BigFix® Data Leak Prevention Deployment Guide

BigFix, Inc.
Emeryville, CA

Last Modified: 8/13/2008
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 Data Leak Prevention (DLP). 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 parts:

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

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 Data Leak Prevention, Version 2.0 and later.

Introduction

BigFix Data Leak Prevention (DLP) stops data leaks at the source before they can get on the network and ruin your organization's reputation. This site follows the BigFix distributed real-time visibility and control architecture by installing fast, flexible and effective data-leak prevention on all your managed clients, allowing you to manage it all through the BigFix Console.

Highlights:

- Stops data leaks at their source including data transfers to local ports and storage.
- Recognizes over 300 file types including email, office documents, graphics files, and engineering content in native, compressed, or archived formats.
- Highly customizable & fine-grained policy-based framework.
- Supports multiple compliance standards.
- Real-Time execution and reporting.
  - Logging and audit, violation alerting, full lockdown.
  - Non-intrusive, lightweight operation.
- Active only during data transfer events.
- Intelligent Matching/Detection Engine.
  - Entity/Regex, Keyword, File Metadata.
  - Policies and Signatures Supported.
- Complete mobile, branch office, corporate data-leak prevention.
- Superior, highly accurate leak protection—fewest false positives.
- Enterprise-grade to support minimal network impact with central management.
- Supports compliance efforts—reporting, inventory and forensics.
- Integrated with BigFix's Convergent Management Platform:
  - Pervasive real-time visibility and control.
  - Single console, single agent management.
  - Massively scalable architecture.
- Easy deployment and management.

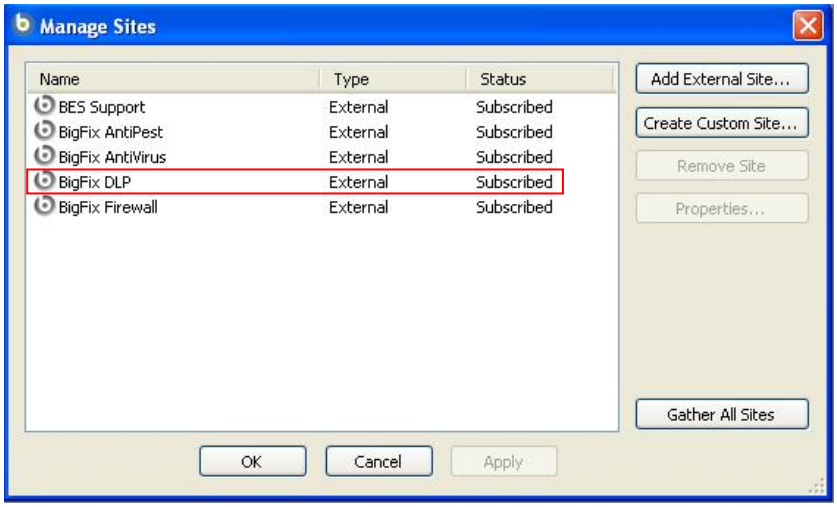
Quick-Start

This procedure assumes that you already have installed BigFix.

1. Obtain a masthead for the BigFix DLP site. Email licensing@bigfix.com to request the masthead. Refer to the ***Console Operators Guide*** for more information about mastheads.
2. Add the BigFix DLP site:
   a. Double-click on the masthead file.
   b. A dialog box appears, asking if you want to proceed with adding the site. Click **Yes**.
   c. Enter your Private Key Password and click **OK**.

At this point, the BigFix DLP site will begin the gathering process, in which Fixlet messages, Tasks, Analyses, Wizards and Dashboards are gathered from the central BigFix server. When the gathering process is complete, the status will change to **Subscribed**.

The DLP site will show as **Subscribed** in the **Manage Sites** dialog. You will also see a new BigFix DLP entry in the **Dashboards** menu and links to DLP Wizards in the **Wizards** menu.



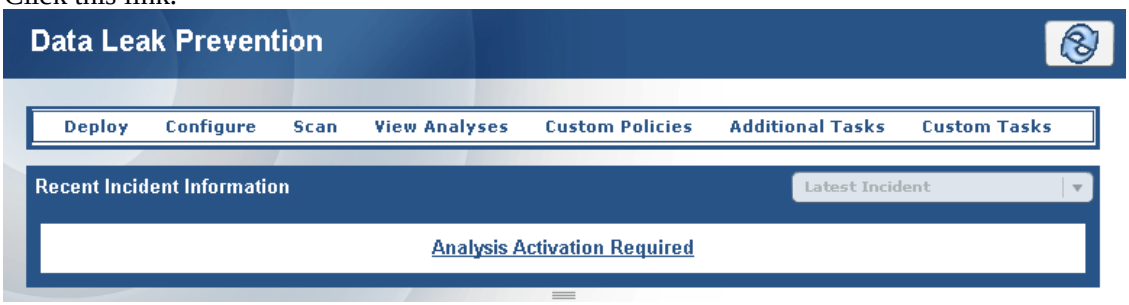
Using the BigFix DLP Dashboard

BigFix DLP provides a dashboard view with overview statistics and charts that enable you to gauge the current status of your system and to track statistics as BigFix DLP enforces data-leak prevention policies throughout your network. In addition, you can use the Dashboard as a central point to manage important tasks such as deployment, analysis and configuration. To open the Dashboard, select **Dashboards > Data Leak Prevention**.

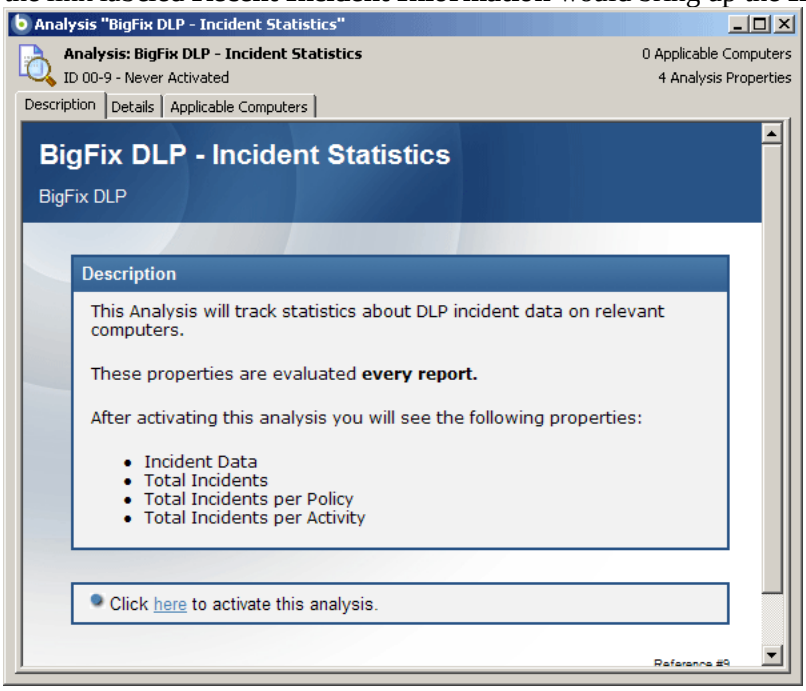
Activating the Dashboard Analyses

To activate the Dashboard, follow these steps:

1. When the Dashboard first appears, you will see a link at the top labeled **Analysis Activation Required**. Click this link.



1. Depending on the screen panel, an Analysis dialog pops up. For instance, in the screen above, clicking the link labeled **Recent Incident Information** would bring up the **Incident Statistics Analysis**:

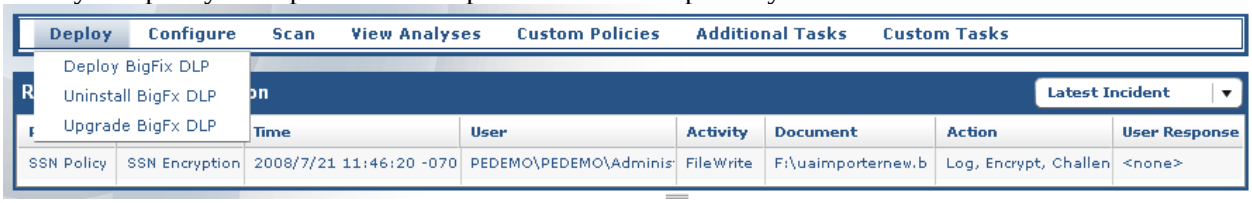


Click the link to activate the analysis. There are several panels, and each one must be activated to view the corresponding analysis.

Understanding the BigFix DLP Dashboard Controls

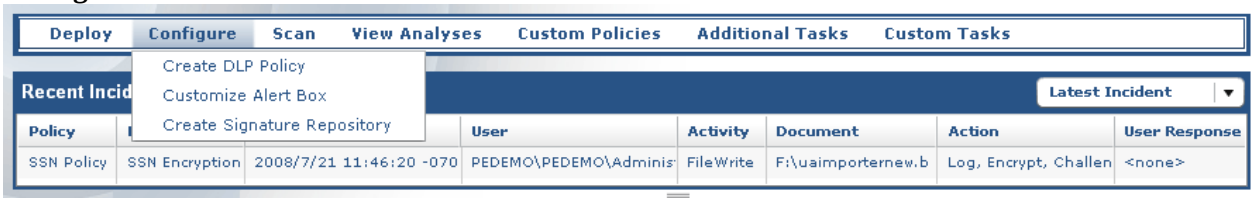
At the top of the Dashboard, you see the BigFix DLP Menu. The controls that BigFix DLP provides are:

- **Deploy** – Use these links to deploy, uninstall or upgrade DLP. Each computer with a DLP agent must have exactly one policy. Computers without policies will not report any DLP data.

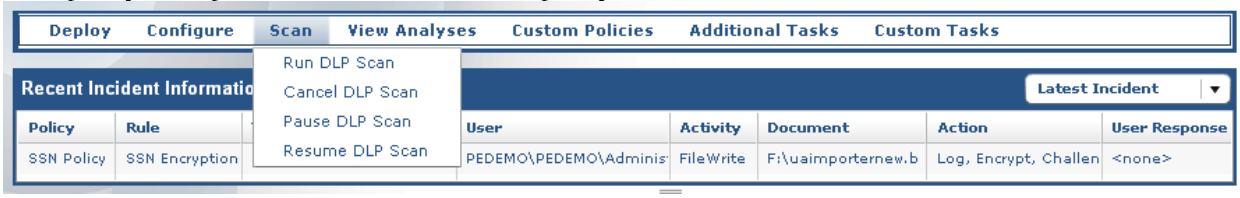


  - Deploy BigFix DLP
  - Uninstall BigFix DLP
  - Upgrade BigFix DLP

- **Configure**

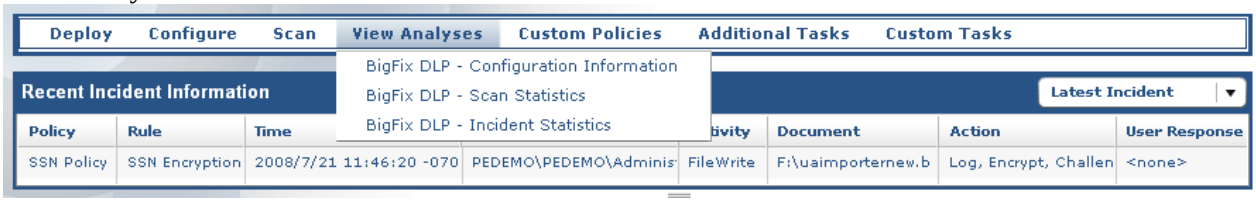


  - Create DLP Policy – This link brings up the BigFix DLP: **Policy and Rule Management Center**.
  - Customize Alert Box – This link brings up the BigFix DLP Alert Box Customization Wizard.
  - Create Signature Repository – This link brings up the Signature Generation Tool that provides information on how to fingerprint documents and maintain a signature repository.
    (For more information about creating a signature repository, see the knowledge-base article at: http://support.bigfix.com/cgi-bin/kbdirect.pl?id=489)
  - **Scan** – Use scans to search for sensitive documents. Sensitive documents are defined by your current DLP policy. Computers must have a set DLP policy in order to run a DLP scan.



