



Web Protection Module

powered by  **TREND
MICRO**

User's Guide

Version 1.0

March, 2010

Copyright © 2009-2010 BigFix, Inc. All rights reserved.

Copyright © 1998-2010 Trend Micro Incorporated.

BigFix®, Fixlet® and "Fix it before it fails"® are registered trademarks of BigFix, Inc. i-prevention™, Powered by BigFix™, Relevance Engine™, and related BigFix logos are trademarks of BigFix, Inc.

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, Damage Cleanup Services, ScanMail, ServerProtect, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated or its affiliated entities. All other product or company names may be trademarks or registered trademarks of their respective owners. BigFix and Trend Micro use of any other company's trademarks, trade names, product names and logos or images of the same does not necessarily constitute: (1) an endorsement by such company of BigFix, Trend Micro, or their products, or (2) an endorsement of such company or its products by either BigFix or Trend Micro.

No part of this documentation or any related software may be reproduced, transmitted, or otherwise distributed in any form or by any means (electronic or otherwise) without the prior written consent of BigFix, Inc. or Trend Micro Incorporated. You may not use, modify, perform or display this documentation or any related software for any purpose except in connection with your use or evaluation of the BigFix/Trend Micro software delivered herewith as expressly set forth in a separate written agreement executed by BigFix, Inc. or Trend Micro, and any other use, including the reverse engineering of such software or creating compatible software or derivative works, is prohibited. If the license to the software that this documentation accompanies is terminated, you must immediately return this documentation and any related software to BigFix, Inc. or Trend Micro, Inc., or destroy all copies thereof that you may have and so certify upon request by BigFix, Inc. or Trend Micro Incorporated.

Both BigFix, Inc. and Trend Micro Incorporated reserve the right to make changes to this document and to the products described herein without notice.

All rights reserved.

Contents

CONTENTS

PART 1	4
Preface	4
System Requirements	4
Web Protection Module Dashboard.....	5
PART 2	9
Using the Web Protection Module	9
Blacklist and Whitelist Policies	9
Creating and Deploying a New Policy	9
Importing Lists of Web Sites	13
Viewing an Existing Policy	16
Copying and Editing a Policy	17
Editing Custom Actions	18
Deleting a Policy	21
Analyses	22
Viewing the Client Information Analysis.....	23
Viewing the Site Statistics Analysis.....	24
PART 3	26
Support.....	26
FAQs	26
Technical Support.....	27

Preface

The BigFix® Web Protection Module joins its real-time visibility and control capabilities with your existing desktop security solution to prevent Web-based malware from infecting your users' computers. WPM intercepts malware "in-the-cloud" before it reaches your users' systems, reducing the need for resource-intensive threat scanning and clean-up. Specifically, WPM monitors outbound web requests, stops web-based malware before it's delivered, and blocks users' access to potentially malicious websites in real time.

This guide will help you optimize the features of WPM for your environment by detailing how to manage Blacklist and Whitelist policies, Analyses, and the WPM Dashboard.

System Requirements

Supported Client Operating Systems

- Microsoft™ Windows™ 2000 Professional Edition (with the latest service pack)
- Microsoft™ Windows™ 2000 Server (with the latest service pack)
- Microsoft™ Windows™ 2000 Advanced Server (with the latest service pack)
- Microsoft™ Windows™ Server 2003 Enterprise Edition (with the latest service pack)
- Microsoft™ Windows™ Vista™ Business Edition (with the latest service pack)
- Microsoft™ Windows™ Vista™ Enterprise Edition (with the latest service pack)
- Microsoft™ Windows™ Server 2008 Enterprise Edition (with the latest service pack)
- Microsoft™ Windows™ XP Professional Edition (with the latest service pack)
- Microsoft™ Windows™ XP Home Edition (with the latest service pack)

Hardware Requirements

- Intel™ Pentium™ 350 MHz and above
- Windows Vista needs at least Intel Pentium 800 MHz
- At least 128 MB RAM
- Windows Vista needs at least 512 MB RAM
- At least 250 MB free disk space
- IPv4 Internet connection

Compatible Software

- Trend Micro™ OfficeScan™ Client/Server Edition 7.0
- Trend Micro™ Data Leak Prevention 3.1

- McAfee™ VirusScan™ Enterprise 8.0i
- McAfee™ VirusScan™ Enterprise 8.5i
- Symantec™ Anti-Virus Corporate Edition 10.0
- Symantec™ Endpoint Security and Control 7.0
- BigFix™ AntiVirus (CA™ eTrust™ Anti-Virus 7.1)
- CA™ eTrust™ Anti-Virus for the Enterprise r8.0

Note: You should conduct a thorough examination of untested security products for compatibility issues *before* deploying the Web Protection Module in your environment.

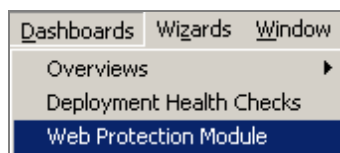
Incompatible Software

- Trend Micro™ RUBotted (Beta)
- Trend Micro™ TrendProtect 1.2
- Trend Micro™ Web Protection Add-On (Any)
- Trend Micro™ OfficeScan™ Client/Server Edition 8.0
- Any other Trend Micro product with Trend Micro Web Reputation Services enabled

Web Protection Module Dashboard

The Web Protection Module provides a dashboard that enables you to view statistics about the Web sites users' access and the number of threats that it blocks. You can access the Dashboard one of two ways:

1. To access the Dashboard from the BES Console, click the *Dashboards* pull down and select Web Protection Module.

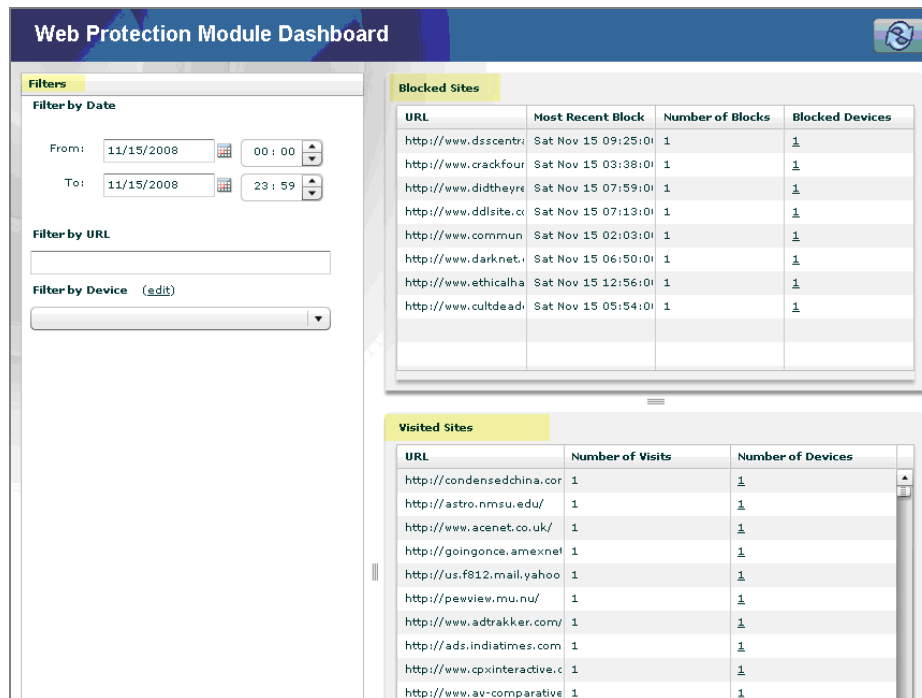


2. To access the Dashboard from Web Reports, click *Reports* then click the Web Protection Module *Dashboard* link in the Content Reports area of the Report Management pane.

