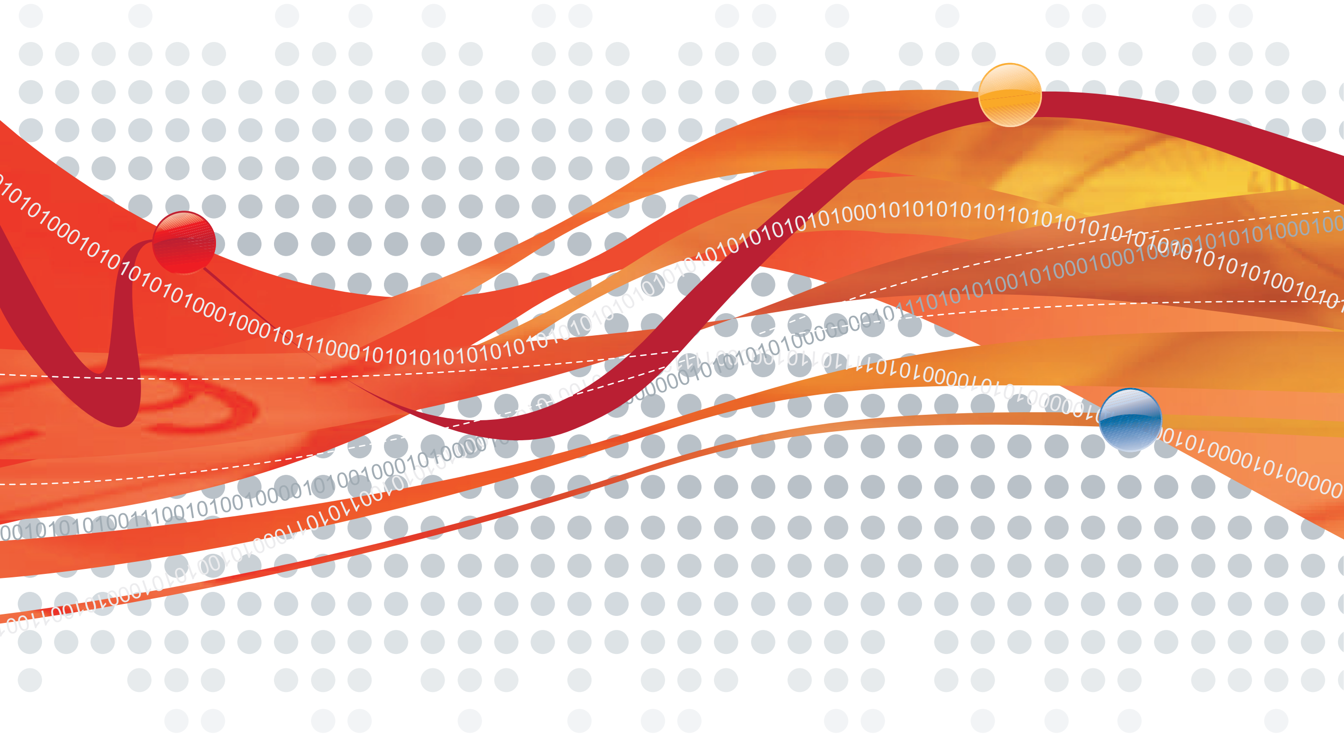
TREND MICRO™

Web Protection Module^{1}

for Endpoint Security Platform

Administrator's Guide



Endpoint Security

Document Part No. WPEM14324/91006

Release Date: October 2009

The user documentation for Trend Micro™ Web Protection Module 1.0 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at `docs@trendmicro.com`.

Please evaluate this documentation on the following site:

`http://www.trendmicro.com/download/documentation/rating.asp`

Contents

Preface

Chapter 1: Installing Trend Micro Web Protection Module

Chapter 2: Using Trend Micro Web Protection Module

Preface

Preface

Welcome to the *Trend Micro™ Web Protection Module User's Guide*. This guide contains information about product settings and service levels.

Trend Micro Web Protection Module (WPM) joins its real-time visibility and control platform with your existing desktop security solution to prevent Web-based malware from infecting your users' computers. Trend Micro Web Protection Module reduces the need for threat scanning and clean-up by intercepting malware before it reaches your users' computers. Specifically, WPM monitors outbound Web requests, stops Web-based malware before it's delivered, and blocks users' access to potentially malicious Web sites in real time.

This guide walks you through the installation and configuration of Trend Micro Web Protection Module, and addresses proxy settings, Web reputation technology, deploying WPM Agents, alert notifications, and uploading logs.

This preface discusses the following topics:

- *Trend Micro Web Protection Module Documentation*
- *Audience*
- *Document Conventions*
- *Supported Client Operating Systems*
- *Hardware Requirements*
- *Compatible Software*

- *Incompatible Software*
- *Process Overview*

Trend Micro Web Protection Module Documentation

The Trend Micro Web Protection Module documentation consists of the following:

Trend Micro™ Web Protection Module User's Guide — Helps you install, plan for deployment, and configure all product settings.

TrendEdge — The TrendEdge program works with Trend Micro employees, partners, and other interested parties to provide information on unsupported innovative techniques, tools, and best practices for Trend Micro products.

TrendEdge is available at:

http://trendedge.trendmicro.com

Audience

This document is intended to be used by new users of Trend Micro Web Protection Module, including system administrators, operators, sensitive content contributors, information security staff, executives, and other users with other specific roles.

The audience should have a thorough understanding of Trend Micro's Web Protection system, including general operations and critical concepts. Familiarity with Web browsers and Web-based user interfaces are also required.

Document Conventions

To help you locate and interpret information easily, the Web Protection Module documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

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 800MHz
- At least 128MB RAM
- Windows Vista needs at least 512MB RAM
- At least 250MB 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: Users should conduct a thorough examination of untested security products for compatibility issues before deploying Trend Micro Web Protection Module in their 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

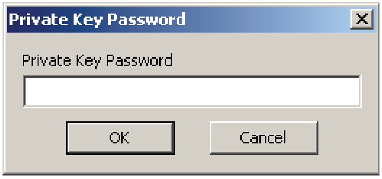
Process Overview

This procedure assumes that you have already installed the Trend Micro Endpoint Security Platform.

To begin the gathering process:

1. Obtain a masthead for the Web Protection Module site. Email `http://us.trendmicro.com/us/about/company/user_license_agreements/` to request the masthead.
2. Add the Web Protection Module site. Double-click on the masthead file. A window will appear, asking if you want to proceed with adding the site.
3. Click **Yes**.
4. Enter your Private Key Password and click **OK**.

FIGURE P-1. Private Key Password screen

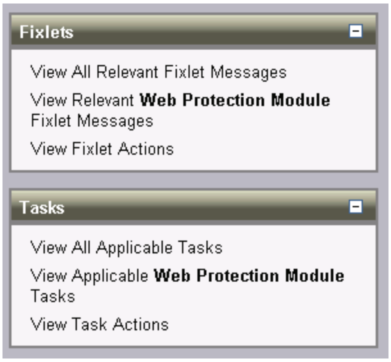


At this point, the Web Protection Module site begins the gathering process, in which it collects the Fixlets, Tasks, Analyses, and other components that will be used in the WPM solution.

When the gathering process is complete, the status changes to Subscribed.

You will see a new Web Protection Module entry in the Dashboards menu and links to Web Protection Module Tasks and Wizards in your Navigation Bar.

FIGURE P-2. Web Protection Module Entry



Fixlets

View All Relevant Fixlet Messages

View Relevant **Web Protection Module** Fixlet Messages

View Fixlet Actions

Tasks

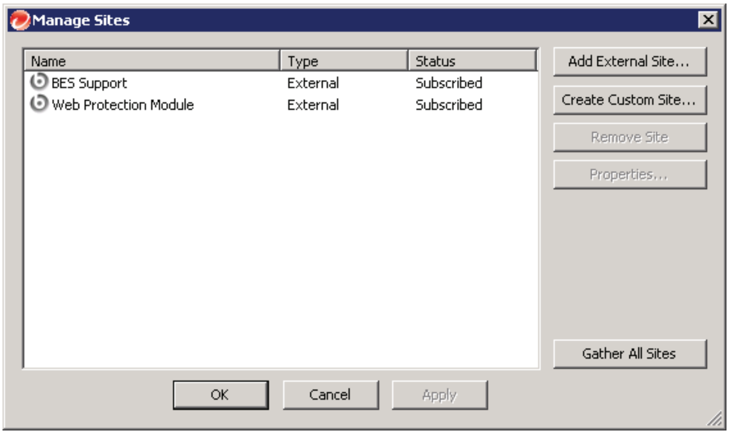
View All Applicable Tasks

View Applicable **Web Protection Module** Tasks

View Task Actions

In addition, the Web Protection Module site displays the Subscribed status in the Manage Sites window.