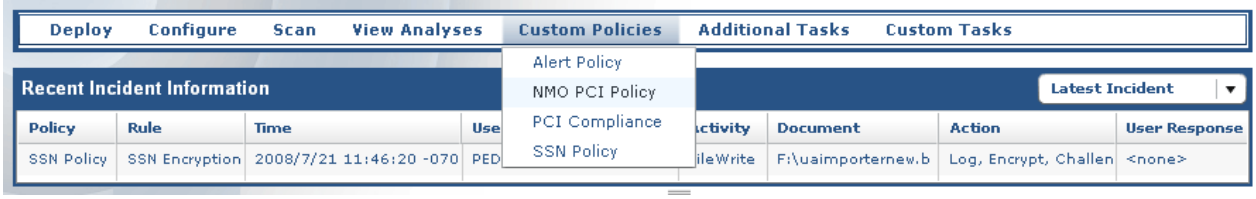
  - Run DLP Scan
  - Cancel DLP Scan
  - Pause DLP Scan
  - Resume DLP Scan

- **View Analyses** – Analyses enable you to view configuration information as well as incident and scan data. These analyses are marked if activated.

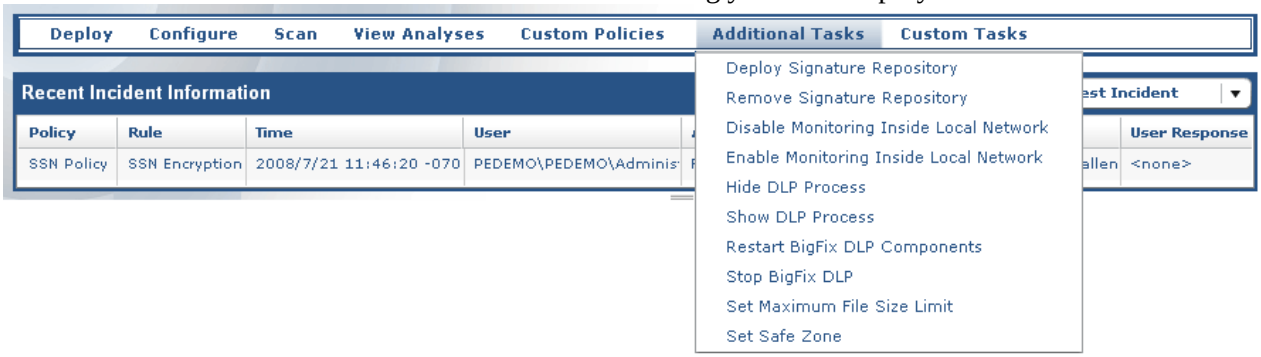


  - BigFix DLP - Configuration Information
  - BigFix DLP - Scan Statistics
  - BigFix DLP - Incident Statistics

- **Custom Policies** –This section lists any custom policies you have created.



- **Additional Tasks** – These tasks are used for troubleshooting your DLP deployment.



  - Deploy Signature Repository (For more information about deploying a signature repository, see the knowledge-base article at: http://support.bigfix.com/cgi-bin/kbdirect.pl?id=490)
  - Remove Signature Repository
  - Disable Monitoring Inside Local Network
  - Enable Monitoring Inside Local Network
  - Hide DLP Process
  - Show DLP Process
  - Restart BigFix DLP Components
  - Stop BigFix DLP
  - Set Maximum File Size Limit
  - Set Safe Zone

- **Custom Tasks**—This section lists any alert box customization or signature deployment tasks you may have created.

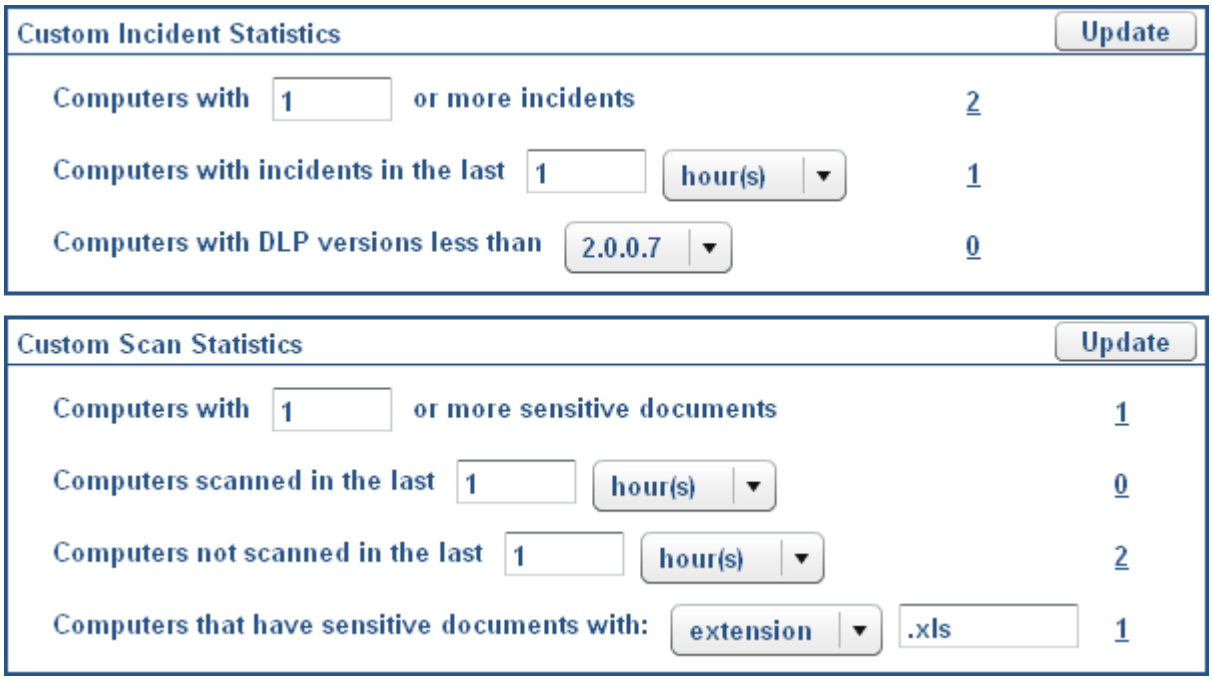
Reading the Dashboard's Overview Statistics and Charts

Below the controls, you see reports on your deployment of BigFix DLP in chart and text format. Note that these charts are clickable to expose more details.

BigFix DLP provides charts or graphs displaying:

- **Recent Incident Information**
  - Policy
  - Rule
  - Time
  - User
  - Activity
  - Document

  - Action
  - User Response
- **Incidents By Activity**—Bar Chart
- **Incidents By Policy**—Bar Chart
- **Overall DLP Agent Status**—Pie Chart
- **Policy Distribution**—Pie Chart



The dashboard also provides charts presenting the following statistics:

- **Custom Incident Statistics**
  - Computers with <*number*> or more incidents <*number*>
  - Computers with incidents in the last <*hour(s)/day(s)/week(s)*> <*number*>
  - Computers with DLP versions less than <*version*>
- **Custom Scan Statistics**
  - Computers with <*number*> or more sensitive documents
  - Computers scanned/not scanned in the last <*hour(s)/day(s)/week(s)*>
  - Computers that have sensitive documents with: <*extension/filename*> <*extension or filename*> <*number*>

Working with BigFix DLP

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

Deploying BigFix DLP

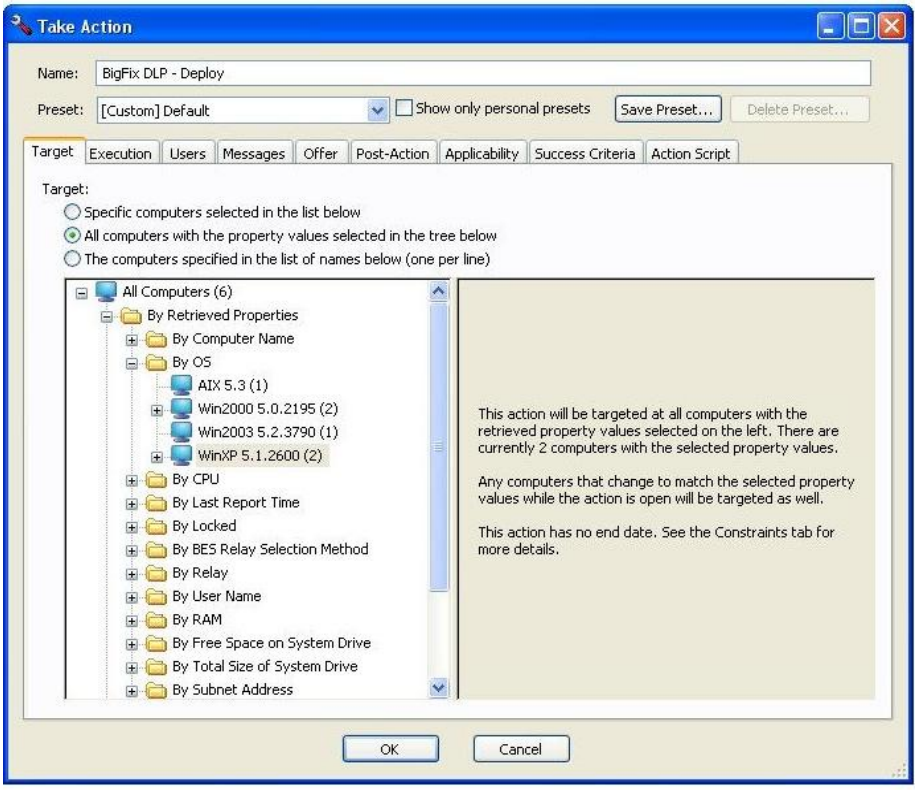
This section contains instructions for deploying BigFix DLP.

To deploy BigFix DLP:

1. From the Dashboard, click the Deploy BigFix DLP link. The **BigFix DLP - Deploy** Task opens.

2. Click the click here link located in the Description section to accept the extension license. Additional links will appear 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 deploy BigFix DLP.
   b. Set any desired options such as for scheduling, messages to users, etc.
   c. For more information about setting options using the tabs in the Take Action dialog box, consult the ***BigFix Console Operators Guide***.
   d. Click **OK** when you are finished.
4. Enter your **Private Key Password** to continue. An Action window appears, in which you can track the progress of your deployment. When it is finished, the status will show "Pending Restart."

Status	Count	Percentage
Pending Restart	1	100.00%

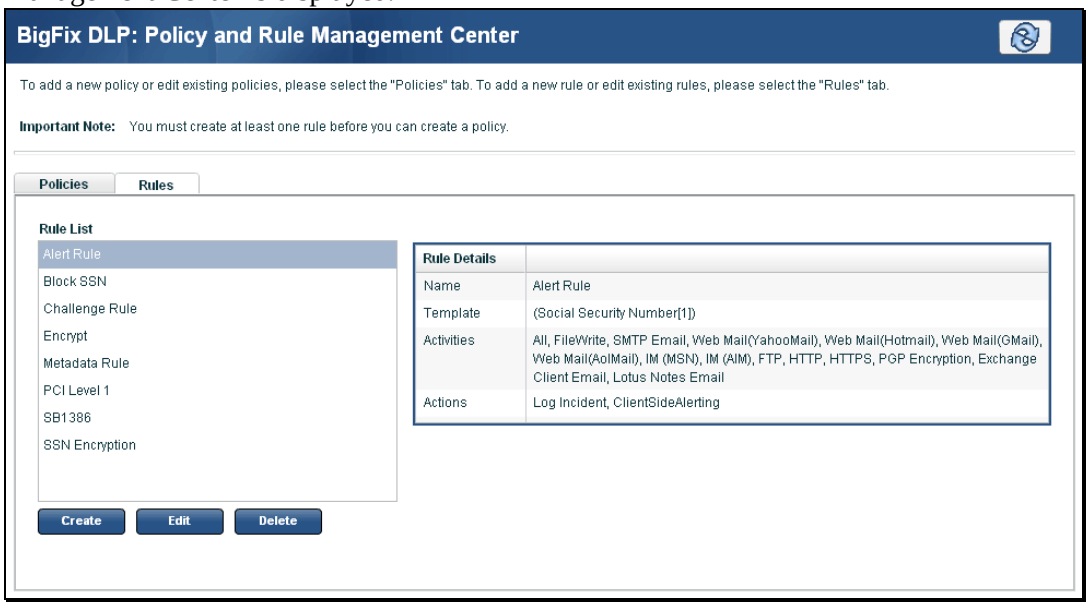
5. Restart the client computers using the BigFix Console.