Report Management [?]				
Content Reports				
(1 report found. Displaying report 1-1)				
Name ▲	Sitename	Category	Source	Favorite
[?] Web Protection Module Dashboard	Web Protection Module	Web Protection	BigFix, Inc.	No[add] copy

The Web Protection Module Dashboard provides summary information about the Web threats blocked by each Web Protection Agent. When you initially see the screen, it displays information for all deployed Web Protection Agents.

The Dashboard is organized into *Filters*, *Blocked Sites*, and *Visited Sites*.



You can use the Web Protection Module Dashboard to view overall Web statistics or drill down to the individual endpoints.

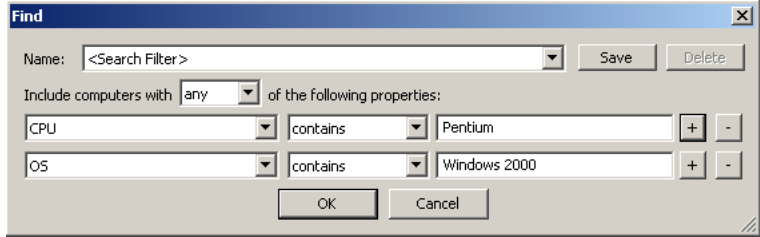
Note: The Web Protection Module Dashboard only reports information that is currently on each endpoint. If you have both a Log Maintenance and corresponding Log Upload policy in place, which BigFix recommends as a best practice, historical information older than your specified aging threshold is archived on the BES server.

To see historical information for blocked and visited sites, review the log entries in the following directory:

```
<server installation directory>\UploadManagerData\BufferDir\sha1\<last 2 digits of the client id>\<client id>\
```

Statistics are available for the following parameters:

- **Filters**—Use these filters to restrict and organize Dashboard information. Once you set them, these settings enable you to do the following:

Filter Category	Description
Filter by Date	<p>Set the date and time range of the information you want displayed in the Blocked Sites and Visited Sites tables. The entries default to the current date and time in 24-hour format beginning at 00:00 hrs. and ending at 23:59 hrs.</p> <p>To change the date range, you can either:</p> <ul style="list-style-type: none"> ▪ Choose each day by picking it from a calendar, which you display by clicking the Calendar icon ▪ Enter each date manually <p>To change the time, you can either:</p> <ul style="list-style-type: none"> ▪ Use the arrow keys to select the appropriate hours and minutes ▪ Enter the times manually
Filter by URL	<p>Display information for specific URLs. If a URL is blocked, it appears in both the Blocked Sites and Visited Sites tables. If the URL was not blocked, information for it only appears in the Visited Sites table.</p>
Filter by Device	<p>Display information in the Blocked Sites and Visited Sites tables for only those Web Protection Agents meeting the specified criteria. This feature allows you to use a modified version of the BES Console's Find feature to search for endpoints containing the specified property or properties (for example, OS, subnet, computer name, etc.). To access the Find feature, click (edit). The following illustration depicts this window:</p> 

- **Blocked Sites**—This table lists the Web sites blocked for the endpoints specified using Filters. Information is displayed by:
 - URL
 - Most Recent Block
 - Number of Blocks
 - Blocked Devices

- **Visited Sites**—This table lists the Web sites visited by endpoints using Filters. Information is displayed by:
 - URL
 - Number of Visits
 - Number of Devices

You can also resize the display according to your needs by moving one of the “handle” icons. Additionally, a Refresh button is available to clear any modified selections and reload the default values.

Further Refining Dashboard Listings

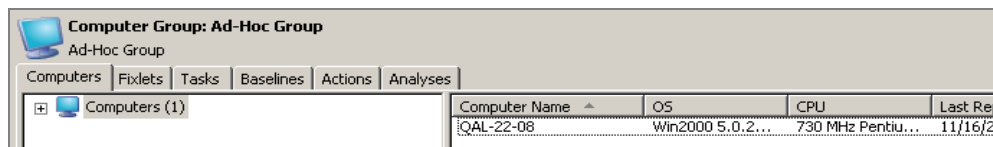
In addition to restricting the information in Blocked and Visited Sites tables through filter options, you can also sort and “drill down” to the individual endpoints using the Web Protection Module Dashboard.

To further sort a display, click or double-click on a column header. The header color changes and displays an arrow to indicate least to greatest (up arrow) or greatest to least (down arrow) number of entries.



URL	Number of Visits	Number of Devices ▲
http://www.comsoc.org/	1	1
http://www.henrikc.dk/	1	1
http://www.indo.com/	1	1
http://www.gomusic.ru/	1	1
http://thefurnituredomain.	1	1
http://www.despair.com/	1	1
http://articles.moneycentr	1	1

Additionally, you may create “ad-hoc” listings and drill down to individual endpoints by double-clicking an entry in the **Number of Devices** column.



Computer Group: Ad-Hoc Group				
Ad-Hoc Group				
Computers Fixlets Tasks Baselines Actions Analyses				
Computers (1)				
Computer Name ▲	OS	CPU	Last Rep	
iQAL-22-08	Win2000 5.0.2...	730 MHz Pentiu...	11/16/20	

Using the Web Protection Module

Blacklist and Whitelist Policies

The Web Protection Module Blacklist-Whitelist Wizard enables you to create and maintain global lists of Web sites in the form of policies that you can use to control your users' Web access. Once you have defined these policies, you use them to create Custom Tasks, which you can then apply to your endpoints.

There are two types of URL lists you can create and group into policies using the Wizard:

- **Blacklists** – These are lists of blocked Web sites. If the endpoint tries to access a site in one of these lists, they receive a message in their Web browser indicating that access to the site is blocked.
- **Whitelists** – These are lists of Web sites you allow your endpoints to access without restriction.

Note: Use care when selecting sites for Whitelists. Once a site is added to a Whitelist, it will no longer be checked. Therefore, endpoints connecting to that site would no longer be protected by WPM, should that site become a host for malware at some point in the future.

By creating multiple tasks, you can apply different sets of Blacklist and Whitelist policies to different users or groups of users. You can perform the following tasks using the Wizard:

- Create and Deploy a New Blacklist / Whitelist Policy
- Create and Deploy a New Blacklist / Whitelist Policy by importing an existing list
- View an existing Blacklist / Whitelist Policy
- Copy a Blacklist / Whitelist Policy
- Copy and edit a Blacklist / Whitelist Policy
- Delete a Blacklist / Whitelist Policy

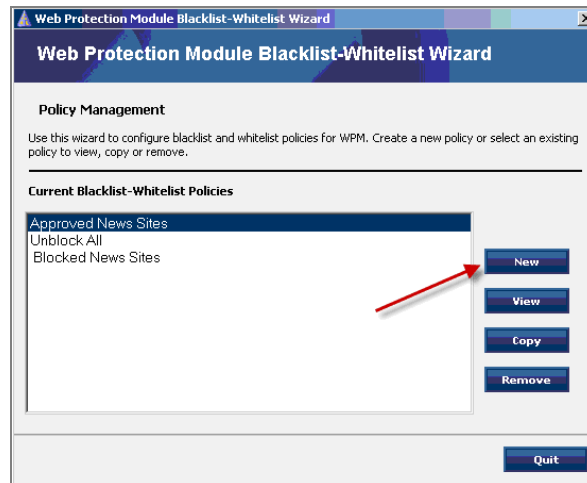
Note: The Blacklist / Whitelist file import feature requires that ActiveX controls are enabled in your browser. If you do not have this feature enabled, you will receive an error. For more information, check <http://support.bigfix.com/cgi-bin/kbdirect.pl?id=514>.