FIGURE P-3. Manage Sites page



Name	Type	Status
BES Support	External	Subscribed
Web Protection Module	External	Subscribed

Chapter 1

Installing Trend Micro Web Protection Module

This section provides instructions for performing the most common tasks with Trend Micro Web Protection Module.

This chapter covers the following topics:

- *Deploying Trend Micro Web Protection Module Agents*
- *Uninstalling Trend Micro Web Protection Module Agents*
- *Configuring Log Maintenance*
- *Configuring Proxy Settings*

Checking for Incompatible Software

Trend Micro Web Protection Module includes several AUDIT fixlets that automatically detect any of the following Trend Micro products:

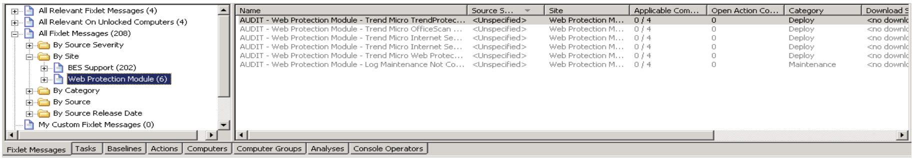
- Trend Micro™ OfficeScan™ Client/Server Edition 8.0
- Trend Micro™ TrendProtect
- Trend Micro™ Internet Security 2009
- Trend Micro™ Internet Security Pro

ESP cannot install Trend Micro Web Protection Module on an endpoint if one of these applications is installed. Before you deploy the Trend Micro Web Protection Module agent to your endpoints, verify that none of your endpoints are running these applications by completing the following steps:

To check for incompatible software:

1. Click the **Fixlet Messages** tab.
2. Select **All Fixlet Messages > By Site > Web Protection Module**.

FIGURE 1-1. Display of All Fixlet Messages



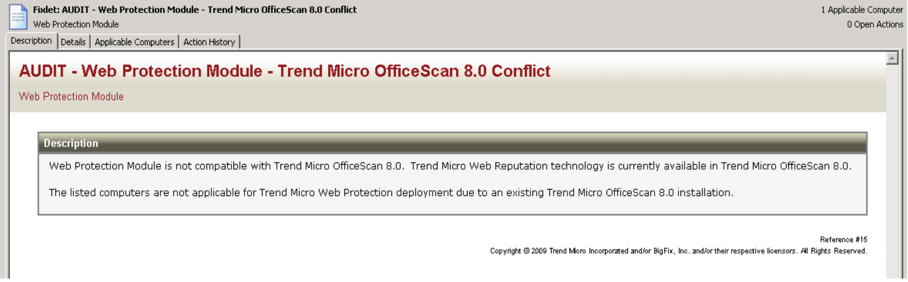
- All Relevant Fixlet Messages (4)
- All Relevant On Unlocked Computers (4)
- All Fixlet Messages (208)
  - By Source Severity
  - By Site
    - BES Support (202)
    - Web Protection Module (6)
  - By Category
  - By Source
  - By Source Release Date
- My Custom Fixlet Messages (0)

Name	Source S...	Site	Applicable Com...	Open Action Co...	Category	Download S
AUDIT - Web Protection Module - Trend Micro TrendProtec...	<Unspecified>	Web Protection M...	0 / 4	0	Deploy	<no downlo
AUDIT - Web Protection Module - Trend Micro OfficeScan ...	<Unspecified>	Web Protection M...	0 / 4	0	Deploy	<no downlo
AUDIT - Web Protection Module - Trend Micro Internet Se...	<Unspecified>	Web Protection M...	0 / 4	0	Deploy	<no downlo
AUDIT - Web Protection Module - Trend Micro Internet Se...	<Unspecified>	Web Protection M...	0 / 4	0	Deploy	<no downlo
AUDIT - Web Protection Module - Trend Micro Web Protec...	<Unspecified>	Web Protection M...	0 / 4	0	Deploy	<no downlo
AUDIT - Web Protection Module - Log Maintenance Not Co...	<Unspecified>	Web Protection M...	0 / 4	0	Maintenance	<no downlo

3. Check to see if any of the following AUDIT fixlets appear in the List Panel:
   - AUDIT – Web Protection Module – Trend Micro OfficeScan 8.0 Conflict
   - AUDIT – Web Protection Module – Trend Micro TrendProtect Conflict
   - AUDIT – Web Protection Module – Trend Micro Internet Security 2009 Conflict
   - AUDIT – Web Protection Module – Trend Micro Internet Security Pro Conflict
   - AUDIT - Web Protection Module – Trend Micro Web Protect Add-on Conflict
   - AUDIT - Web Protection Module – Log Maintenance Not Configured

4. If one of the AUDIT fixlets appears, double-click on it to display the Document tabs for the message.

FIGURE 1-2. AUDIT Fixlet Document tabs



AUDIT - Web Protection Module - Trend Micro OfficeScan 8.0 Conflict

Web Protection Module

Description

Web Protection Module is not compatible with Trend Micro OfficeScan 8.0. Trend Micro Web Reputation technology is currently available in Trend Micro OfficeScan 8.0.

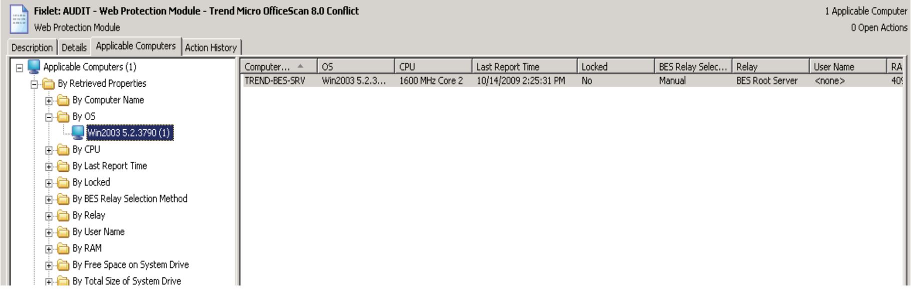
The listed computers are not applicable for Trend Micro Web Protection deployment due to an existing Trend Micro OfficeScan 8.0 installation.

Reference #15

Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

5. Click the **Applicable Computers** tab to determine which endpoint or endpoints are running the software.

FIGURE 1-3. Applicable Computers tab



Computer...	OS	CPU	Last Report Time	Locked	BES Relay Selec...	Relay	User Name	RA
TREND-BES-SRV	Win2003 5.2.3...	1600 MHz Core 2	10/14/2009 2:25:31 PM	No	Manual	BES Root Server	<none>	40

6. Manually remove the incompatible software from the endpoint or endpoints, and then reboot.
7. Access the **Fixlet Messages** tab again. The message should no longer appear.

Note: Repeat this process for each AUDIT fixlet message that appears. You should have no AUDIT messages present when you begin deploying your Trend Micro Web Protection Module agents.

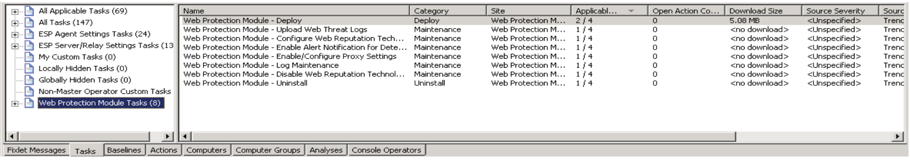
Deploying Trend Micro Web Protection Module Agents

You will now need to deploy the applicable Trend Micro Web Protection Module tasks.

To deploy Trend Micro Web Protection Module Agents:

1. From the Tasks Navigation bar, click to **View Applicable Web Protection Module Tasks** link. The Web Protection Module Tasks window appears.