Creating DLP Policies Using the Wizard

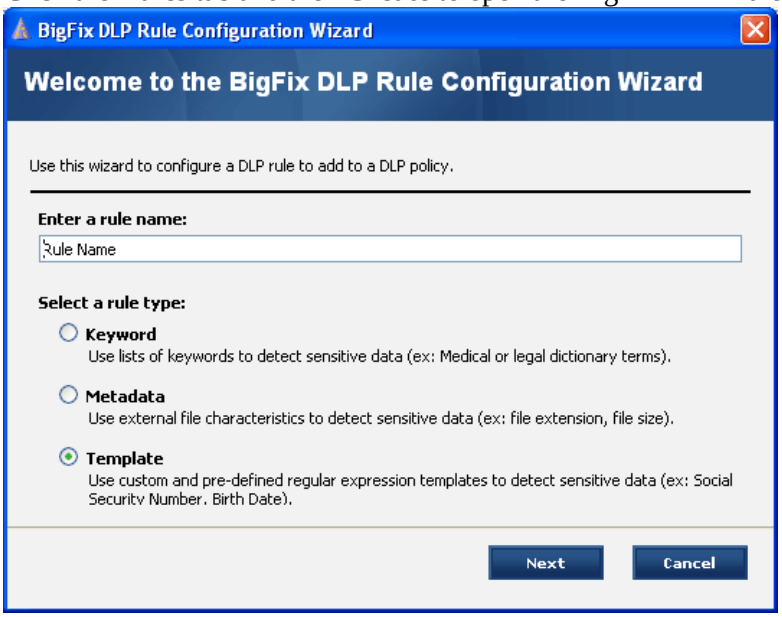
This section demonstrates how to set data-leak prevention policies using the BigFix DLP Policy and Rule Management Center

Creating and Deploying Template-Based Policies

1. From the Dashboard, click the **Create DLP Policy** link from the **Configure** menu. The Policy and Rule Management Center is displayed.

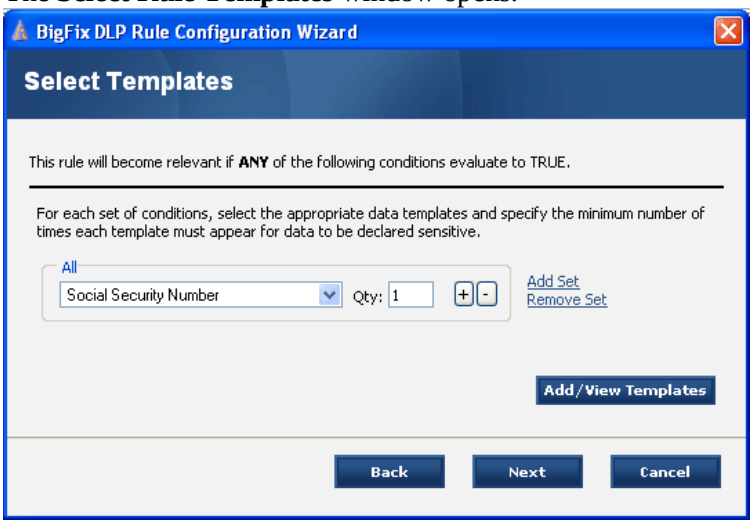


2. Click the **Rules** tab and then **Create** to open the BigFix DLP Rule Configuration Wizard.



3. Enter a rule name. To create a template-based rule, select the **Template** option and click the **Next** button.

The **Select Rule Templates** window opens.



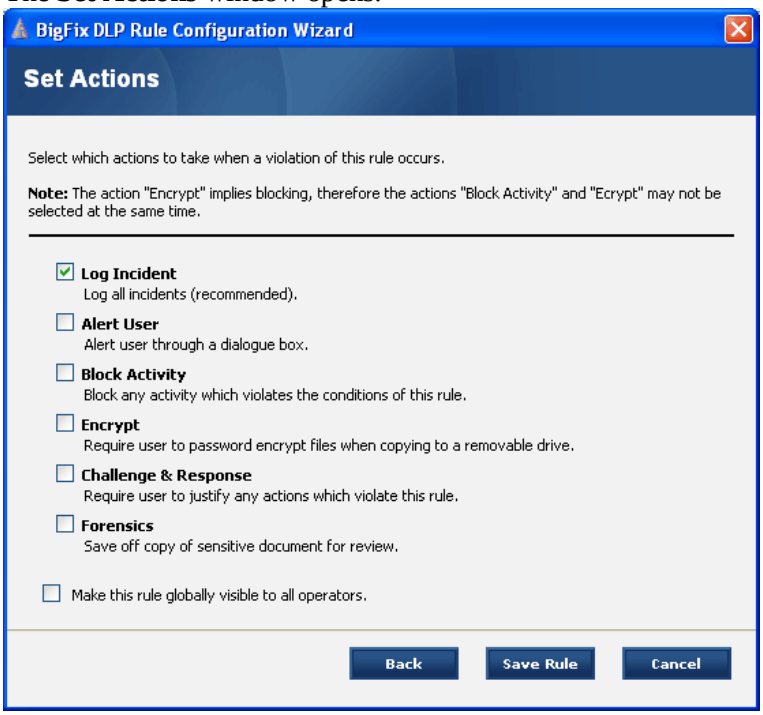
4. To select templates for your rule:
   a. From the drop-down list, select the data template you wish to include.
   b. In the **Qty** box, specify the minimum number of times each template must appear for data to be declared sensitive.
   c. Click **Next**.

NOTE: Each condition must consist of at least one data template and a quantity for that data template. Data templates are used to detect sensitive information such as credit card numbers and social security numbers.

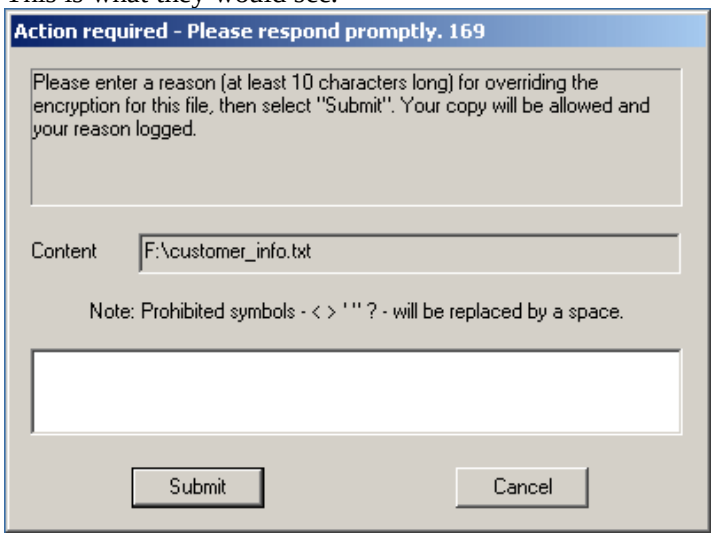
The **Select Activities** window opens.

5. In the **Select Activities** window:
   a. Select the activities you would like to monitor for sensitive data transfer.
   b. Click **Next**.

   The **Set Actions** window opens.



6. In the **Set Actions** dialog:
   a. Select the actions you would like the DLP agent to take when a violation occurs.
   b. Check the box labeled **Block Activity** or **Encrypt** if you wish to prompt the user about violations of DLP policy. This will cause a **Challenge and Response** message to appear to the user if they attempt to override encryption, asking them to provide a reason for overriding the file encryption. This is what they would see.



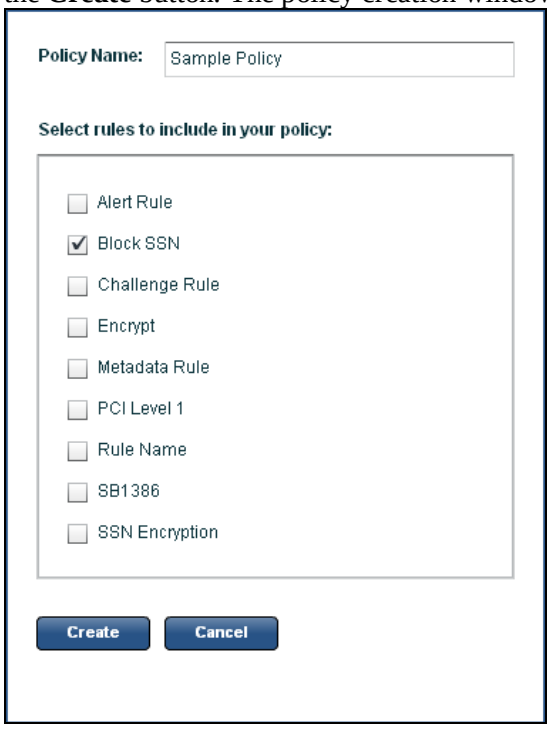
c. Finally, check the box labeled **Make this rule globally visible to all operators** if you would like the rule to be available to other BigFix operators. Leave the checkbox unchecked if you would like the rule to be private.

d. Click **Save Rule**. The rule is now saved to the **Policy and Rule Management Center**. Click on the **Rule List** to update the contents.

NOTE: It is recommended that you log incidents without blocking for a period of time to gauge the effectiveness of your rule. Note also that the Encrypt action only applies to USB transfers. If Encrypt is chosen, then user blocking is implied. This means that if users subsequently choose not to encrypt the file, it will be blocked. Encryption is password-based and requires a password length of at least 6 characters. The internal mechanism is Blowfish.

7. Repeat these steps to create additional rules.

8. From the **Policy and Rule Management Center**, click the **Policies** tab. To create a new policy, click the **Create** button. The policy creation window opens.



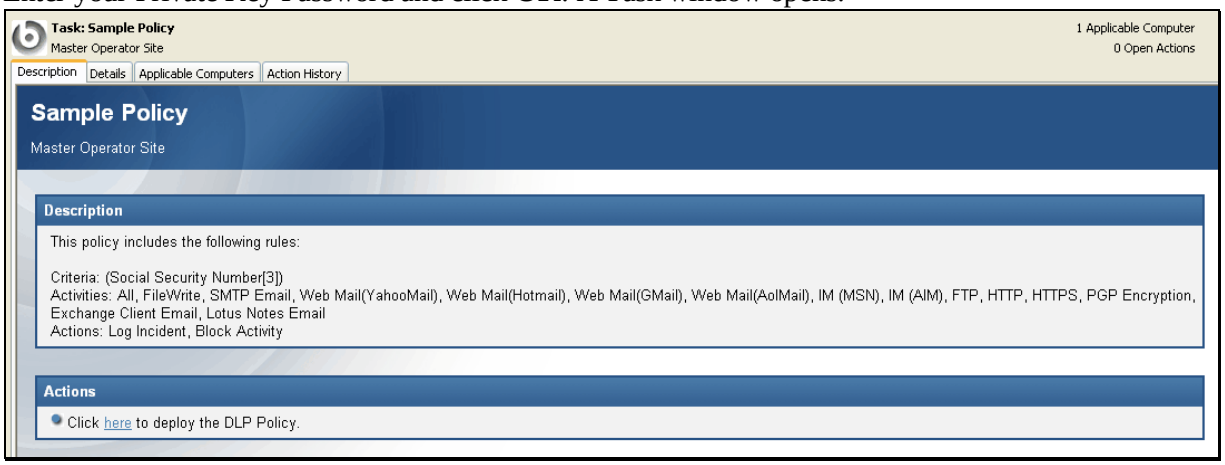
9. To create a DLP Policy:

a. Enter a policy name.

b. Select the rules you would like to include in your policy.