Creating and Deploying a New Policy

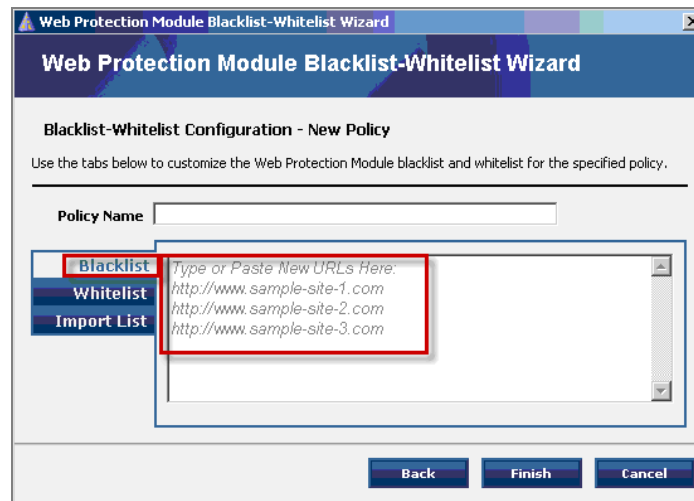
To create a new Blacklist / Whitelist policy:

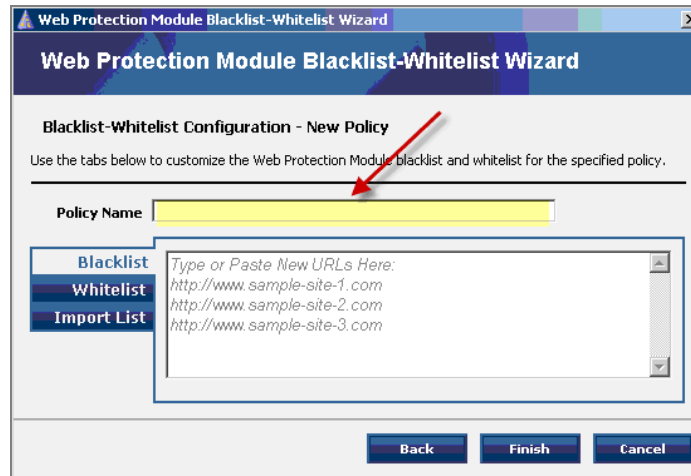
1. Click *Wizards > Web Protection Module Blacklist-Whitelist Wizard* to access the Web Protection Module Blacklist-Whitelist Wizard from the BES Console menu bar.

The Blacklist-Whitelist Wizard Policy Management window opens, showing a list of your currently available policies:



2. Click *New*. The *Blacklist-Whitelist Configuration – New Policy* window opens with the *Blacklist* tab open by default.



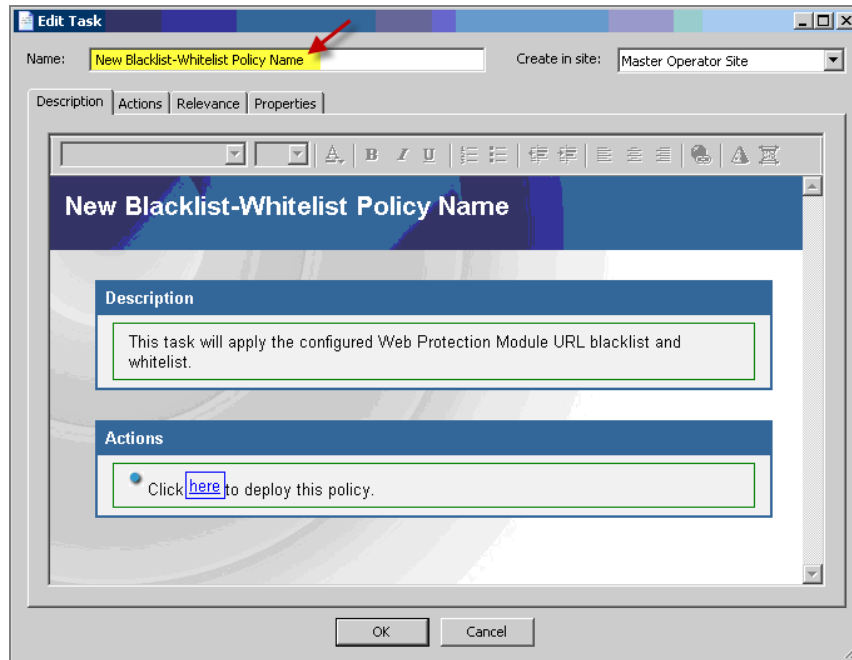


3. Enter a name for your policy in the *Policy Name* field.
4. In the Blacklist pane below the Policy Name field, enter or copy/paste the URLs you want to block. You may enter up to 500 URLs. You also must have “<http://>” before each URL entry. To block all the pages for a site, enter the name of the domain followed by “/*”, for example: http://www.badURL.com/*

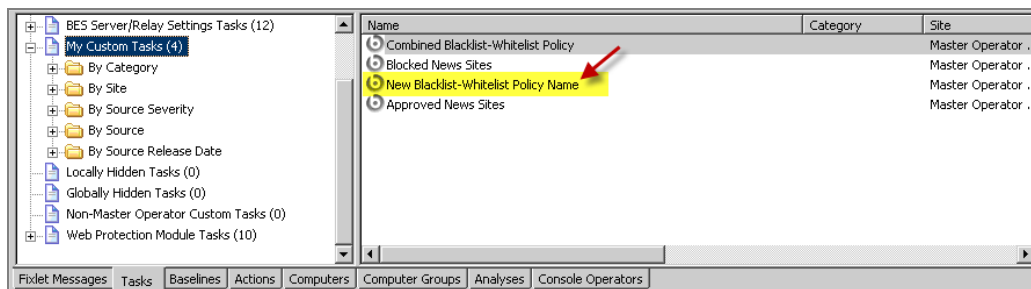
Note: You may block a maximum of 500 URLs per policy. If you wish to block additional URLs, create a different policy for each category of URLs that you would like to block.

Note: If you do not want to include a Whitelist in the policy, you may skip this part of the process. The Web Protection Module allows you to create Blacklist / Whitelist policies with *both* list types (Blacklist and Whitelist), *only* a Blacklist, or *only* a Whitelist.

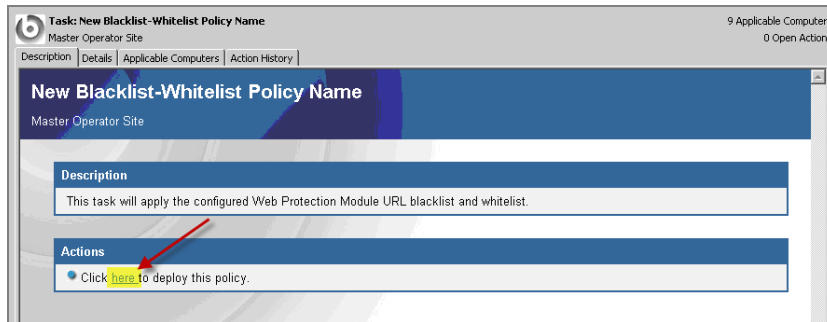
5. To enter a Whitelist, click the *Whitelist* tab. The Whitelist pane appears.
6. In the Whitelist pane, enter or copy/paste the URLs you want your users to be able to access without restriction. You may enter up to 499 URLs per policy. You also must have “<http://>” before each URL entry. To grant access to all the pages on a site, enter the name of the domain followed by “/*”, for example: http://www.goodURL.com/*
7. When you are finished creating your policy, click *Finish*. The Edit Task window appears.