FIGURE 1-4. Web Protection Module Tasks window

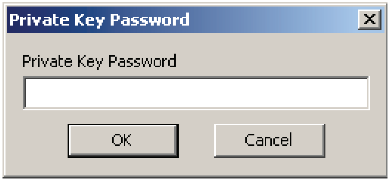


- All Applicable Tasks (69)
- All Tasks (147)
- ESP Agent Settings Tasks (24)
- ESP Server/Relay Settings Tasks (13
- My Custom Tasks (0)
- Locally Hidden Tasks (0)
- Globally Hidden Tasks (0)
- Non-Master Operator Custom Tasks
- Web Protection Module Tasks (8)

Name	Category	Site	Applicabl...	Open Action Co...	Download Size	Source Severity	Sourc
Web Protection Module - Deploy	Deploy	Web Protection M...	2 / 4	0	5.08 MB	<Unspecified>	Trenc
Web Protection Module - Upload Web Threat Logs	Maintenance	Web Protection M...	1 / 4	0	<no download>	<Unspecified>	Trenc
Web Protection Module - Configure Web Reputation Tech...	Maintenance	Web Protection M...	1 / 4	0	<no download>	<Unspecified>	Trenc
Web Protection Module - Enable Alert Notification for Dete...	Maintenance	Web Protection M...	1 / 4	0	<no download>	<Unspecified>	Trenc
Web Protection Module - Enable/Configure Proxy Settings	Maintenance	Web Protection M...	1 / 4	0	<no download>	<Unspecified>	Trenc
Web Protection Module - Log Maintenance	Maintenance	Web Protection M...	1 / 4	0	<no download>	<Unspecified>	Trenc
Web Protection Module - Disable Web Reputation Technol...	Maintenance	Web Protection M...	1 / 4	0	<no download>	<Unspecified>	Trenc
Web Protection Module - Uninstall	Uninstall	Web Protection M...	1 / 4	0	<no download>	<Unspecified>	Trenc

2. In the List Panel, click the **Web Protection Module – Deploy** link. The Web Protection Module – Deploy Task window appears.
3. Click the **here** link located in the Actions box to begin the installation process. The Take Action window appears.
4. In the Take Action window, select the computer(s) to which you would like to deploy the Trend Micro Web Protection Module agent. Set any desired options, such as scheduling, messages to users, and so on.
5. Click **OK** when finished. The Private Key Password page appears.

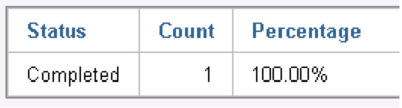
FIGURE 1-5. Private Key Password page



6. 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 shows "Completed."

FIGURE 1-6. Action window



Status	Count	Percentage
Completed	1	100.00%

Note: Trend Micro recommends configuring new Trend Micro Web Protection Module agents to prevent them from accumulating overly-large URL log files. (By default, ESP does not deploy new Agents with log maintenance configured.) For more information, see the section entitled Configuring Automatic Log Maintenance for New Agents.

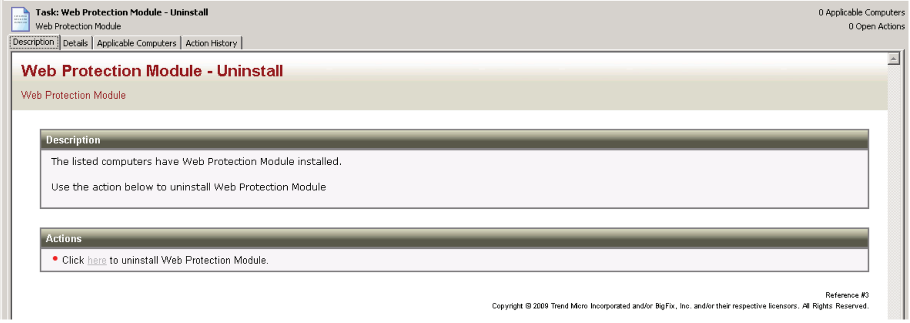
Uninstalling Trend Micro Web Protection Module Agents

In the event you would like to uninstall the Trend Micro Web Protection Module agents, you will need to complete the steps that follow.

To uninstall Trend Micro Web Protection Module Agents:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Uninstall** link. The **Web Protection Module – Uninstall Task** window appears.

FIGURE 1-7. Web Protection Module - Uninstall Task page



Task: Web Protection Module - Uninstall
Web Protection Module

0 Applicable Computers
0 Open Actions

Web Protection Module - Uninstall

Web Protection Module

Description

The listed computers have Web Protection Module installed.

Use the action below to uninstall Web Protection Module

Actions

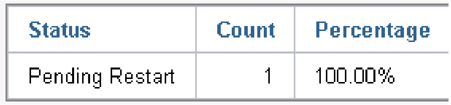
- Click here to uninstall Web Protection Module.

Reference #3

Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions box. The Take Action window appears.
4. Select the computer or computers from which you want to uninstall the Web Protection Agent and click **OK**. The Private Key Password window appears.
5. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your uninstall. When it is finished, the status shows "Pending Restart."

FIGURE 1-8. Action window



Status	Count	Percentage
Pending Restart	1	100.00%

Configuring Log Maintenance

The Web Protection Agent maintains two logs on your endpoints:

- A history of the URLs accessed on the endpoint (`urlhist.txt`)
- A record of the threats blocked per day by the Web Protection Agent (`urlthreats.txt`)

Trend Micro Web Protection Module agents can accumulate very large log files. Trend Micro recommends that you configure Agents to perform automatic log maintenance regularly to prevent these files from consuming excessive disk space.

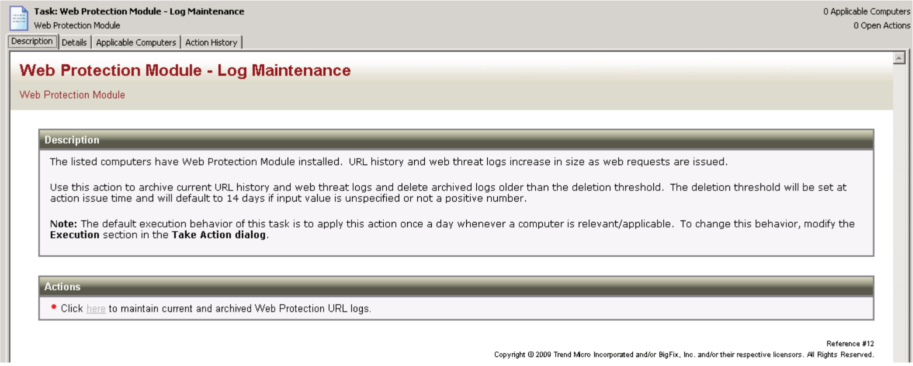
Use the Web Protection Module – Log Maintenance task to set the maximum amount of time (in days) that the Web Protection Agent will maintain these logs on the endpoint.

Note: Trend Micro strongly recommends setting up a global log maintenance regimen. If you do not perform regular log maintenance, large Web Protection Module logs will accumulate on each endpoint. The existence of these logs can slow the performance of both the endpoint itself and the Web Protection Module Dashboard. To archive Web Threat logs to the ESP server for later analysis, use the Web Protection Module – Upload Web Threat Logs task. For more information on using this task, see the Uploading Logs section below.

To enable log maintenance:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Log Maintenance** link. The Web Protection Module – Log Maintenance task window appears.

FIGURE 1-9. Web Protection Module - Log Maintenance page



Task: Web Protection Module - Log Maintenance
Web Protection Module

0 Applicable Computers
0 Open Actions

Description | Details | Applicable Computers | Action History

Web Protection Module - Log Maintenance
Web Protection Module

Description

The listed computers have Web Protection Module installed. URL history and web threat logs increase in size as web requests are issued.

Use this action to archive current URL history and web threat logs and delete archived logs older than the deletion threshold. The deletion threshold will be set at action issue time and will default to 14 days if input value is unspecified or not a positive number.

Note: The default execution behavior of this task is to apply this action once a day whenever a computer is relevant/applicable. To change this behavior, modify the **Execution** section in the **Take Action dialog**.

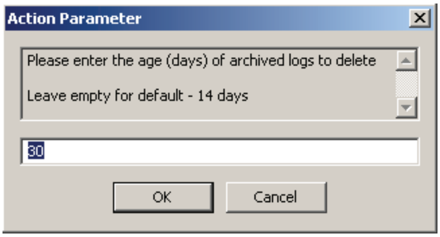
Actions

- Click here to maintain current and archived Web Protection URL logs.

Reference #12
Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions window. An Action Parameter window appears.