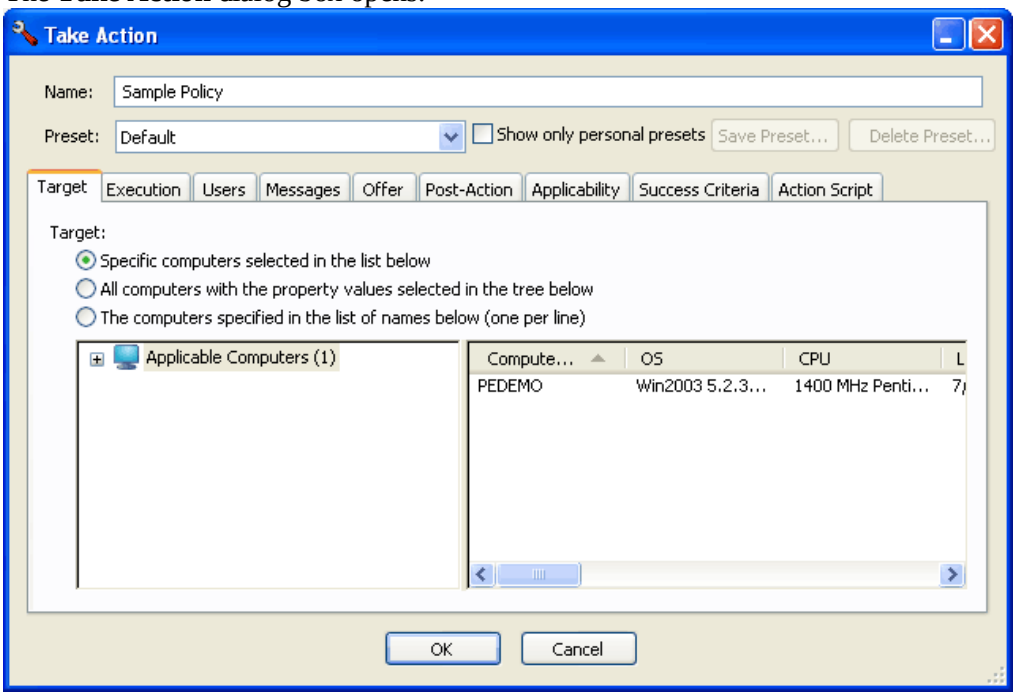
c. Click **Create** to start a custom Task that will deploy your DLP Policy to applicable computers.

10. Enter your Private Key Password and click **OK**. A Task window opens.



11. Click the Action link to **deploy the DLP policy**.

    The **Take Action** dialog box opens.



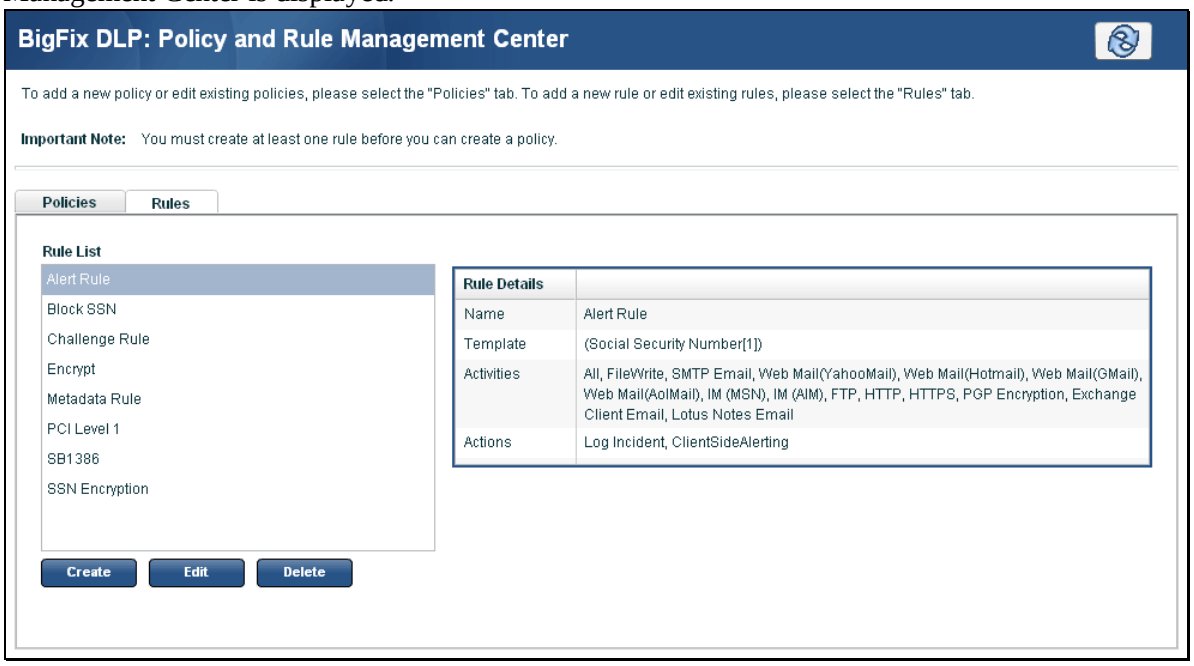
12. In the **Take Action** dialog box:
    a. Select the computer(s) to which you would like to deploy your policy.
    b. Set any desired options such as for scheduling, messages to users, etc.
    c. For more information about setting options using the tabs in the Take Action dialog box, consult the ***BigFix Console Operators Guide***.
    d. Click **OK** when you are finished.
13. Enter your **Private Key Password** to deploy the task.

An Action window will appear, allowing you to track the progress of the deployment.

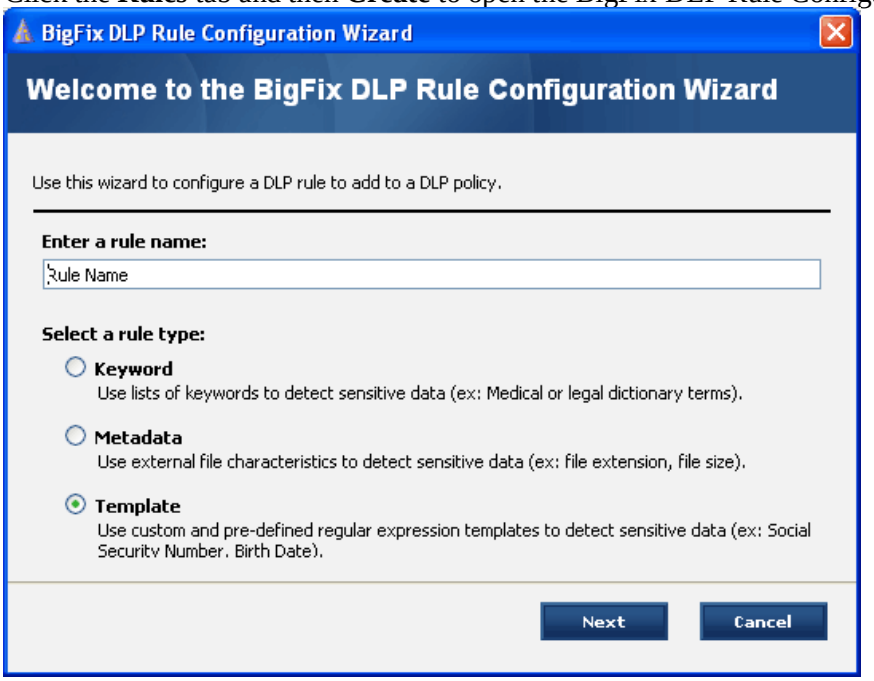
Creating and Deploying Policies with Custom Data Templates

To create a policy that uses a custom data template:

1. From the Dashboard, click the **Create DLP Policy** link from the **Configure** menu. The Policy and Rule Management Center is displayed.

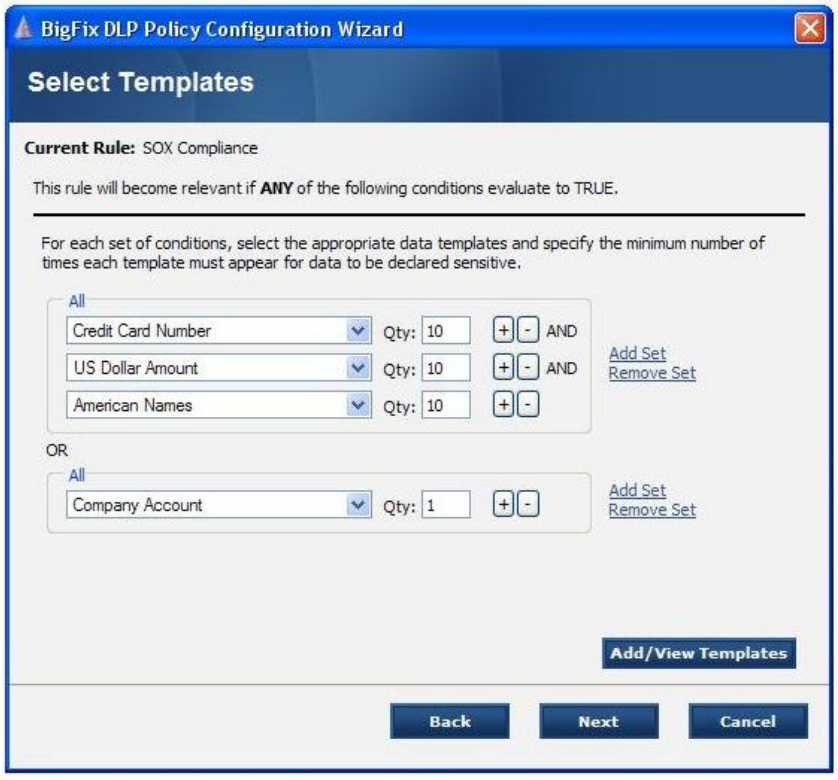


2. Click the **Rules** tab and then **Create** to open the BigFix DLP Rule Configuration Wizard.

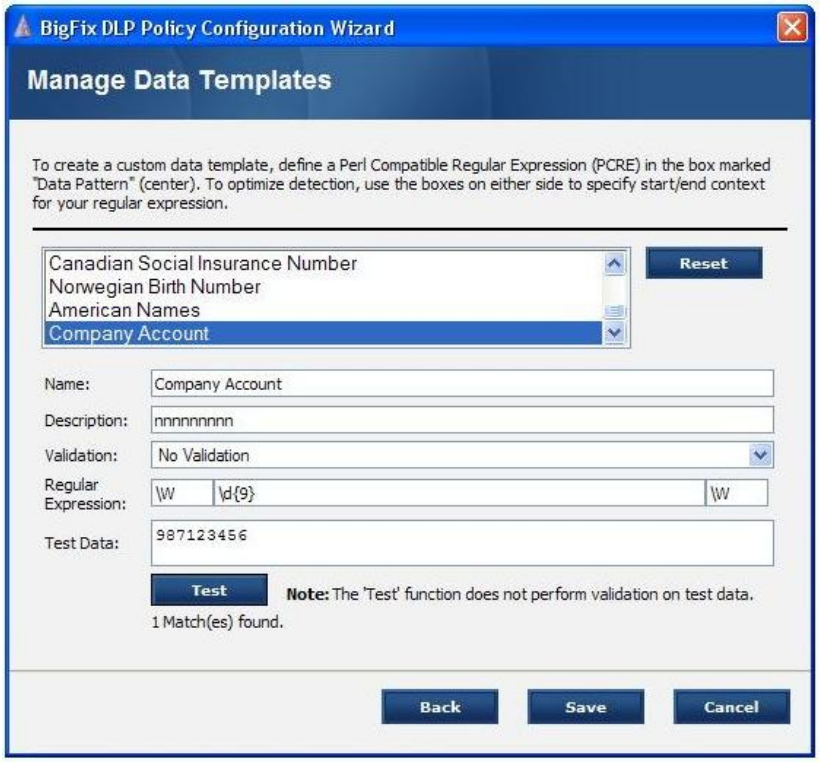


3. Enter a rule name. To create a template-based rule, select the **Template** option and click the **Next** button.

The **Select Templates** window opens.