8. Enter the name of your Blacklist / Whitelist policy in the Name field. This ensures that the name of the policy appears as the name of the custom task when you generate it.
9. Click *OK*.
10. Enter your Private Key Password and click *OK*. An Action window appears that displays the deployment status of your Custom Task. When it is finished, the status shows “Completed.”
11. In the Filter Panel, click *My Custom Tasks*. Your new Blacklist / Whitelist policy appears in the List Panel.



12. Double-click the name of your new Blacklist / Whitelist policy. The task pane for the policy appears.



13. Click where indicated in the *Actions* box. The Take Action window opens.
14. Select the computer or computers in the window to which you want to deploy your Blacklist / Whitelist policy and set any desired options (such as for scheduling, messages to users, etc).

Note: For more information about setting options using the tabs in the Take Action window, see the [BigFix Console Operator's Guide](#).

15. When you have finished selecting options, click *OK*.
16. Enter your Private Key Password and click *OK*. An Action window appears in which you can track the progress as BES deploys your Blacklist / Whitelist policy to your endpoints. When it is finished, the status shows “Completed.”

Importing Lists of Web Sites

The Web Protection Module allows you to import URLs for new Blacklist and Whitelist policies from newline-delimited files.

Note: The Blacklist / Whitelist file import feature requires ActiveX controls to be enabled on your browser. If you do not have this feature enabled, you will receive an error when you try to browse a file. For more information, check the following link: <http://support.bigfix.com/cgi-bin/kbdirect.pl?id=514>.

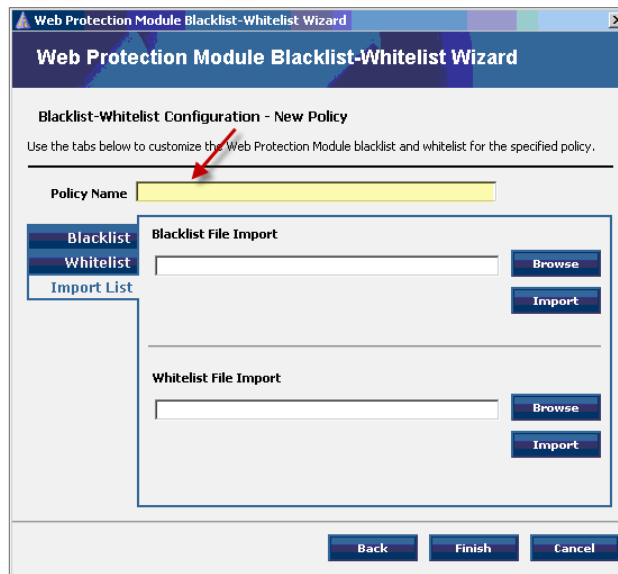
To create a new policy by importing lists of blacklisted and whitelisted Web sites:

1. Create two text files - one for the Web sites you want this policy to block and another for the Web sites to which you want to give your users unrestricted access.

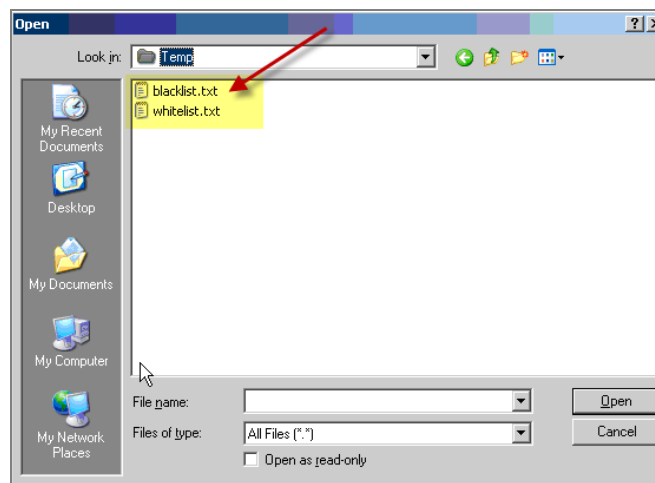
Note: If you do not want to include a Whitelist in the policy, you may skip this part of the process. The Web Protection Module allows you to create Blacklist / Whitelist policies with *both* list types (Blacklist and Whitelist), *only* a Blacklist, or *only* a Whitelist.

2. Press *Enter* or place a “newline” code at the end of each line to separate each entry. You must have “http://” before each URL entry. To block all the pages for a site, enter the domain name followed by “/*”, for example: `http://www.badURL.com/*`
3. Click *Wizards > Web Protection Module Blacklist-Whitelist Wizard* to access the Web Protection Module Blacklist-Whitelist Wizard from the BES Console menu bar. The Blacklist-Whitelist Wizard Policy Management window opens.

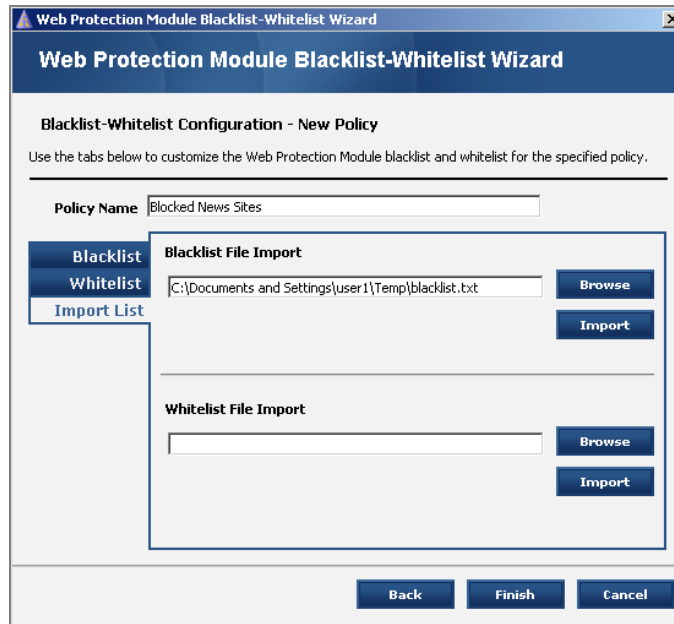
- Click *New*. The *Blacklist-Whitelist Configuration – New Policy* window opens.
- Click the *Import List* tab. The Import List pane appears.



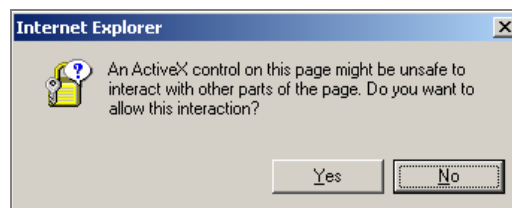
- Enter the name for the new policy in the *Policy Name* field.
- Select the text file you wish to import by either manually entering the path in the field under the Blacklist File Import / Whitelist File Import heading or by clicking *Browse* next to the type of file you wish to import. If you click *Browse*, the Open window appears.