FIGURE 1-10. Action Parameter window



Action Parameter

Please enter the age (days) of archived logs to delete

Leave empty for default - 14 days

30

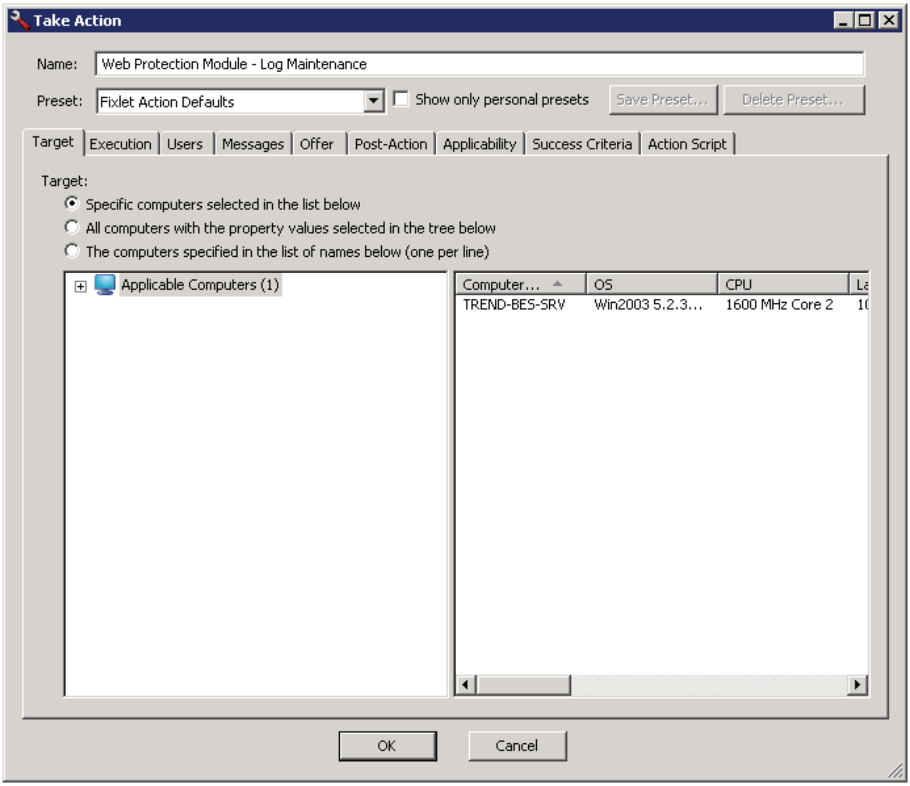
This window allows you to set the number of days the Web Protection Agent maintains logs on the selected endpoints.

4. Enter the number of days (for example, 30) you want to maintain logs, or leave the field blank to set the default (14).

   Click **OK** when finished. If desired, you can increase or decrease the frequency of the period between reapplications of the Log Maintenance action by adjusting the value in the indicated drop-down. You can increase the frequency with which logs are archived to as little as 15 minutes or decrease it to as long as 30 days.

5. The Take Action window appears and displays "Fixlet Action Defaults" in the Action Preset drop down box.

FIGURE 1-11. Take Action window



Take Action

Name: Web Protection Module - Log Maintenance

Preset: Fixlet Action Defaults

□ Show only personal presets

Target:

● Specific computers selected in the list below

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

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

Applicable Computers (1)

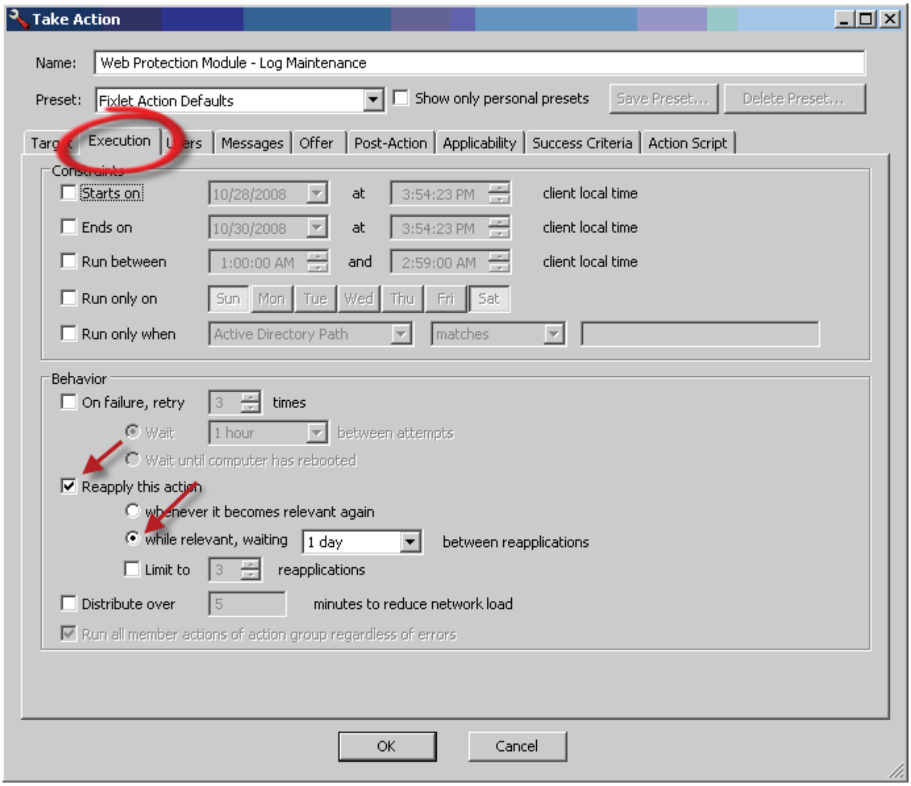
Computer...	OS	CPU	La
TREND-BES-SRV	Win2003 5.2.3...	1600 MHz Core 2	1(

Note: On the Targeting tab, select the **All Computers** button to target by property.

6. Click the **Execution** tab to view the default Behavior for this Action. The default is to perform the following tasks once per day:

- Archive the current URL history and Web threat logs
- Delete archived logs older than number of days you specify in Action Parameter window

FIGURE 1-12. Take Action - Applicability tab



Take Action

Name: Web Protection Module - Log Maintenance

Preset: Fixlet Action Defaults ☐ Show only personal presets [Save Preset...] [Delete Preset...]

Target | Execution | Users | Messages | Offer | Post-Action | Applicability | Success Criteria | Action Script

Constraints

☐ Starts on 10/28/2008 at 3:54:23 PM client local time

☐ Ends on 10/30/2008 at 3:54:23 PM client local time

☐ Run between 1:00:00 AM and 2:59:00 AM client local time

☐ Run only on Sun Mon Tue Wed Thu Fri Sat

☐ Run only when Active Directory Path matches

Behavior

☐ On failure, retry 3 times

● Wait 1 hour between attempts

○ Wait until computer has rebooted

☑ Reapply this action

○ whenever it becomes relevant again

● while relevant, waiting 1 day between reapplications

☐ Limit to 3 reapplications

☐ Distribute over 5 minutes to reduce network load

☑ Run all member actions of action group regardless of errors

7. Click **OK**. The Private Key Password window appears.
8. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your change. When it is finished, the status shows "Completed."

Note: If you want to change log maintenance behavior, first find any older log maintenance actions under the Actions tab and stop them. Then repeat steps 1-8.

Note: You can audit endpoints to ensure they are configured with a log maintenance action by checking that no machines are relevant for the "Log Maintenance Not Configured" Fixlet. Trend Micro recommends that you check this Fixlet on a regular basis.

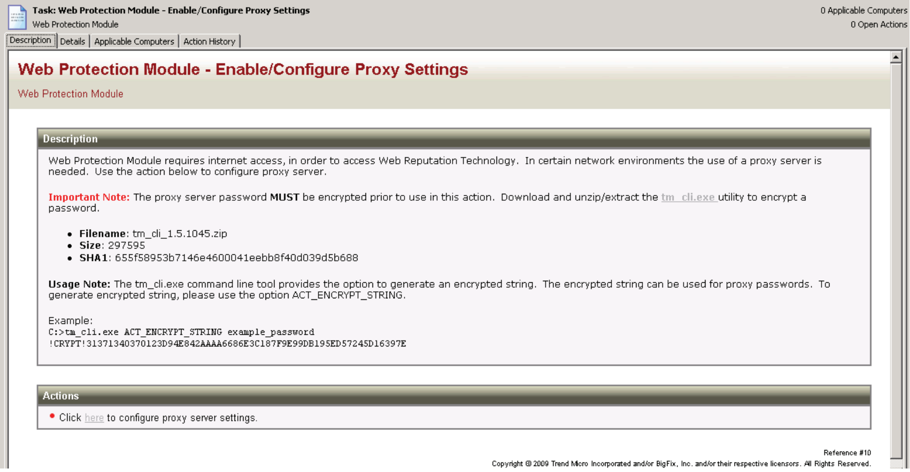
Configuring Proxy Settings

The Web Protection Agent supports the use of an internal Web proxy. It supports both password encrypted and non-password encrypted proxies.