4. Click the **Add/View Templates** button. The **Manage Data Templates** window opens.



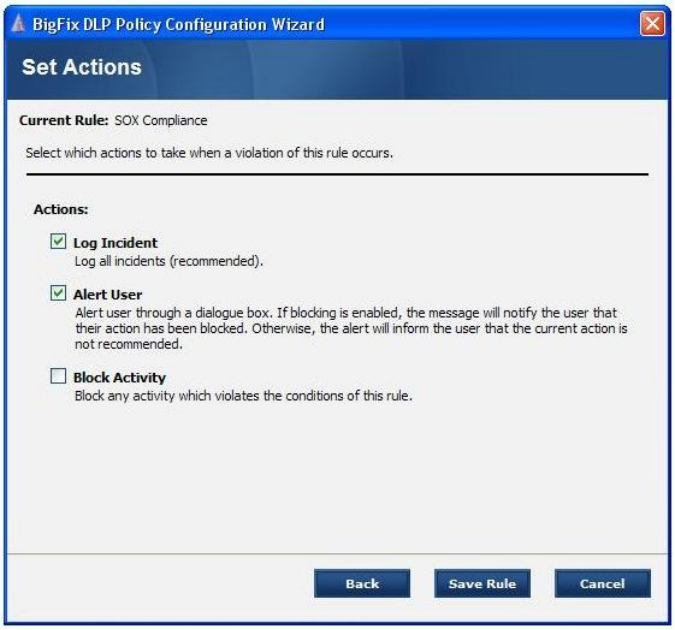
5. In the **Manage Data Templates** window:
   a. Select a criterion from the scroll box.
   b. **Name** your data template, enter a **description**, and select a **Validation** criterion from the drop-down box, or accept the default values.
   c. Enter a Perl-Compatible **Regular Expression** (PCRE) in the Regular Expression box.
   d. Enter some **test data** and click the **Test** button.
   e. After you are satisfied, click **Save**.

   Your custom template will now be available for use in configuring policies.

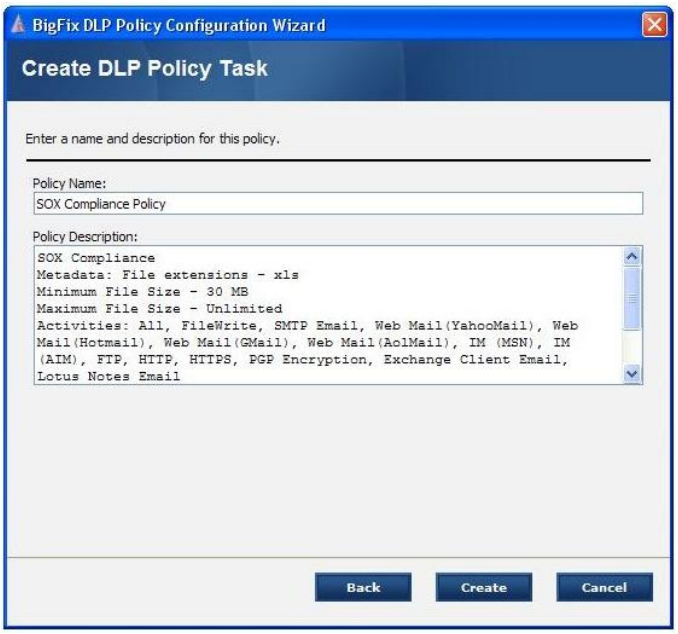
   The **Select Activities** window opens.

6. In the **Select Activities** window:
   a. Select the activities you would like to monitor for sensitive data transfer.
   b. Click **Next**.

The **Set Actions** window opens.

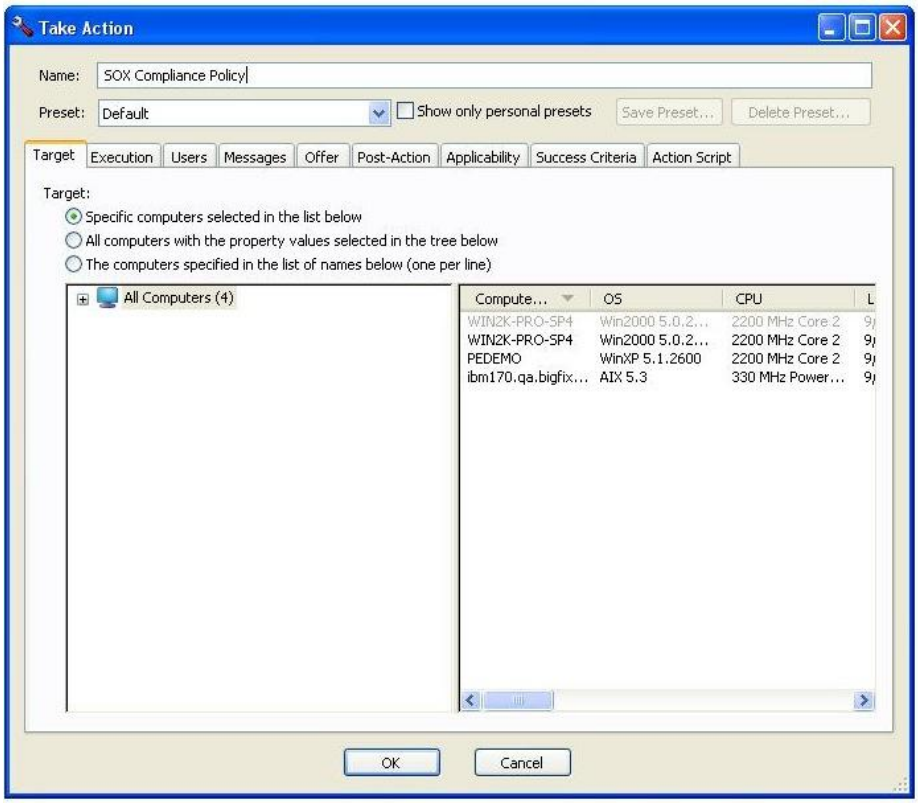


7. Select the actions you would like the DLP agent to take when a violation occurs.
8. **Note**: It is recommended that you log incidents without blocking for a period of time to gauge the effectiveness of your rule.
9. Click **Save Rule**. The **Create DLP Policy Task** window opens.



10. To create a custom Task that can be used to deploy your policy, enter a name for your policy and then click **Create**.
11. Enter your Private Key Password and click **OK**. A Task window opens.

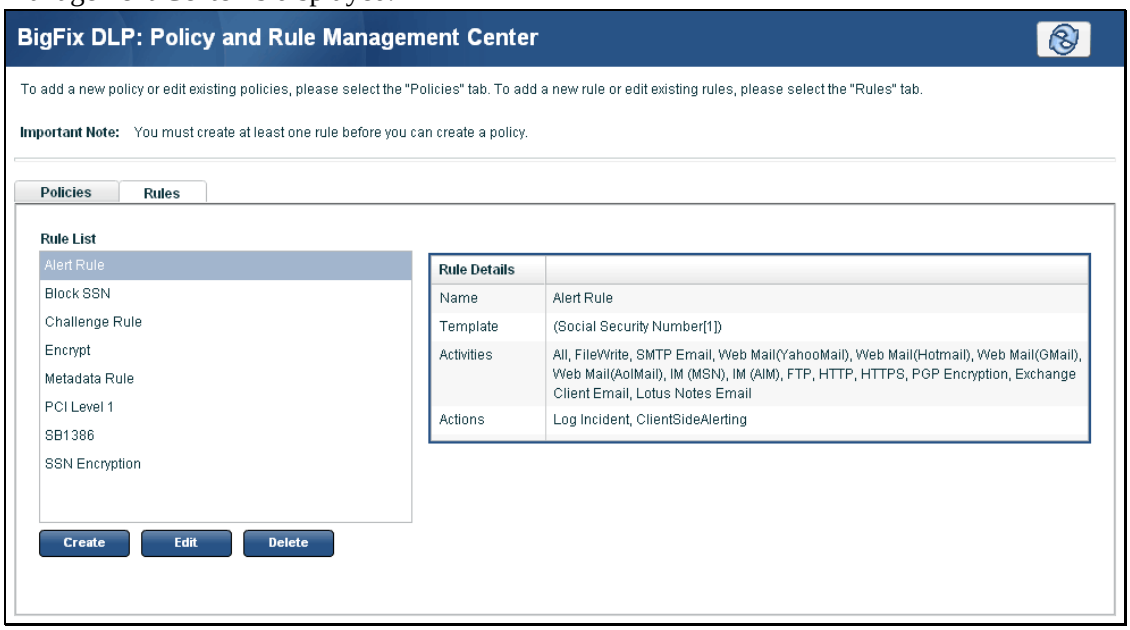
12. Click the Task **Action** link to deploy your DLP policy. The **Take Action** dialog opens.



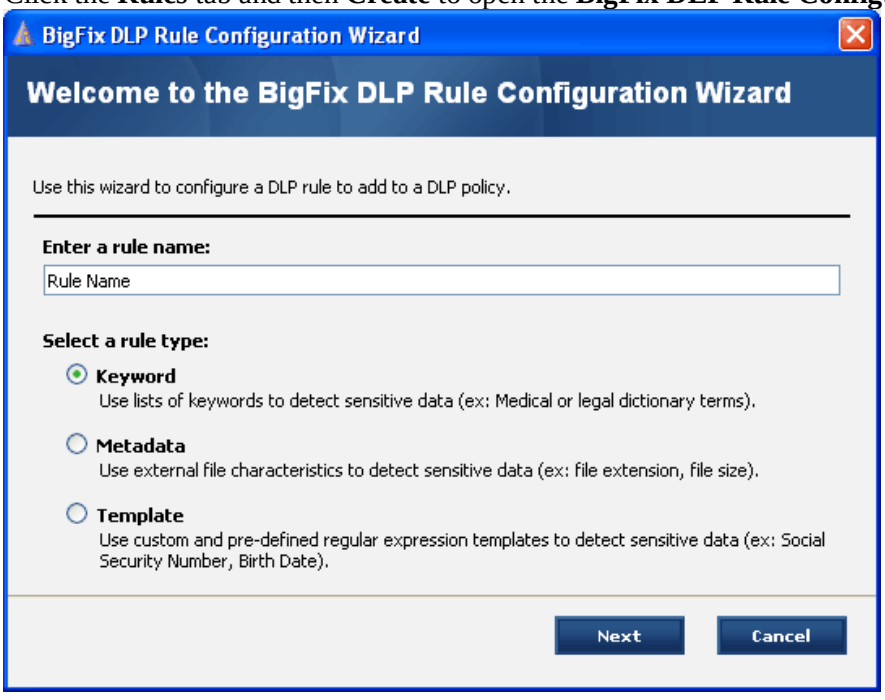
13. In the **Take Action** window:
    a. Select the computer(s) to which you would like to deploy your policy.
    b. Set any desired options such as for scheduling, messages to users, etc.
    c. For more information about setting options using the tabs in the Take Action dialog box, consult the ***BigFix Console Operators Guide***.
    d. Click **OK** when you are finished.
14. Enter your **Private Key Password** to continue.
15. An Action window will appear, allowing you to track the progress.

Creating and Deploying Keyword-Based Policies

1. From the Dashboard, click the **Create DLP Policy** link from the **Configure** menu. The Policy and Rule Management Center is displayed.

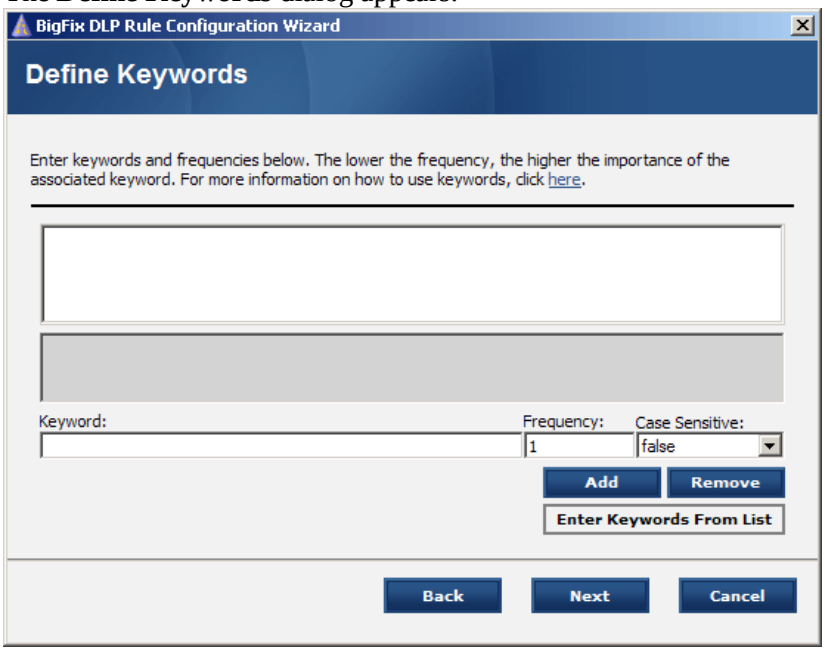


2. Click the **Rules** tab and then **Create** to open the **BigFix DLP Rule Configuration Wizard**.



3. Enter a **rule name**. To create a keyword-based rule, select the **Keyword** option and click the **Next** button.

The **Define Keywords** dialog appears.