- Use the Open window to navigate to the location where you have the text file.
- Select the file and click *Open*. The path to the selected file appears in the Import pane.



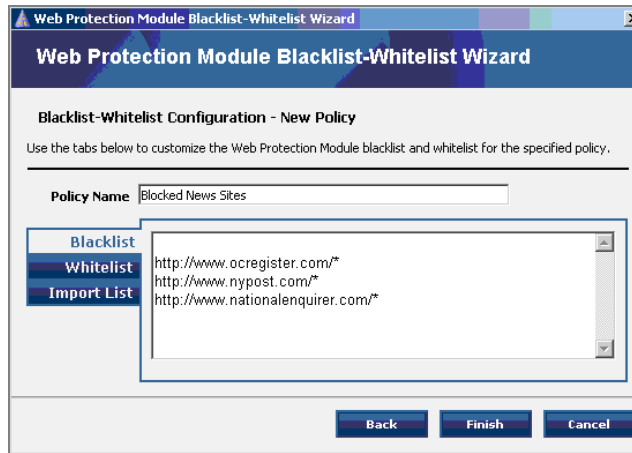
10. Click *Import*. An ActiveX warning message appears.



11. Click *Yes* to import the file. If you click *No*, you must re-launch the Wizard and perform the import process again to properly import the list.

After you click *Yes*, the Blacklist / Whitelist Wizard displays the contents of the tab associated with the file.

Note: When importing both a Blacklist and Whitelist in the same policy, the *Blacklist-Whitelist Configuration – New Policy* window, as shown below, does not appear. Instead the *Edit Task* window displays. Finish creating the Custom Action and deploy the combined policy in the *Creating and Deploying a New Blacklist / Whitelist Policy* section above.



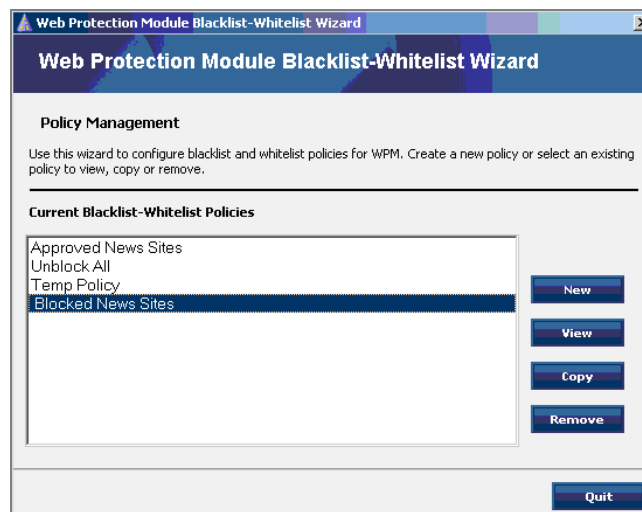
12. Click *Finish* to end the import process and start generating the relevant Custom Action.

Note: To see the process required to finish generating your Custom Action and deploy the policy, see steps 7-16 in the *Creating and Deploying a New Blacklist / Whitelist Policy* section above.

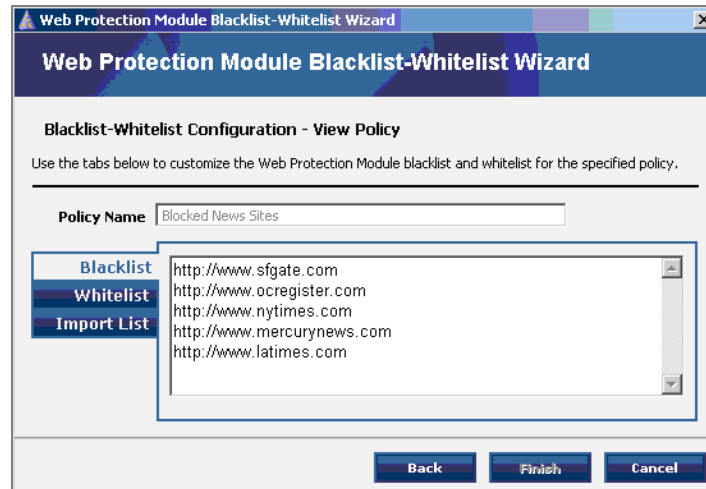
Viewing an Existing Policy

To view an existing Blacklist / Whitelist policy:

1. Click *Wizards > Web Protection Module Blacklist-Whitelist Wizard* to access the Web Protection Module Blacklist-Whitelist Wizard from the BES Console menu bar. The Blacklist-Whitelist Wizard Policy Management window opens:

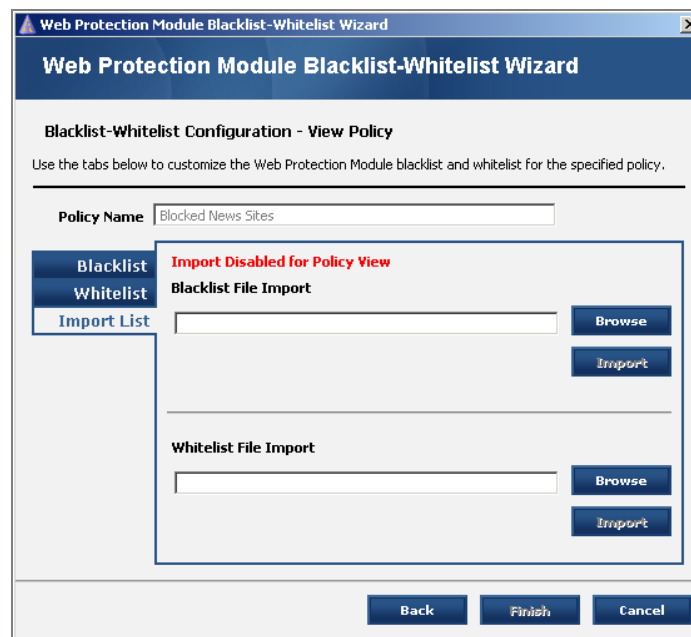


2. Select the name of the Blacklist / Whitelist policy you want to examine and click *View*. The *Blacklist-Whitelist Configuration – View Policy* window appears.



Notice that the contents of the *Policy Name* field and the *Finish* button are grayed out. This indicates that you are in *View-only* mode and cannot make any changes.

3. You may view either the Blacklist or Whitelist entries for this policy by clicking the appropriate tab and scrolling up or down using the arrow buttons on your keyboard. You can also return to the *Policy* view by clicking the *Back* button. (In this case, the Import List feature is disabled).

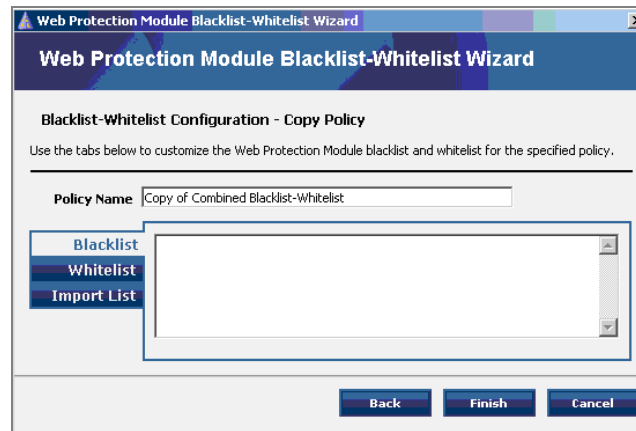


4. To exit the *Blacklist-Whitelist Configuration – View Policy* window, click either *Cancel* or *Close*.

Copying and Editing a Policy

The Web Protection Module enables you to create copies of existing Blacklist / Whitelist policies. Use this feature to create copies of existing policies or to create slightly modified versions of existing policies. To create a copy of an existing Blacklist / Whitelist policy:

1. Click *Wizards > Web Protection Module Blacklist-Whitelist Wizard* to access the Web Protection Module Blacklist-Whitelist Wizard from the BES Console menu bar. The Blacklist-Whitelist Wizard Policy Management window opens.
2. Select the name of the Blacklist / Whitelist policy you want to duplicate and click *Copy*. The Blacklist-Whitelist Configuration – Copy Policy window appears.