To configure one or more of the Agent's proxy settings:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Enable/Configure Proxy Settings** link. The Web Protection Module – Enable/Configure Proxy Settings task window appears.

FIGURE 1-13. Web Protection Module - Enable/Configure Proxy Settings page



Web Protection Module - Enable/Configure Proxy Settings

Web Protection Module

Description

Web Protection Module requires internet access, in order to access Web Reputation Technology. In certain network environments the use of a proxy server is needed. Use the action below to configure proxy server.

Important Note: The proxy server password **MUST** be encrypted prior to use in this action. Download and unzip/extract the tm_cli.exe utility to encrypt a password.

- **Filename**: tm_cli_1.5.1045.zip
- **Size**: 297595
- **SHA1**: 655f58953b7146e4600041eebb8f40d039d5b688

Usage Note: The tm_cli.exe command line tool provides the option to generate an encrypted string. The encrypted string can be used for proxy passwords. To generate encrypted string, please use the option ACT_ENCRYPT_STRING.

Example:

```
C:>tm_cli.exe ACT_ENCRYPT_STRING example_password
!CRYPT!31371340370123D94E842AAAA6686E3C187F9E99DB195ED57245D16397E
```

Actions

- Click here to configure proxy server settings.

Reference #10

Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. If your proxy requires a password, complete the steps in the following section. Otherwise, follow the steps in the section entitled *Configuring the Proxy*.

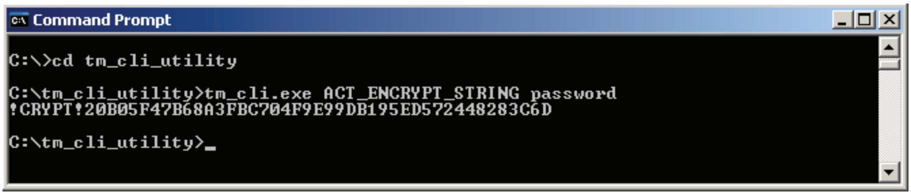
Encrypting a Proxy String

If your proxy server requires a password, you must encrypt it before you can continue. Click the `tm_cli.exe` link in the Web Protection Module – Enable/Configure Proxy Settings document page to download a zipped version of the password encryption utility.

1. Unzip the `tm_cli.zip` file and place both the `tm_cli.exe` and `TmpxCfg.dll` contents in a folder or `target_directory` that you can easily access.
2. Open a DOS Command window and use the cd command to navigate to your `target_directory`.
3. Enter the following command where the password you want to encrypt appears in italics.

   `C:\target_directory\tm_cli.exe ACT_ENCRYPT_STRING` *password.*

FIGURE 1-14. Command prompt



```
C:\>cd tm_cli_utility

C:\tm_cli_utility>tm_cli.exe ACT_ENCRYPT_STRING password
!CRYPT!20B05F47B68A3FBC704F9E99DB195ED572448283C6D

C:\tm_cli_utility>_
```

4. Copy and paste the encrypted string that appears under the command into a text editor, such as Windows Notepad, and save it for later use.

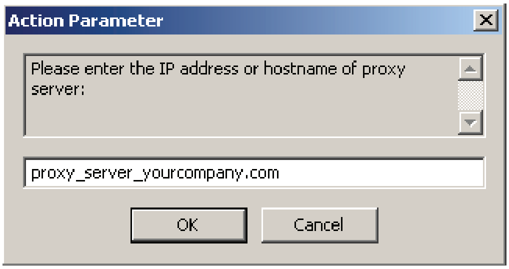
Configuring the Proxy

You must configure the proxy settings as described in the section that follows.

To configure the proxy:

1. Access the Web Protection Module – Enable/Configure Proxy Settings document page and click the **here** link in the Actions window. The first of four Action Parameter windows appears.

FIGURE 1-15. Action Parameter window 1



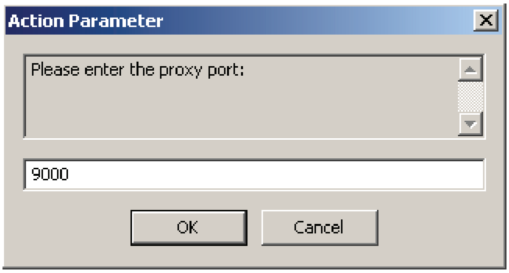
Action Parameter

Please enter the IP address or hostname of proxy server:

proxy_server_yourcompany.com

2. Enter the **IP address** or **hostname** of the Web proxy your wish to use and click **OK**. A second window appears, prompting you for the number of the proxy server port you wish to use.

FIGURE 1-16. Action Parameter window 2



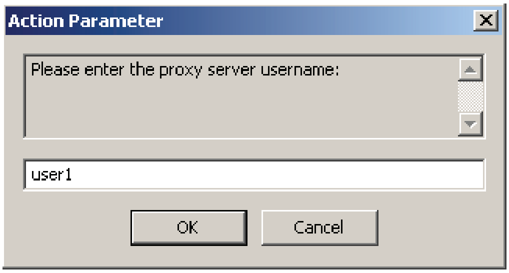
Action Parameter

Please enter the proxy port:

9000

3. Enter the port number and click **OK**. Another window appears asking for the username for accessing the proxy.

FIGURE 1-17. Action Parameter window 3



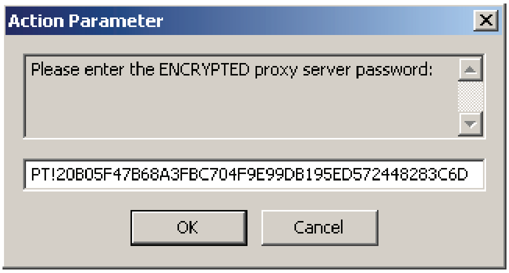
Action Parameter

Please enter the proxy server username:

user1

4. Enter the username you would like to use. If your proxy does not require a username, leave the field blank. When you are finished, click **OK**. Another window appears, asking you to enter the password you would like to use to access the proxy.

FIGURE 1-18. Action Parameter window 4



Action Parameter

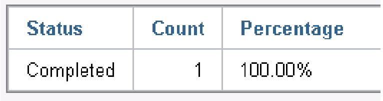
Please enter the ENCRYPTED proxy server password:

PT!20B05F47B68A3FBC704F9E99DB195ED572448283C6D

5. If you do not use a password to access the proxy, leave the field blank. Otherwise, copy and paste the encrypted string you saved earlier into the indicated field and click **OK**. The Take Action window appears.
6. Select the computers for which you would like to use the proxy and click **OK**. A window appears asking for your Private Key Password.

7. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your uninstall. When it is finished, the status shows **Completed**.

FIGURE 1-19. Action window



Status	Count	Percentage
Completed	1	100.00%

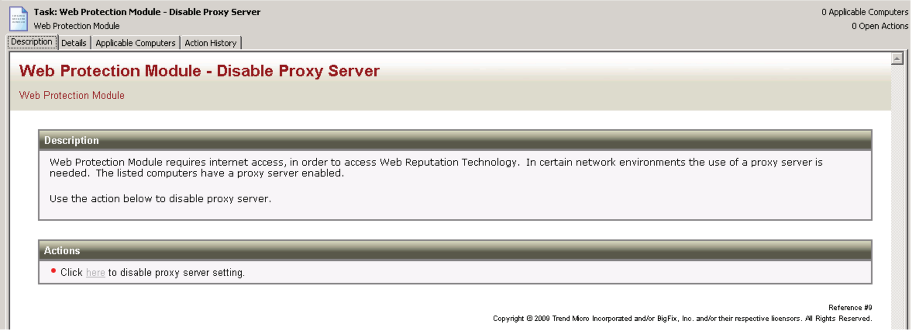
Disabling a Proxy Server

You can also disable a proxy server without uninstalling it.

To disable one or more Agent’s proxy settings:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Disable Proxy Server** link. The Web Protection Module – Disable Proxy Server window appears.