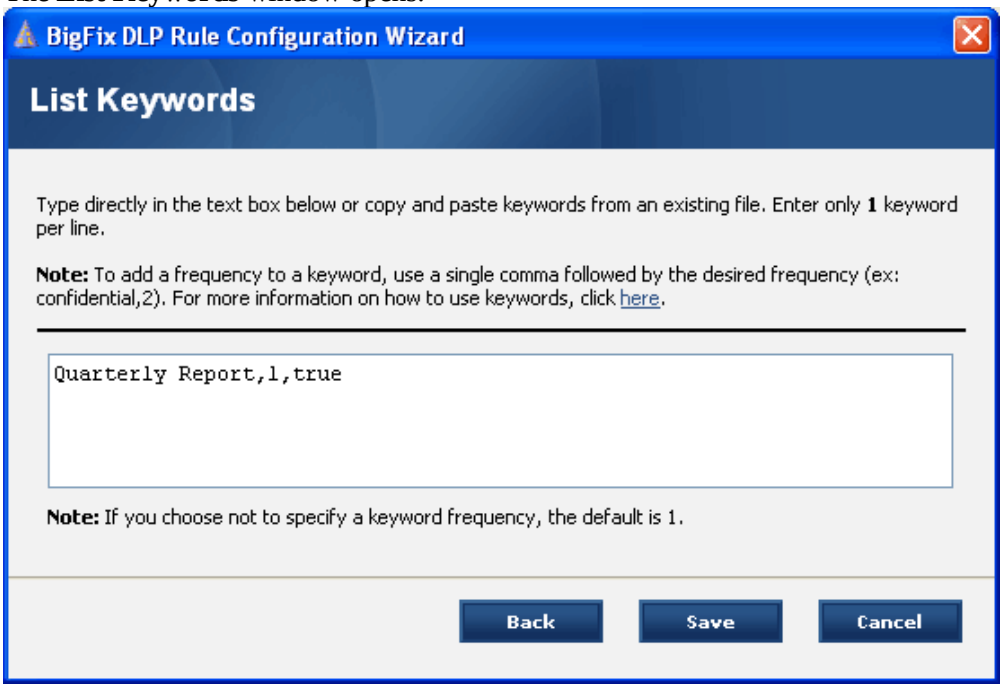
4. To define keywords for your rule:
   a. Type the keyword in the text box labeled **Keyword**.
   b. If desired, specify a **frequency** for the keyword.
   c. If case sensitivity is required, select the **true** option in the case sensitive select box.
   d. Click the **Add** button to add the keyword to the keyword list.

   Scoring information for the keyword will appear in the grey box below the keyword list.

NOTE: Any document with a total score of 100 or more will be considered sensitive. For example, keyword A has a frequency of 2 and a score of 50. This means that a document must contain at least 2 instances of keyword A to be considered sensitive. Keyword B has a frequency of 4 and a score of 25. This means that a document must contain at least 4 instances of keyword B to be considered sensitive. A document containing 1 instance of keyword A and 2 instances of keyword B will also be considered sensitive.

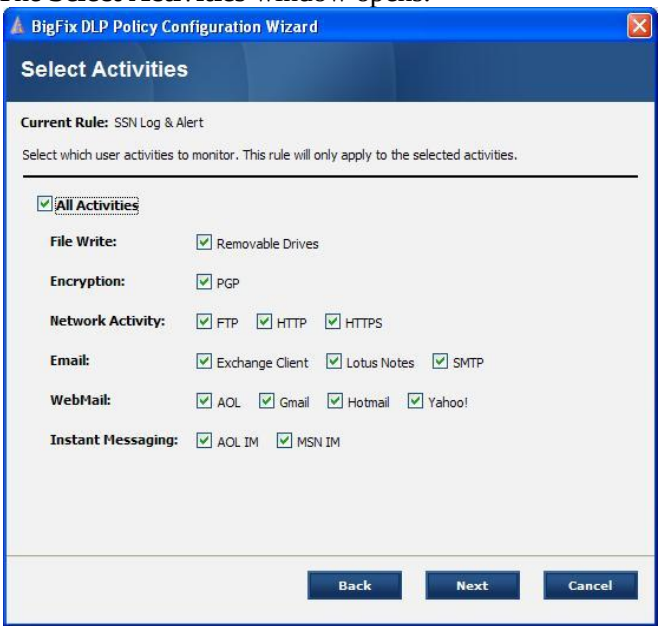
5. To add keywords from an existing list click the **Enter Keywords From List** button.

The **List Keywords** window opens.



6. In the **List Keywords** window:
   a. Copy and paste keywords into the text area box, optionally using a single comma to separate a keyword from its frequency and case sensitivity.
   b. If you choose not to specify a frequency for each keyword, the default frequency will be 1.
   c. If you choose not to specify case sensitivity, the default will be false (not case sensitive).
   d. Click the **Save** button when you are finished.
7. When you are finished defining keywords, click the **Next** button.

The **Select Activities** window opens.



8. In the Select Activities window:
   a. Select the activities you would like to monitor for sensitive data transfer.
   b. Click **Next**.

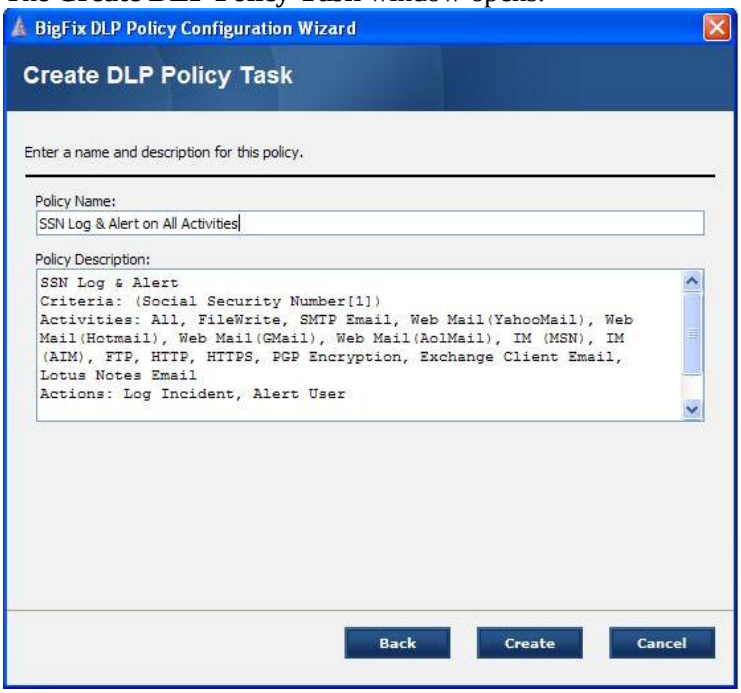
   The **Set Actions** window opens.

9. Select the actions you would like the DLP agent to take when a violation occurs. Click **Save Rule**.

NOTE: It is recommended that you log incidents without blocking for a period of time to gauge the effectiveness of your rule.

10. Repeat the previous steps until you have completed your policy. Click **Finish**.

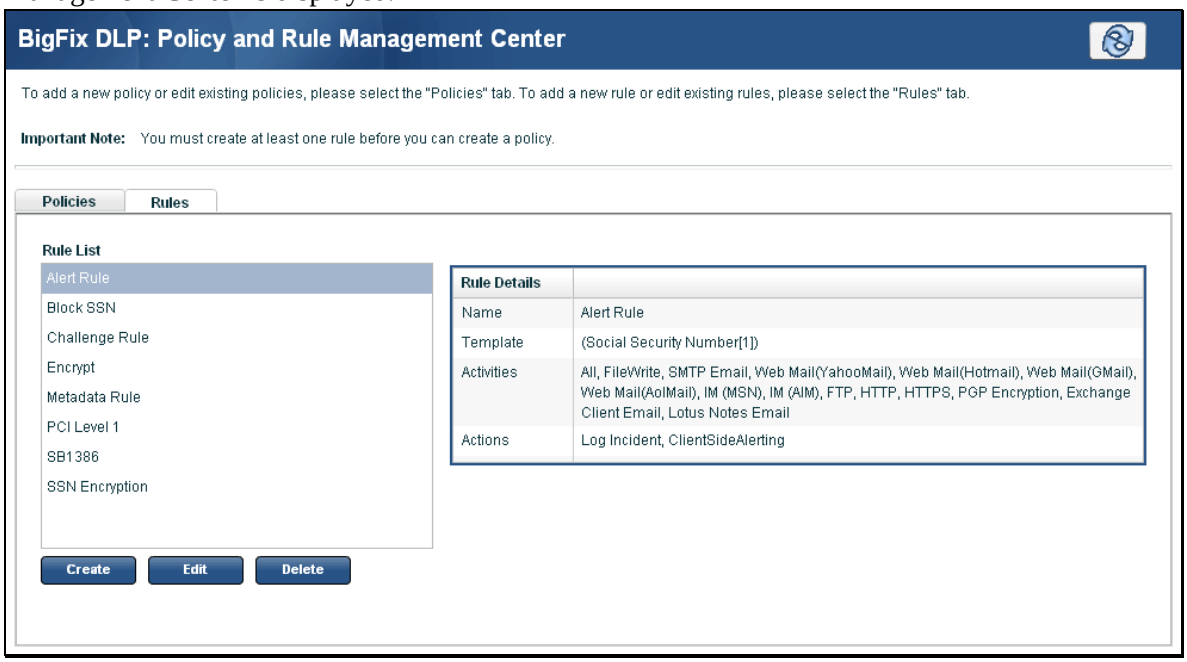
    The **Create DLP Policy Task** window opens.



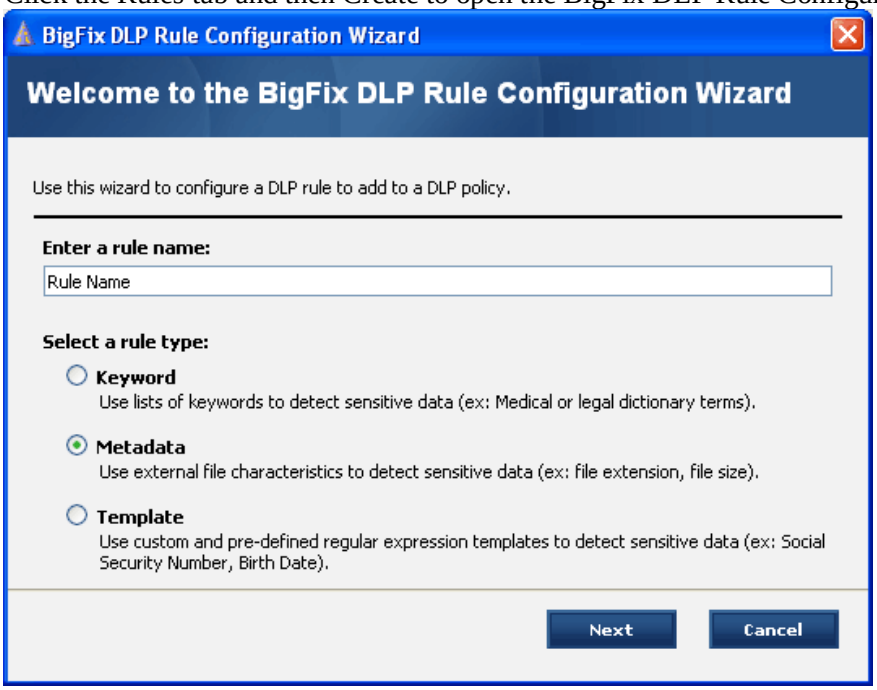
11. To create a custom Task that can be used to deploy your policy, enter a name for your policy and then click **Create**.
12. Enter your **Private Key Password** and click **OK**.
13. A **Task** window opens.
14. Click the **here** link to deploy your DLP policy. The **Take Action** dialog box opens.
15. In the **Take Action** dialog box:
    a. Select the computer(s) to which you would like to deploy your policy.
    b. Set any desired options such as for scheduling, messages to users, etc.
    c. For more information about setting options using the tabs in the Take Action dialog box, consult the ***BigFix Console Operators Guide***.
    d. Click **OK** when you are finished.
16. Enter your **Private Key Password** to continue. An Action window appears, allowing you to track the progress.