The name of the policy appears in the form of “Copy of...” followed by the policy name you chose to copy. The Web Protection Module automatically copies the contents of the Blacklist and Whitelist fields into the new policy.

3. Change the name in the Policy Name field to what you want it to be.
4. Make any other changes you want to the policy. For example, in copied policies you can:
 - Add new URLs to the copied Blacklist or Whitelist
 - Remove URLs from the Blacklist or Whitelist
 - Import and append either an external Blacklist or an external Whitelist to your Blacklist and Whitelist entries
5. When you have modified the policy, click *Finish* to end the process and start generating the relevant Custom Action.

Note: To see the process required to finish generating your Custom Action and deploy the policy, see steps 7-16 in the *Creating and Deploying a New Blacklist / Whitelist Policy* section above.

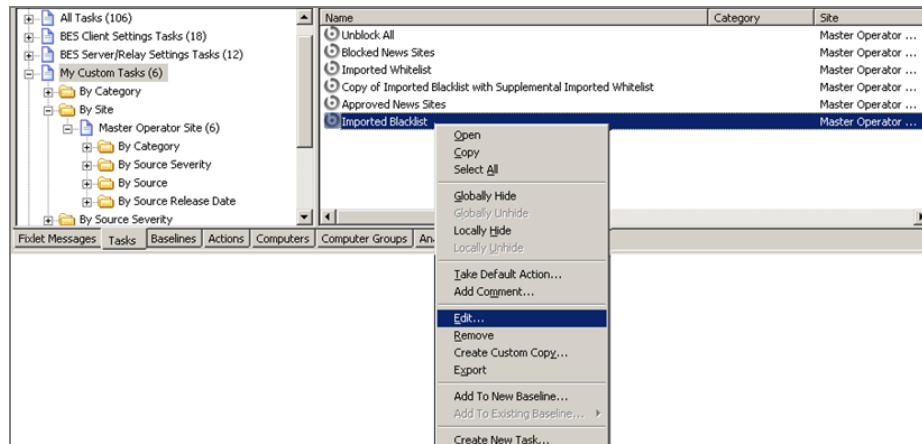
Editing Custom Actions

The Blacklist / Whitelist Wizard does *not* allow you to edit existing Blacklist / Whitelist policies. (You can only make modifications to new copies of policies, not the originals.) If necessary, however, you may edit the Custom Actions generated by the Wizard.

You may edit these Custom Actions in two different ways:

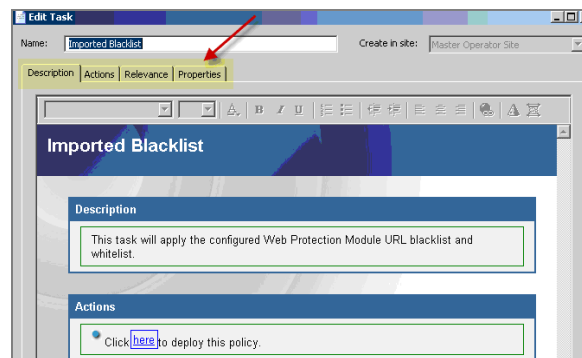
- By making modifications using the Edit Task window immediately after you click Finish to create the Custom Task
- By accessing the Edit Task window *after* you have completely generated the Custom Task

To make modifications using the Edit Task window, either access it as part of Custom Task generation process or select it by right-clicking on the name of an existing Custom Task and selecting Edit.



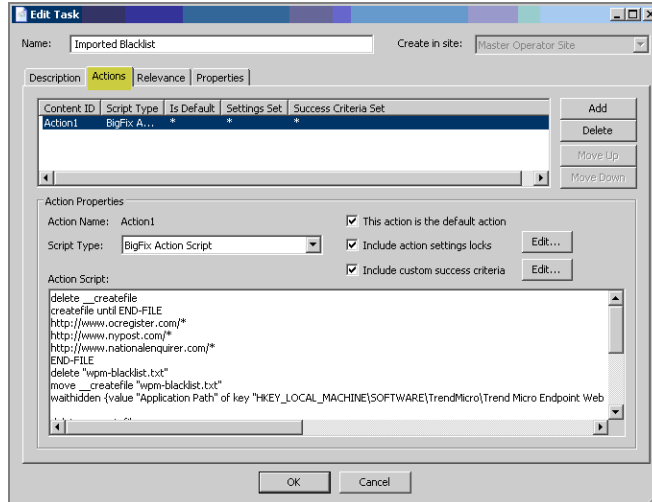
The Edit Task window consists of four tabs:

- *Description*
- *Actions*
- *Relevance*
- *Properties*

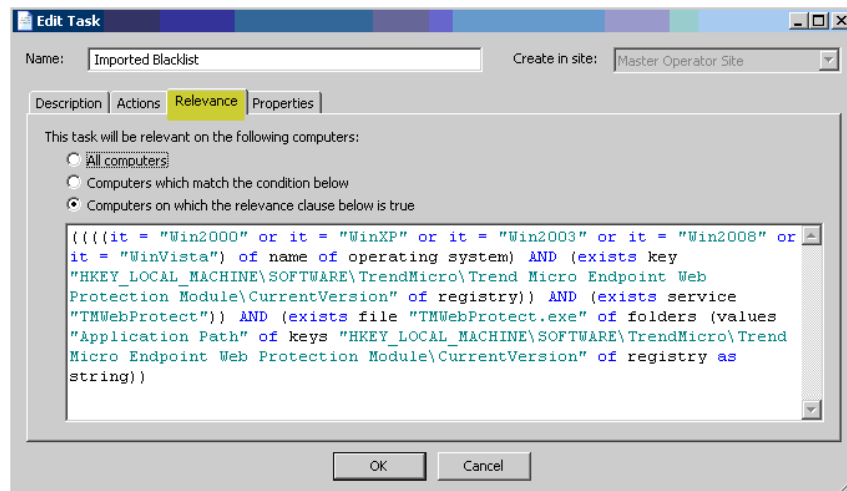


Use the *Description* tab to make modifications to the task name, title, and description. Use the *Actions* tab to view or change the Action this Custom Task performs. For example, use this window to add or remove Blacklisted or Whitelisted URLs from the presented Action Script.

