Can BigFix AntiVirus update definitions on mobile or remote computers?

Yes. BigFix AntiVirus 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.

In what environments can BigFix AntiVirus be installed?

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

Does BigFix AntiVirus provide an uninstaller to help remove other antivirus products?

Yes. BigFix provides a library of packaged, tested uninstallers for several other antivirus products.

Can BigFix AntiVirus scan mail servers?

Yes. BigFix AntiVirus has virus detection and removal capabilities for Microsoft Exchange and Lotus Notes/Domino environments.

Does BigFix AntiVirus support multi-site, cross-domain deployment?

Yes. The BigFix platform provides multi-site deployment that operates without requiring Active Directory, but can utilize an Active Directory hierarchy already in place. BigFix is typically installed in an enterprise environment spanning geographically distributed sites. The BigFix platform provides various features to make this possible, which include a highly scalable, distributed architecture.

Does BigFix AntiVirus 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 points for new virus definitions and other update files. BigFix is capable of automatically finding the closest available relay for communication and load balancing. Fail-over to alternate relays is automatic and highly configurable.

Does BigFix AntiVirus offer bandwidth controls?

Yes. The BigFix AntiVirus product uses all of the capabilities of the BigFix platform, which includes use of "relays" to reduce overall bandwidth requirements on the WAN and sophisticated policy-based bandwidth limitation options for slow connections.

Can BigFix AntiVirus help with managing a zero-day attack?

Yes. The BigFix Platform provides real-time visibility of the endpoints, and full control of endpoint configuration, which can be used to rapidly mitigate a zero-day threat. For example, the BigFix Platform can aid in turning off a particular affected service, deregistering a library from the operating system, or deleting vulnerable files on managed computers, thereby preventing exploitation by a zero-day attack.

BigFix can also assist in identifying the impact of brand new viruses that have infected your network by allowing you to rapidly query all computers for the existence of relevant processes, registry keys, or files that appear to be related to the new virus. With this ability to detect and remove brand-new viruses within minutes across your organization, you can fill the time gap between when a new virus is released and when definitions (which can be deployed in minutes) are released.

What type of antivirus configuration reporting does BigFix AntiVirus provide?

BigFix AntiVirus leverages the reporting capabilities of the BigFix platform to deliver visibility into the antivirus efforts of the enterprise. Reports are available in the Administrative Console application, as well as a

Web-based reporting environment. Data elements are reported for both the installed antivirus client and for detected viruses. A partial list of reported data elements includes:

- BigFix AntiVirus Engine Version
- BigFix AntiVirus Install Date
- First Scan
- Number of Files Scanned
- Number of Scans
- Number of Infected Files Found
- Virus Definition Version
- Real-Time Scanner Status
- Last Scan
- Number of Files With Errors Scanning
- Number of Viruses Found

Reporting

Can I export report data?

Yes, data can be exported via the Web Report interface in CSV format. Alternately, BigFix also provides a BigFix 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 AntiVirus provide a dashboard view containing high-level statistics?

Yes. BigFix AntiVirus provides a dashboard view with overview statistics and charts that enable administrators to gauge the current health of the system and to track progress as BigFix AntiVirus enforces antivirus compliance and pushes updates throughout the network.

Acknowledgements and Notices

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

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

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

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

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

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

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

ACKNOWLEDGEMENTS AND NOTICES

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

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.

ACKNOWLEDGEMENTS AND NOTICES

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; University of Minnesota, 1300 South Second Street; Minneapolis, MN 55454, USA

ACKNOWLEDGEMENTS AND NOTICES

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.

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**