FIGURE 1-20. Web Protection Module - Disable Proxy Server page



Web Protection Module - Disable Proxy Server

Web Protection Module

Description

Web Protection Module requires internet access, in order to access Web Reputation Technology. In certain network environments the use of a proxy server is needed. The listed computers have a proxy server enabled.

Use the action below to disable proxy server.

Actions

- Click here to disable proxy server setting.

Reference #9

Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions box. The Take Action window appears.
4. Select the computer or computers for which you want to disable the proxy server and click **OK**. The Private Key Password window appears.
5. Enter your Private Key Password and click **OK**. A window appears in which you can track the progress of your Action. When it is finished, the status shows **Completed**.

Note: Because ESP saves the proxy configuration for each user, you can easily re-enable the use of the proxy by running the Enable/Configure Proxy Settings task again.

Disabling Web Reputation Technology

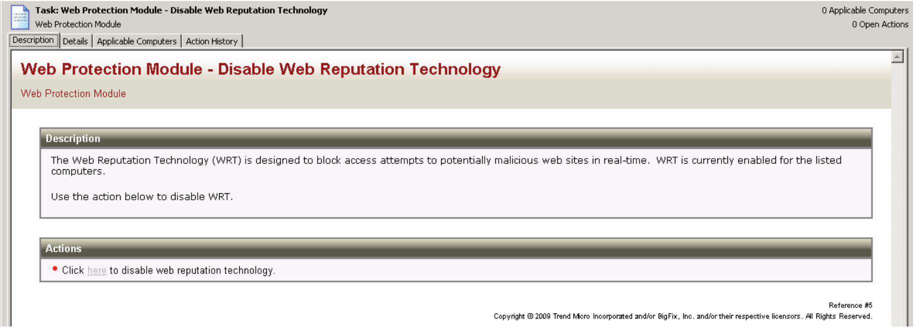
This section contains instructions for disabling Trend Micro Web Reputation Technology (WRT). WRT uses a "reputation score" calculated by heuristics and an "in-the-cloud" database of known threats to detect and block security risks in outbound Web requests.

WRT is activated by default when you install the Web Protection Agent on a computer.

To disable WRT:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Disable Web Reputation Technology** link. The Web Protection Module – Disable Web Reputation Technology task window appears.

FIGURE 1-21. Web Protection Module - Disable Web Reputation Technology page



Web Protection Module - Disable Web Reputation Technology

Web Protection Module

Description

The Web Reputation Technology (WRT) is designed to block access attempts to potentially malicious web sites in real-time. WRT is currently enabled for the listed computers.

Use the action below to disable WRT.

Actions

- Click here to disable web reputation technology.

Reference #5

Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions box. The Take Action window appears.
4. Select the computer or computers in the window and click **OK**. The Private Key Password window appears.

5. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your change. When it is finished, the status shows **Completed**.

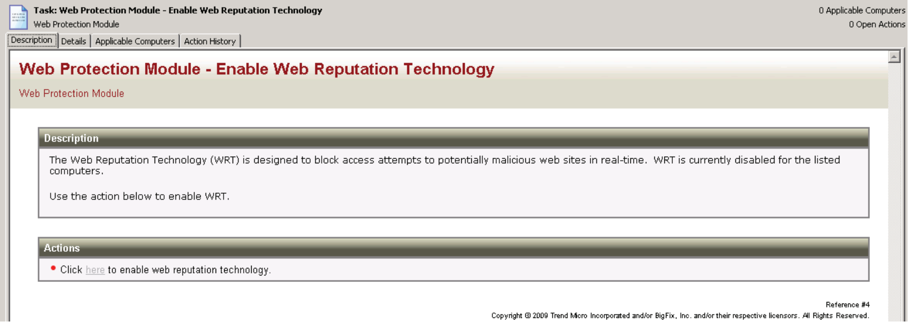
Enabling Web Reputation Technology

You can enable Trend Micro Web Reputation Technology (WRT) for one or more endpoints.

Complete the steps that follow:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Enable Web Reputation Technology** link. The Web Protection Module – Enable Web Reputation Technology task window appears.

FIGURE 1-22. Web Protection Module – Enable Web Reputation Technology page



Web Protection Module - Enable Web Reputation Technology

Web Protection Module

Description

The Web Reputation Technology (WRT) is designed to block access attempts to potentially malicious web sites in real-time. WRT is currently disabled for the listed computers.

Use the action below to enable WRT.

Actions

- Click here to enable web reputation technology.

Reference #4

Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions window. The Take Action window appears.
4. Select the computer or computers in the window and click **OK**. The Private Key Password window appears.
5. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your change. When it is finished, the status shows **Completed**.

Configuring the Web Reputation Technology Security Level

Trend Micro Web Protection Module enables you to set security levels for your endpoints. You can choose one of the following settings for each endpoint or group of endpoints:

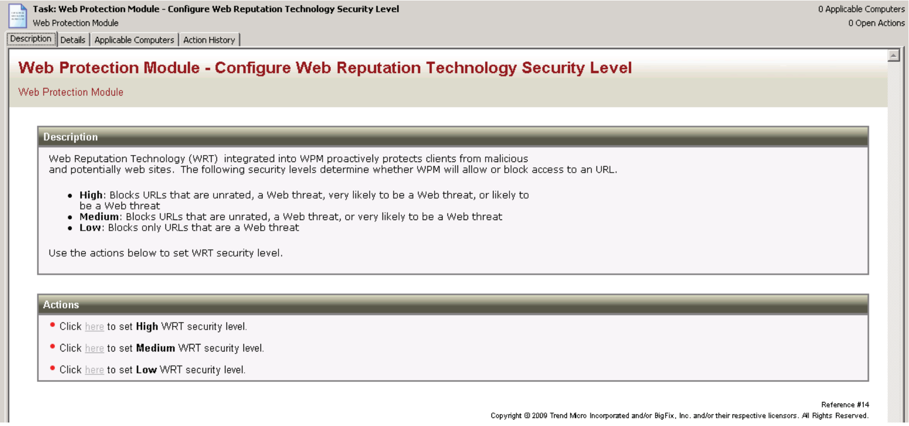
TABLE 1-1.

High	Blocks URLs that have a malicious payload, those that are very likely to have a malicious payload, and those that are likely to have a malicious payload.
Medium	Blocks URLs that have not yet been evaluated, those that have a malicious payload, and those that are very likely to have a malicious payload.
Low	Blocks only those URLs that contain a malicious payload.

To set the WRT security level for one or more of your endpoints:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Configure Web Reputation Technology Security Level** link. The Web Protection Module – Configure Web Reputation Technology Security Level Task window appears.

FIGURE 1-23. Web Protection Module – Configure Web Reputation Technology Security Level page



Web Protection Module - Configure Web Reputation Technology Security Level

Web Protection Module

Description

Web Reputation Technology (WRT) integrated into WPM proactively protects clients from malicious and potentially web sites. The following security levels determine whether WPM will allow or block access to an URL.

- **High**: Blocks URLs that are unrated, a Web threat, very likely to be a Web threat, or likely to be a Web threat
- **Medium**: Blocks URLs that are unrated, a Web threat, or very likely to be a Web threat
- **Low**: Blocks only URLs that are a Web threat

Use the actions below to set WRT security level.

Actions

- Click here to set **High** WRT security level.
- Click here to set **Medium** WRT security level.
- Click here to set **Low** WRT security level.

Reference #14

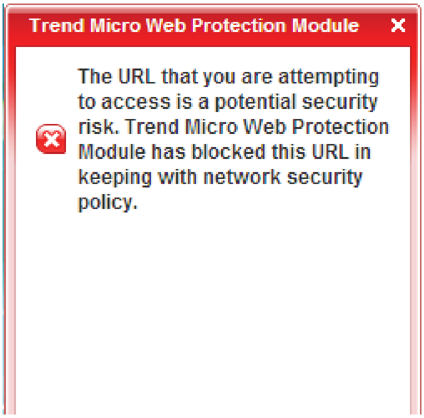
Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. In the Actions box, click the **here** link for the security level you want to set. The Take Action window appears.
4. Select the computer or computers to which you want to apply the security level in the window and click **OK**. The Private Key Password window appears.
5. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your change. When it is finished, the status shows **Completed**.