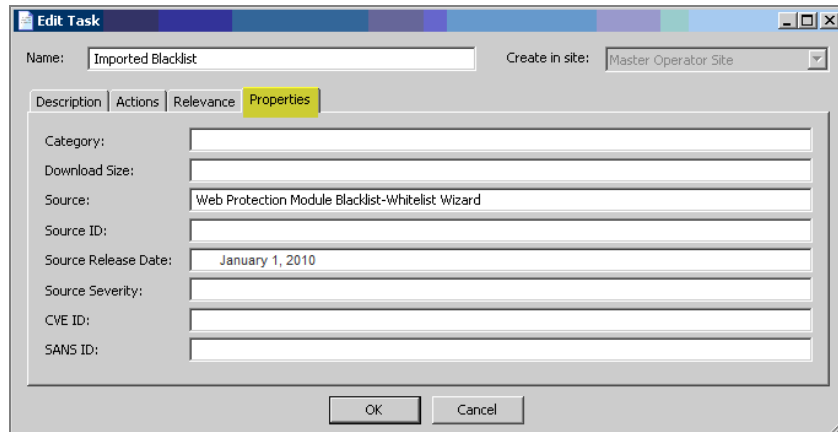
Note: For general information on using the Edit Task window, check the [BigFix Console Operator's Guide](#). For more detailed information on modifications to Custom Actions, see the [BigFix Action Language Reference](#) available on the BigFix support website.



Use the *Relevance* tab to view and make modifications to the relevance for a Custom Task. By default, the relevance for Blacklist / Whitelist is static. Its purpose is to detect endpoints for the Web Protection Module.



Use the *Properties* tab to view and modify the properties for this custom task.

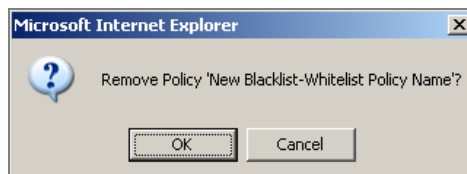


When you have finished making modifications, click *OK*. When the Private Key Password window appears, enter your password and click *OK* again. The edited/changed Blacklist / Whitelist policy appears in the List Panel when you choose My Custom Tasks.

Deleting a Policy

Follow the steps below to delete an existing Blacklist / Whitelist policy from the Wizard's Policy Management list:

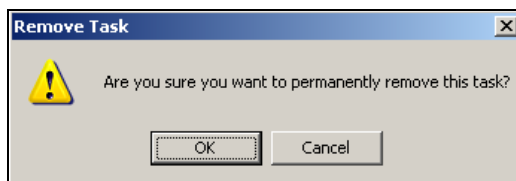
1. Click the *Wizards > Web Protection Module Blacklist-Whitelist Wizard* from the BES Console menu bar. The Blacklist-Whitelist Wizard Policy Management window opens.
2. Select the name of the Blacklist / Whitelist policy you want to delete and click *Remove*. The *Remove* window appears.



3. Click *OK*. The Web Protection Module removes the policy from the Blacklist-Whitelist Wizard Policy Management window.
4. Click *Quit* to exit the Wizard.

Note: The Blacklist-Whitelist Wizard Remove feature only deletes the policy from the Management list. It does not delete the custom Task you created with the policy. To completely remove the Blacklist-Whitelist policy from your endpoints, follow the steps below.

5. Select the name of the policy you wish to delete in the My Custom Tasks list and right-click. The right-click menu appears.
6. Select *Remove* from the right-click menu. The Remove Task confirmation window appears:



7. Click **OK**. The Private Key Password window appears.
8. Enter your Private Key Password and click **OK**. BES displays a series of messages as it removes the Custom Task from the affected WPM Agents and the List Panel.

Analyses

The Web Protection Module allows you to view detailed information about an endpoint or group of endpoints protected by a Web Protection Agent. By default, BigFix delivers these analyses activated.

Use the Client Information analysis to view information about each endpoint protected by a Web Protection Module Agent. You can use this analysis to view the following Properties of each endpoint:

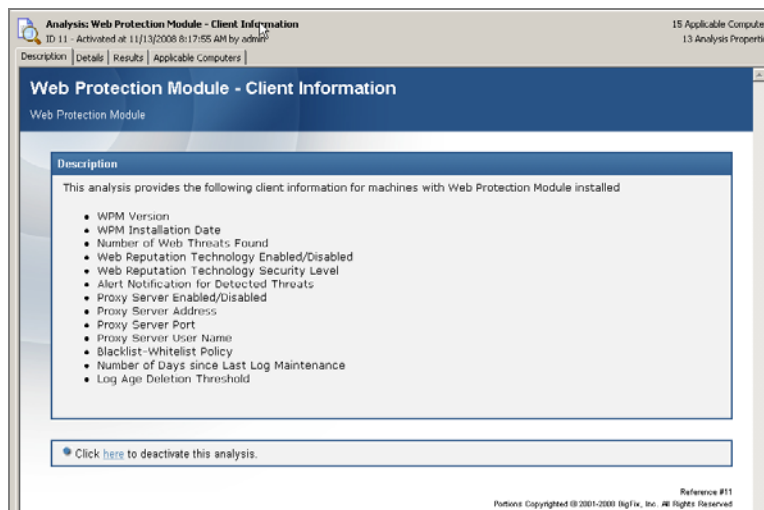
Field Name	Field Description
WPM Version	The version of the Web Protection Module Agent installed on the endpoint
WPM Installation Date	The date the Web Protection Module Agent was installed
Number of Web Threats Found	The number of Web threats encountered and recorded in the endpoint's CONFIG.INI file
Web Reputation Technology Enabled/Disabled	The status of the Agent's Web Reputation feature (Enabled/Disabled)
Web Reputation Technology Security Level	The security level for the Web Reputation feature (High, Medium, or Low)
Alert Notification for Detected Threats	Whether or not the alert notification feature for detected threats is enabled
Proxy Server Enabled/Disabled	If a proxy server is enabled/disabled
Proxy Server Address	The address of the proxy server
Proxy Server Port	The port being used by the proxy server
Proxy Server User Name	The user name used by the client to connect to the proxy server
Blacklist-Whitelist Policy	The name of all Blacklist / Whitelist policies deployed to the Agent
Number of Days since Last Log Maintenance	The number of days that have elapsed since you last performed Log Maintenance
Log Age Deletion Threshold	The number of days that logs will be kept on the endpoint before they are deleted (the log age deletion threshold)

The Site Statistics analysis displays statistical information about the number of Web sites accessed by an endpoint. You can use this analysis to view the following:

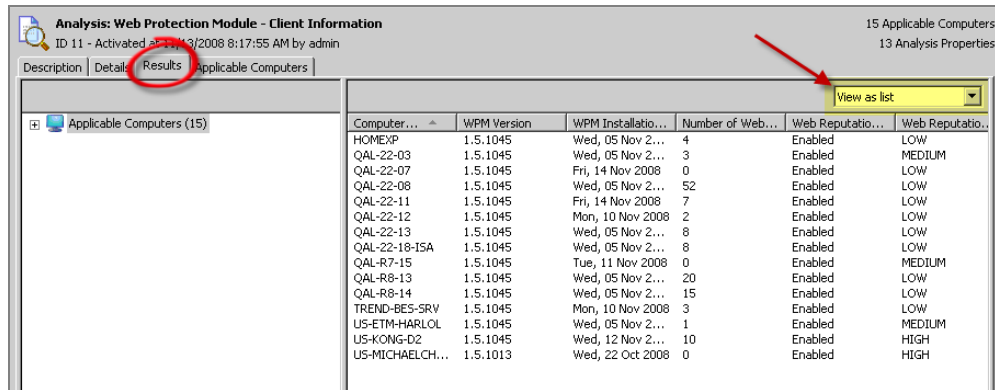
Field Name	Field Description
Blocked Sites	The number of Web sites blocked by an endpoint
Visited Sites	The number of Web sites visited by an endpoint