Creating and Deploying Metadata-Based Policies

1. From the Dashboard, click the Create DLP Policy link from the Configure menu. The Policy and Rule Management Center is displayed.

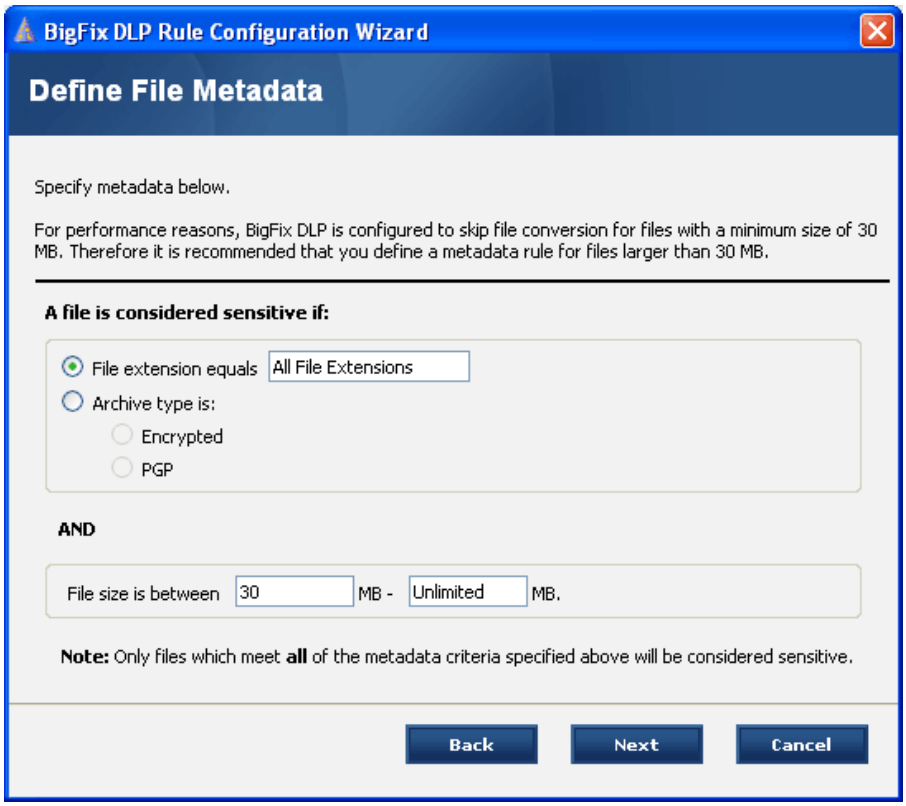


2. Click the Rules tab and then Create to open the BigFix DLP Rule Configuration Wizard.



3. Enter a **rule name**. To create a metadata-based rule, select the **Metadata** option and then click the **Next** button.

The **Define File Metadata** window opens.



1. In the **Define File Metadata** window:
   a. Enter a file extension without the leading period or select an archive type.
   b. Select the **Encrypted** option if you would like to monitor documents such as encrypted .zip or .rar files.
   c. Select the **PGP** option if you would like to monitor PGP encrypted documents.
   d. Enter a minimum and maximum **file size**. To specify an unlimited maximum file size, type **Unlimited** in the maximum file size box.

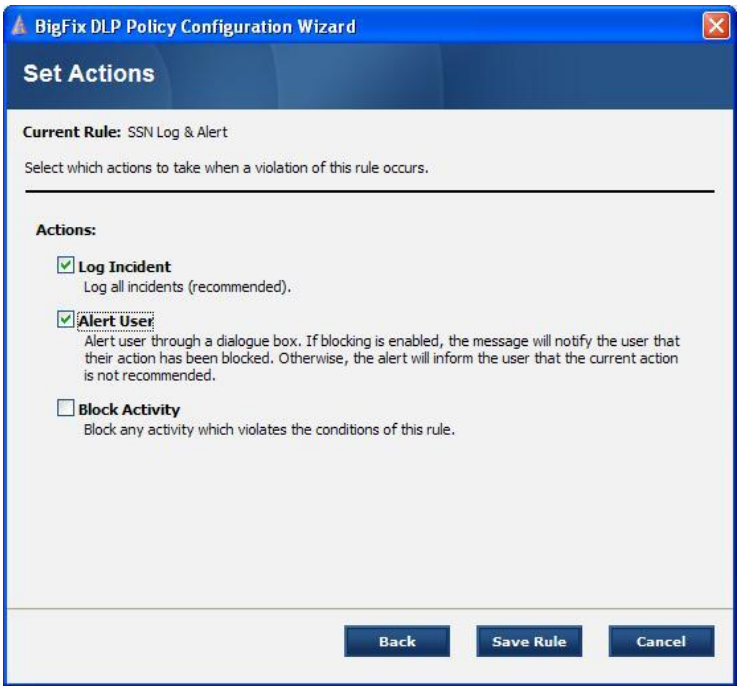
> **NOTE**: For performance reasons, the DLP process is configured to skip file conversion of files larger than 30 MB. Therefore it is recommended that you define at least one file metadata rule for files larger than 30 MB.

   e. When you are finished selecting file metadata, click the **Next** button.

The **Select Activities** window opens.

4. In the Select Activities window:
   a. Select the activities you would like to monitor for sensitive data transfer.
   b. Click Next.

   The **Set Actions** window opens.

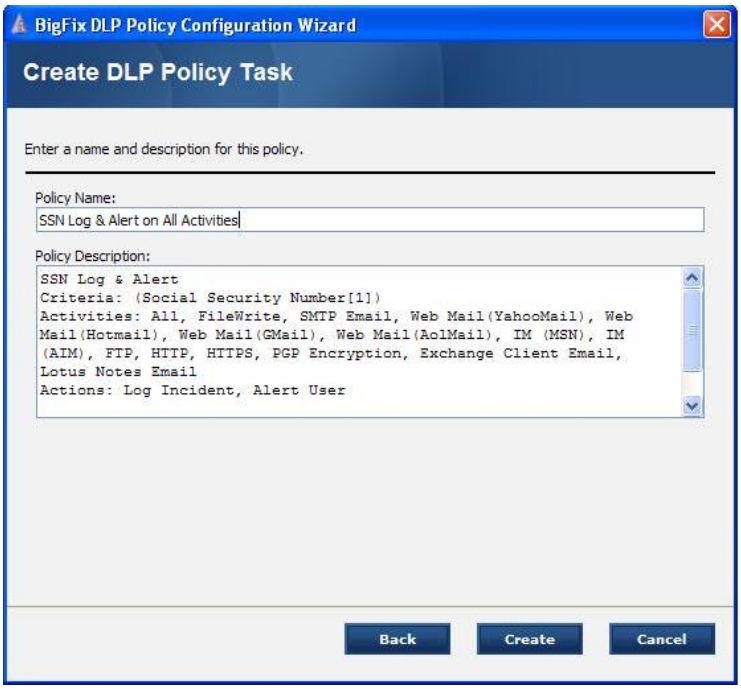


5. Select the actions you would like the DLP agent to take when a violation occurs. Click **Save Rule**.

Note: It is recommended that you log incidents without blocking for a period of time to gauge the effectiveness of your rule.

6. Repeat the previous steps until you have completed your policy. Click Finish.

   The **Create DLP Policy Task** window opens.



7. To create a custom Task that can be used to deploy your policy, enter a name for your policy and then click Create.
8. Enter your Private Key Password and click OK. A Task window opens.
9. Click the here link to deploy your DLP policy. The Take Action dialog box opens.
10. In the Take Action dialog box:
    a. Select the computer(s) to which you would like to deploy your policy.
    b. Set any desired options such as for scheduling, messages to users, etc.
    c. For more information about setting options using the tabs in the Take Action dialog box, consult the ***BigFix Console Operators Guide***.
    d. Click **OK** when you are finished.
11. Enter your **Private Key Password** to continue. An Action window appears, allowing you to track the progress.

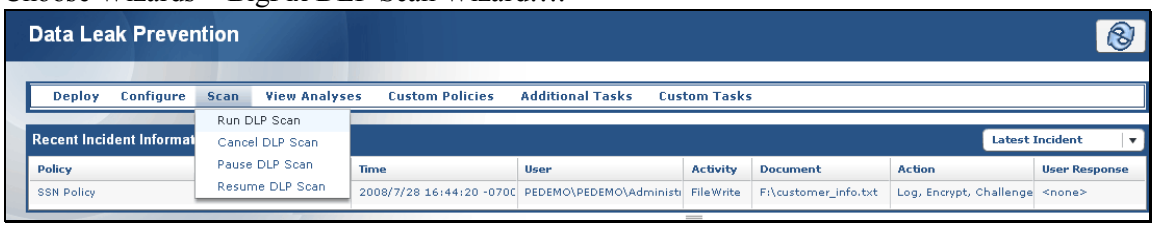
Running Scans

Scanning searches for sensitive files on computers that have the DLP agent installed. Sensitive files are defined by the currently deployed DLP policy. As a result, this task will not be relevant on computers that do not have a set DLP policy.

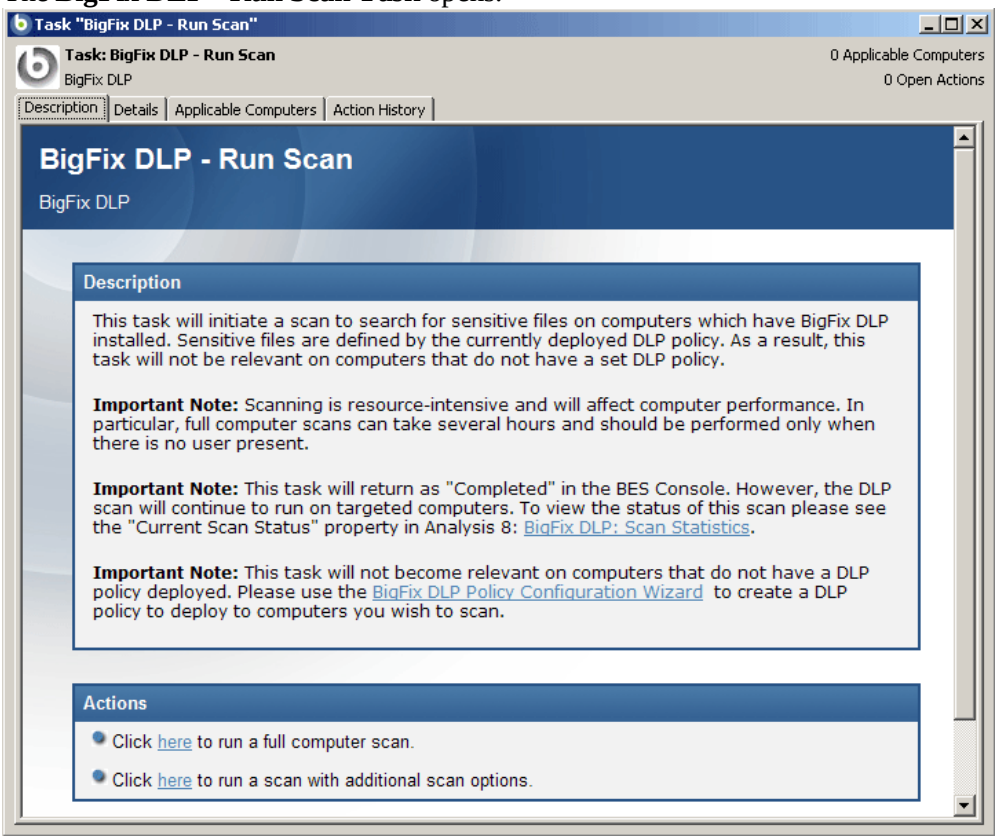
Scanning is resource-intensive and will affect computer performance. In particular, full computer scans can take several hours and should be performed only when there is no user present. The task will return as "Completed" in the BES Console. However, the DLP scan will continue to run on targeted computers. To view the status of this scan please see the "Current Scan Status" property in the DLP Dashboard report.