Enabling Alert Notification for Detected Threats

This feature is turned off by default when you install the Web Protection Agent on a computer. The Web Protection Agent can display a pop-up notification in addition to the browser notification normally displayed each time it detects a threat. This feature is helpful if individuals in your environment use something other than a Web browser to access potentially bad sites. When activated, this feature displays a pop-up window like the one that follows that appears for 30 seconds in the lower left corner of the screen whenever the Agent detects a threat.

FIGURE 1-24. Threat Detection screen



Trend Micro Web Protection Module

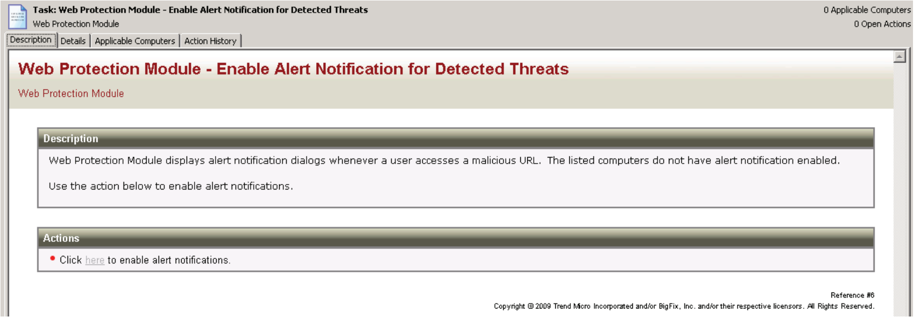
The URL that you are attempting to access is a potential security risk. Trend Micro Web Protection Module has blocked this URL in keeping with network security policy.

Note: Threat events are also recorded in the logs. See the sections on *Log Maintenance* and *Viewing Analyses* for more information.

To enable alert notification:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Enable Alert Notification for Detected Threats** link. The Web Protection Module – Enable Alert Notifications for Detected Threats task window appears.

FIGURE 1-25. Web Protection Module – Enable Alert Notifications for Detected Threats page



Task: Web Protection Module - Enable Alert Notification for Detected Threats
Web Protection Module

0 Applicable Computers
0 Open Actions

Web Protection Module - Enable Alert Notification for Detected Threats

Web Protection Module

Description

Web Protection Module displays alert notification dialogs whenever a user accesses a malicious URL. The listed computers do not have alert notification enabled.

Use the action below to enable alert notifications.

Actions

- Click here to enable alert notifications.

Reference #6
Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions window. The Take Action window appears.
4. Select the computer or computers in the window and click **OK**. The Private Key Password window appears.
5. Enter your Private Key Password and click **OK**. An Action window appears, in which you can track the progress of your change. When it is finished, the status shows **Completed**.

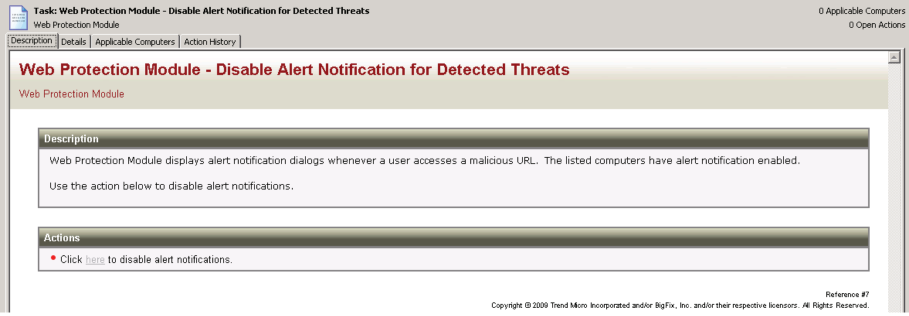
Disabling Alert Notification for Detected Threats

You can also disable alert notifications for detected threats.

To disable alert notification:

1. From the Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Disable Alert Notification for Detected Threats** link. The Web Protection Module – Disable Alert Notifications for Detected Threats task window appears.

FIGURE 1-26. Web Protection Module – Disable Alert Notifications for Detected Threats page



Task: Web Protection Module - Disable Alert Notification for Detected Threats
Web Protection Module

0 Applicable Computers
0 Open Actions

Web Protection Module - Disable Alert Notification for Detected Threats

Web Protection Module

Description

Web Protection Module displays alert notification dialogs whenever a user accesses a malicious URL. The listed computers have alert notification enabled.

Use the action below to disable alert notifications.

Actions

- Click here to disable alert notifications.

Reference #7

Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions window. The Take Action window appears.
4. Select the computer or computers in the window for which you want to disable the notification pop-up and click **OK**. The Private Key Password window appears.
5. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your change. When it is finished, the status shows **Completed**.

Uploading Logs

Use this task to upload the current and archived Web threat (urlthreats.txt) and URL history (`urlhist.txt`) logs stored on the selected endpoints to the ESP server.

This task is useful for archiving or using a third-party tool to perform analyses on your endpoint logs. When you use this task, the Web Protection Agent uploads copies of the logs to the following directory on the ESP server and deletes them from the endpoint:

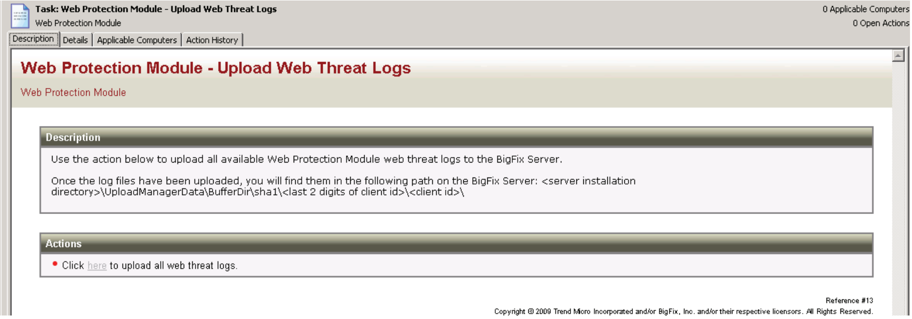
```
<server installation directory>\UploadManagerData\BufferDir\
sha1\<last 2 digits of the client id>\<client id>\
```

To see the client ID for an individual endpoint, see the Properties area of the Computer Summary tab.

To upload logs to the ESP server:

1. From the ESP Tasks Navigation bar, click the **View Applicable Web Protection Module Tasks** link. The Web Protection Module Task window appears.
2. In the List Panel, click the **Web Protection Module – Upload Web Threat Logs** link. The Web Protection Module – Upload Web Threat Logs task window appears.

FIGURE 1-27. Web Protection Module – Upload Web Threat Logs page



Task: Web Protection Module - Upload Web Threat Logs
Web Protection Module

0 Applicable Computers
0 Open Actions

Web Protection Module - Upload Web Threat Logs

Web Protection Module

Description

Use the action below to upload all available Web Protection Module web threat logs to the BigFix Server.

Once the log files have been uploaded, you will find them in the following path on the BigFix Server: <server installation directory>\UploadManagerData\BufferDir\sha1\<last 2 digits of client id>\<client id>\

Actions

- Click here to upload all web threat logs.

Reference #13
Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

3. Click the **here** link in the Actions window. The Take Action window appears.
4. Select the computer or computers in the window containing the logs you want to upload and click **OK**. The Private Key Password window appears.
5. Enter your Private Key Password and click **OK**. An Action window appears in which you can track the progress of your change. When it is finished, the status shows **Completed**.

Chapter 2

Using Trend Micro Web Protection Module

This section provides instructions on using the Web Protection Module.

This chapter covers the following topics:

- *Blacklist and Whitelist Policies*
- *Support*
- *FAQs*

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 user's Web access. After you have defined these policies, you use them to create Custom Tasks that you can then apply to your endpoints.

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

- **Blacklists** – These are lists of blocked Web sites. If the endpoint tries to access a site on one of these lists, it receives a message in its Web browser indicating that access to the site has been blocked.
- **Whitelists** – These are lists of Web sites that you allow your endpoints to access without restriction.