Viewing the Client Information Analysis

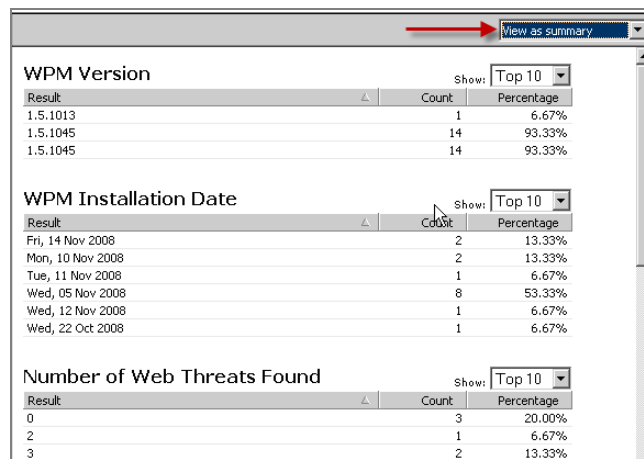
1. Click the *Analyses* tab. The List Panel changes to show all available analyses.
2. Click *All Applicable Analyses*.
3. Click the “+” sign and then click *By Site*.
4. Click *Web Protection*. The Web Protection Module presents you with two analyses:
 - Web Protection Module – Client Information
 - Web Protection Module – Site Statistics
5. Double-click the *Web Protection Module – Client Information Analyses* link. The *Web Protection Module – Client Information* window appears.



To view the view details about each property, click the Results tab.



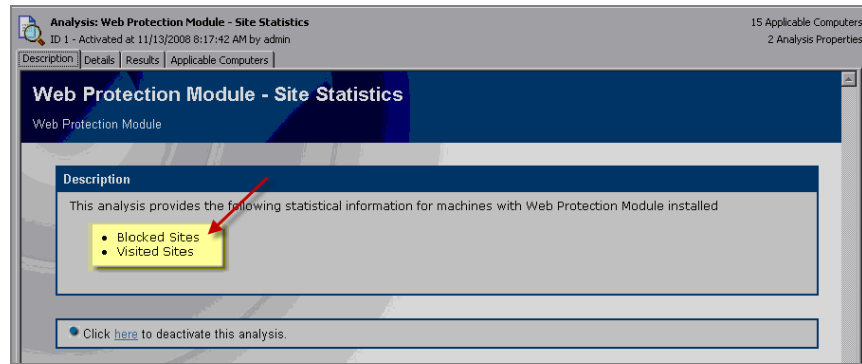
You can view the analysis property results in either List or Summary format. To select a perspective, choose the desired format from the drop down box in the upper-right corner of the analysis in the *Results* tab.



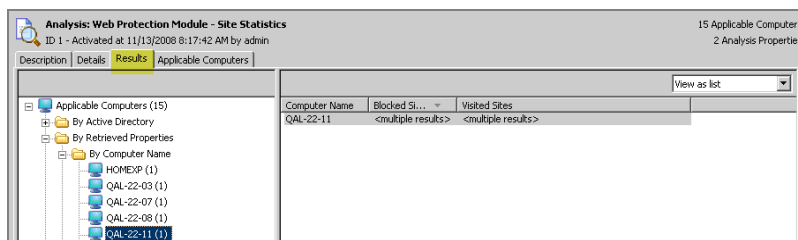
- If you wish to deactivate the analysis, return to the click [here](#) link in the Action window.

Viewing the Site Statistics Analysis

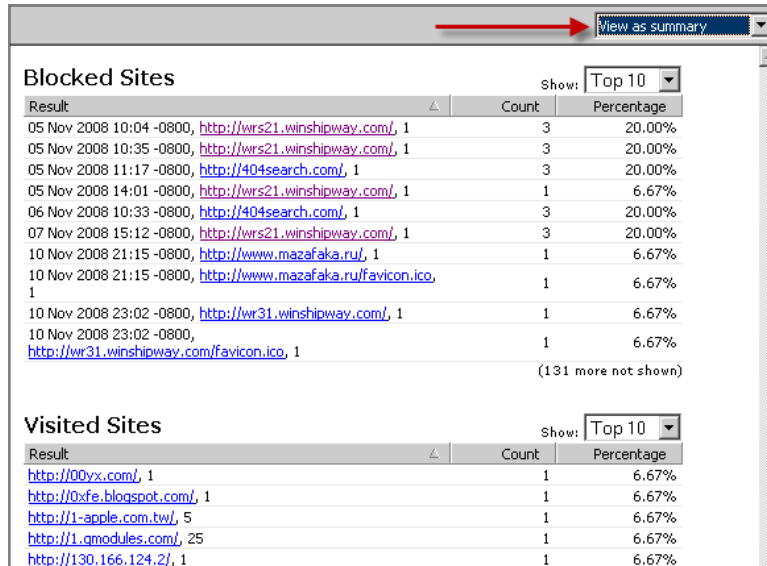
- Click the *Analyses* tab. The List Panel shows all available analyses.
- Click *All Applicable Analyses*.
- Click the “+” sign and then click *By Site*.
- Click *Web Protection Module*. The Web Protection Module presents you with a list of both available analyses.
- Double-click the *Web Protection Module – Site Statistics Analyses* link. The *Web Protection Module – Site Statistics* window appears. The window displays information on the two Web Protection Agent properties you can view with the analysis:
 - Blocked Web sites
 - Visited Web sites



6. To view the details of each property, click the Results tab at the top of the window.



7. You can view the analysis property results as either a list or in summary form. To select a perspective, choose the desired format from the drop down box in the upper-right corner of the analysis in the Results tab.



8. To deactivate the analysis, return to the Action window and click where indicated.

FAQs

What is the performance impact of the Web Protection Module Agent on network performance?

The Web Protection Module Agent is very lightweight and requires no pattern updates. It checks for web threats when the user accesses the Internet by performing a lookup on an “in-the-cloud” database. The Web Protection Module Agent uses the site’s “reputation” score and a security level set by the Console Operator to block access to suspicious sites. Web Protection Module database lookups are optimized to use very little bandwidth (similar in size to a DNS lookup) and have a negligible impact on network performance.

Does the Web Protection Module Agent run on server class computers?

Yes. It fully supports systems running Windows 2000 Server, Windows Server 2003 and Windows Server 2008.

Can Web Protection Module logs be used with other event systems for correlation and long term storage?

Yes. The Web Protection Module solution fully supports integration with SIM, SIEM, or log parsing systems. Web Protection Module URL history and blocked URL logs can either be pulled directly from the BES server or from the individual Agents themselves.

How long does it take the Web Protection Module Agent to upload logs and what happens if the Agent is disconnected from the network?

The interval that the agent uses to send logs to the server is configurable, but the default is once per day. If the agent is not connected to the network, it will upload copies of the logs when it is next connected to the network.

Can the user disable the Web Protection Module Agent?

Only if the user has administrative rights to their computer.

Technical Support

BigFix offers a suite of support options to help optimize your user-experience and success with this product. Here's how it works:

- First, check the BigFix website [Documentation](#) page
- Next, search the BigFix [Knowledge Base](#) for applicable articles on your topic
- Then check the [User Forum](#) for discussion threads and community-based support

If you still can't find the answer you need, [contact](#) BigFix's support team for technical assistance:

- Phone/US: 866 752-6208 (United States)
- Phone/International: 661 367-2202 (International)
- Email: enterprisesupport@bigfix.com