To run a scan:

1. Choose Wizards > BigFix DLP Scan Wizard….

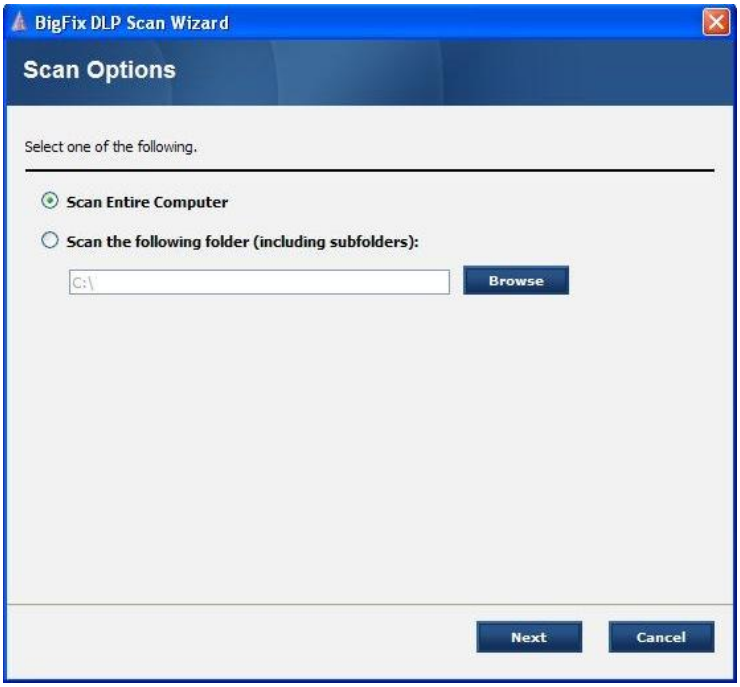


2. The **BigFix DLP - Run Scan Task** opens.

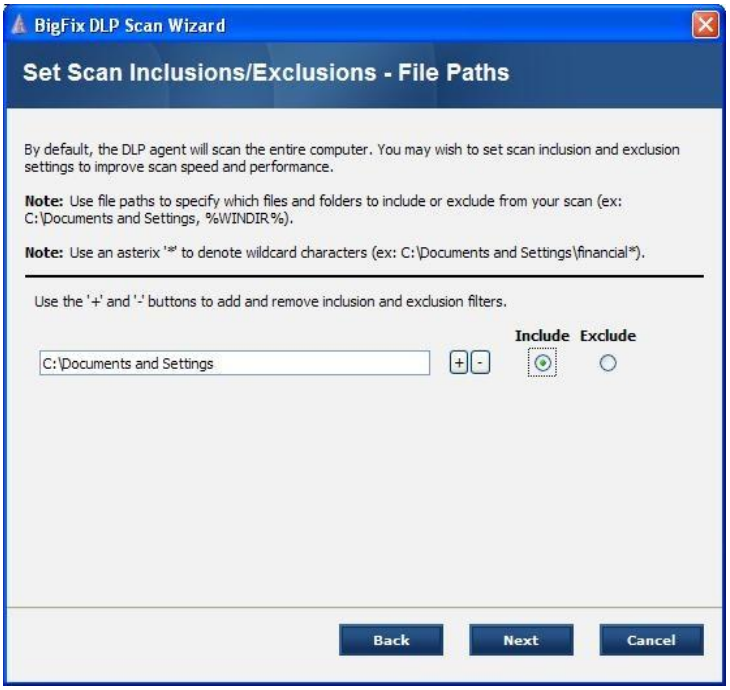


To run a full computer scan, select the first action. To run a customized computer scan, select the second action.

3. The BigFix DLP Scan Wizard opens.

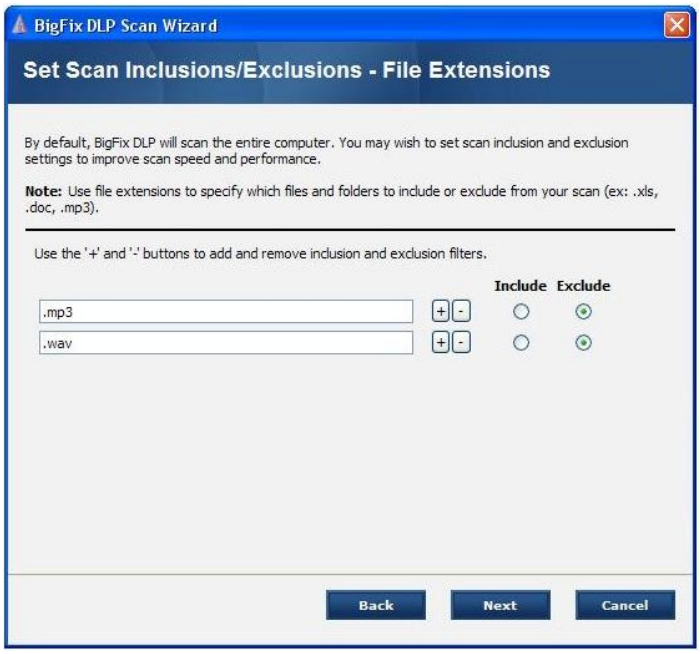


4. Choose whether you want to scan an entire computer or a particular subfolder. Click Next.
5. The **Set Scan Inclusions/Exclusions – File Paths** window opens.



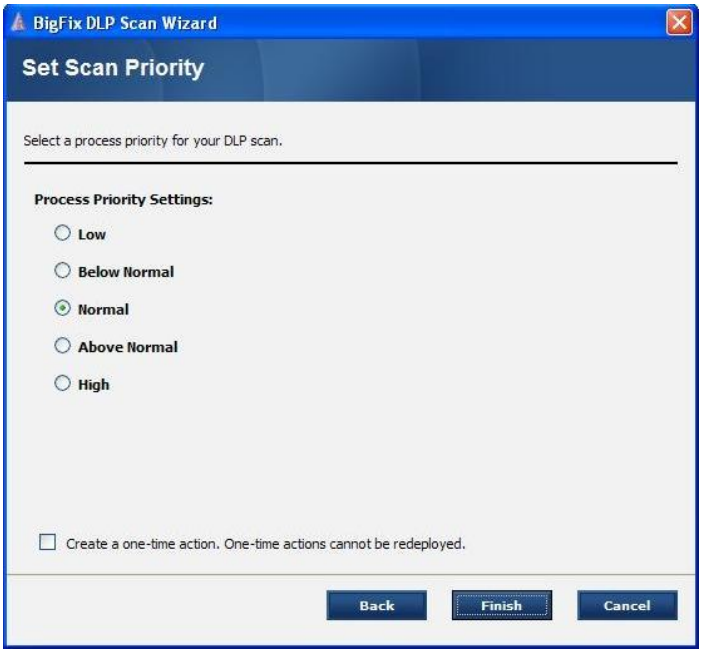
6. Add any filters you want to mark for inclusion or exclusion. Click **Next**.

The **Set Scan Inclusions/Exclusions – File Extensions** window opens.



7. Add filters for inclusion and/or exclusion. Click **Next**.

   The **Set Scan Priority** window opens.



8. In the Set Scan Priority window:
   a. Set the process priority for the DLP scan.
   b. Leave the check box unchecked to create a reusable Task, or check it to create a one-time Action.
   c. Click **Finish**.

9. Enter your Private Key Password and click **OK**. A Task window opens.
10. Click the Action link to deploy your DLP policy. A **Take Action** dialog box opens.
11. In the Take Action dialog box:
    a. Select the computer(s) to which you would like to deploy your policy.
    b. Set any desired options such as for scheduling, messages to users, etc.
    c. For more information about setting options using the tabs in the Take Action dialog box, consult the ***BigFix Console Operators Guide***.
    d. Click **OK** when finished.
12. Enter your Private Key Password to continue. An Action window appears, allowing you to track the progress.

Frequently Asked Questions

What platforms does BigFix DLP support?

BigFix DLP supports Microsoft Windows 2000, XP, and Server 2003. Vista support is coming soon. BigFix recommends running the DLP client on computers with at least 1 GB of memory.

Does BigFix DLP use document tagging to keep track of sensitive information?

No. Our DLP solution does not alter documents in any way and it does not need to track files across computers. We use sophisticated techniques to analyze the contents of a file to determine whether that file contains sensitive information.

Can I create signature repositories?

Yes, you can create signature repositories and deploy them to clients. For more information, view the following knowledge-base articles:

http://support.bigfix.com/cgi-bin/kbdirect.pl?id=489

http://support.bigfix.com/cgi-bin/kbdirect.pl?id=490

Does BigFix DLP require a network appliance?

No. BigFix DLP resides on the endpoints, thereby protecting the main source of data leakage in a company. Note that BigFix DLP will integrate with many industry leading DLP solutions.

Why is the "BigFix DLP: Run Scan" task not relevant?

In order to run a scan, you must first create and deploy a policy using the BigFix DLP Policy Configuration Wizard.

Do I need to run a scan first in order to start monitoring sensitive data transfers?

No. To enable real-time monitoring of sensitive data, all you need to do is install BigFix DLP and create and deploy a policy.

What is the performance impact of the real-time BigFix DLP technology?

The BigFix DLP technology works much like AntiVirus technology (BigFix DLP monitors outbound file and network activities rather than monitoring inbound files like AntiVirus) and has similar performance characteristics. BigFix DLP will remain idle until information leaves the computer and then the data is checked for sensitive information. The amount of time spent checking most files are measured in fractions of seconds and the user experience is not expected to change.

Will BigFix DLP run on server class computers?

Yes. However, it is recommended that you do extensive testing to ensure that the real-time BigFix DLP agent does not affect your server processes (especially servers that send lots of information over the network). In order to prevent accidental deployment of BigFix DLP to server class computers without testing, the default BigFix DLP installation Task is not relevant on servers.

Can BigFix DLP violation events be correlated with other event systems for correlation and long time storage?

Yes. The BigFix DLP solution fully supports integration with SIM, SIEM, or log parsing systems. BigFix DLP events can either by pulled directly from the BigFix Server or the Agents can upload their event logs directly to the event correlation system for import.

How long does it take the agent to send up information about violations and what happens if the agent is disconnected from the network?

The interval that the agent uses to send violation information to the server is configurable, but the default is set to 15-minute intervals. If the agent is not connected to the network, it will send up the violations when it is next connected to the network.

Can the user disable BigFix DLP?

When you deploy BigFix DLP, you have the option to hide BigFix DLP process and files, preventing users from easily seeing or disabling BigFix DLP. You can hide/show BigFix DLP with Tasks on the BigFix DLP Fixlet site. If BigFix DLP is hidden, only administrators on the computer can stop or disable the service.

About BigFix, Inc.

Founded in 1997, BigFix® Inc. offers the only converged IT security and operations platform that enables real-time visibility and control of globally distributed desktop, mobile and server computers. BigFix enables large-scale enterprises to continuously enforce IT security, IT policy compliance, and systems management on all computers, anytime, anywhere. Designed for highly distributed and complex IT infrastructures, BigFix delivers real-time endpoint visibility and control through its single-agent, multi-function, on-demand architecture. Its award-winning technology is proven in production at more than 600 companies, government agencies, and public sector institutions worldwide, and currently manages over 7,000,000 desktop and mobile clients, workstations, and servers. More information can be found at 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