Note: Use care when selecting sites for Whitelists. After 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

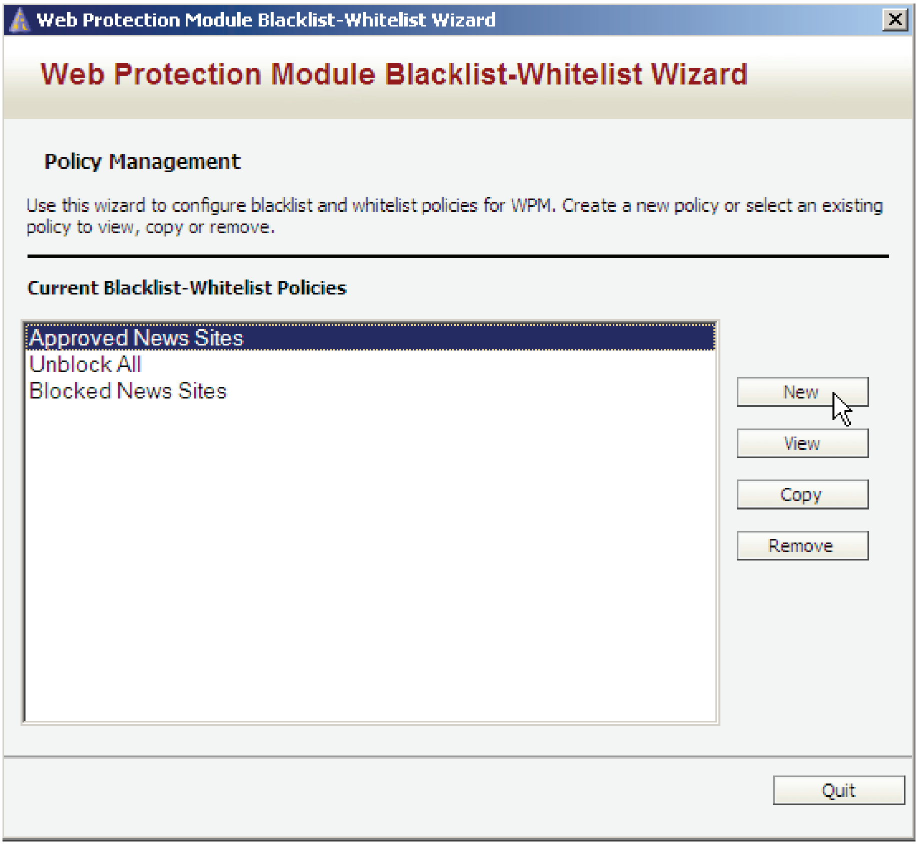
This section describes how to create and deploy a new blacklist/whitelist policy.

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 ESP Console menu bar.

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

FIGURE 2-28. Blacklist-Whitelist Wizard Policy Management window



Web Protection Module Blacklist-Whitelist Wizard

Web Protection Module Blacklist-Whitelist Wizard

Policy Management

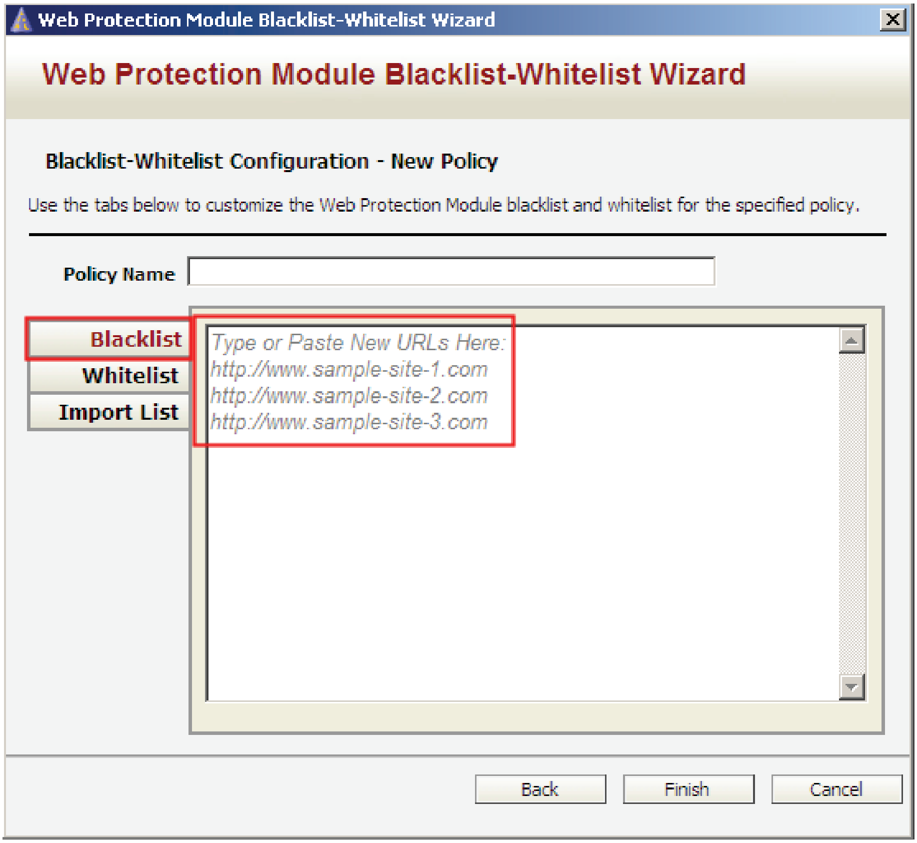
Use this wizard to configure blacklist and whitelist policies for WPM. Create a new policy or select an existing policy to view, copy or remove.

Current Blacklist-Whitelist Policies

Approved News Sites
Unblock All
Blocked News Sites

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

FIGURE 2-29. Blacklist-Whitelist Configuration – New Policy window



Web Protection Module Blacklist-Whitelist Wizard

Web Protection Module Blacklist-Whitelist Wizard

Blacklist-Whitelist Configuration - New Policy

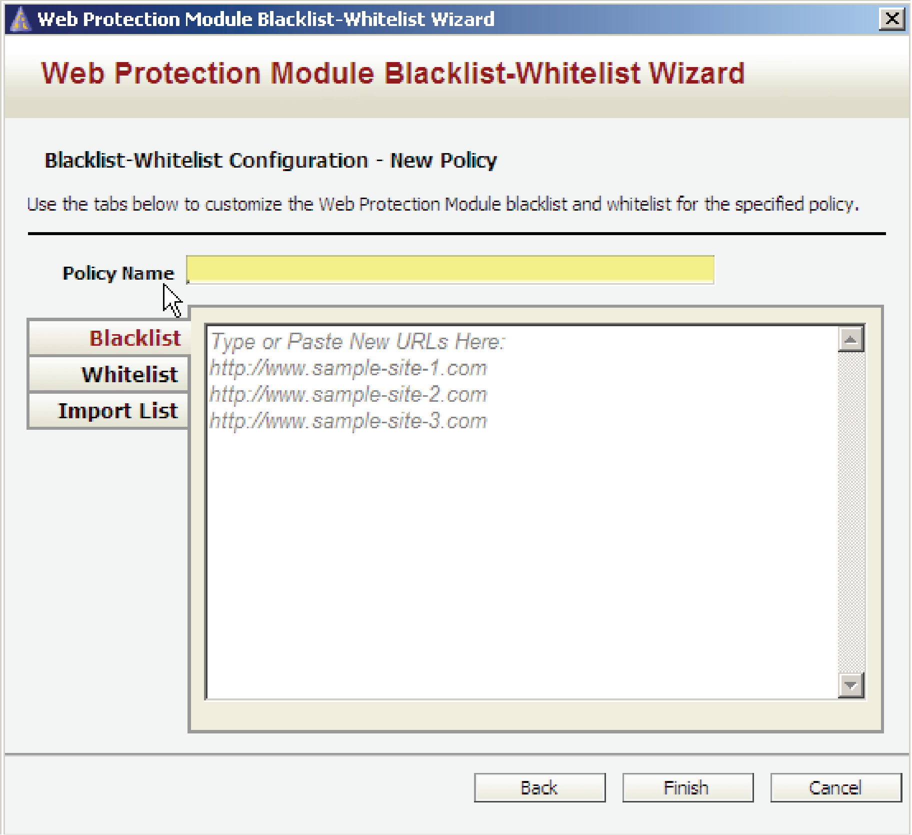
Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name

Type or Paste New URLs Here:
http://www.sample-site-1.com
http://www.sample-site-2.com
http://www.sample-site-3.com

3. Enter a name for your policy in the Policy Name field.

FIGURE 2-30. Policy Name field



Web Protection Module Blacklist-Whitelist Wizard

Blacklist-Whitelist Configuration - New Policy

Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name

Type or Paste New URLs Here:
http://www.sample-site-1.com
http://www.sample-site-2.com
http://www.sample-site-3.com

4. In the Blacklist pane below the Policy Name field, enter, copy or paste the URLs you want to block. You can 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/*`

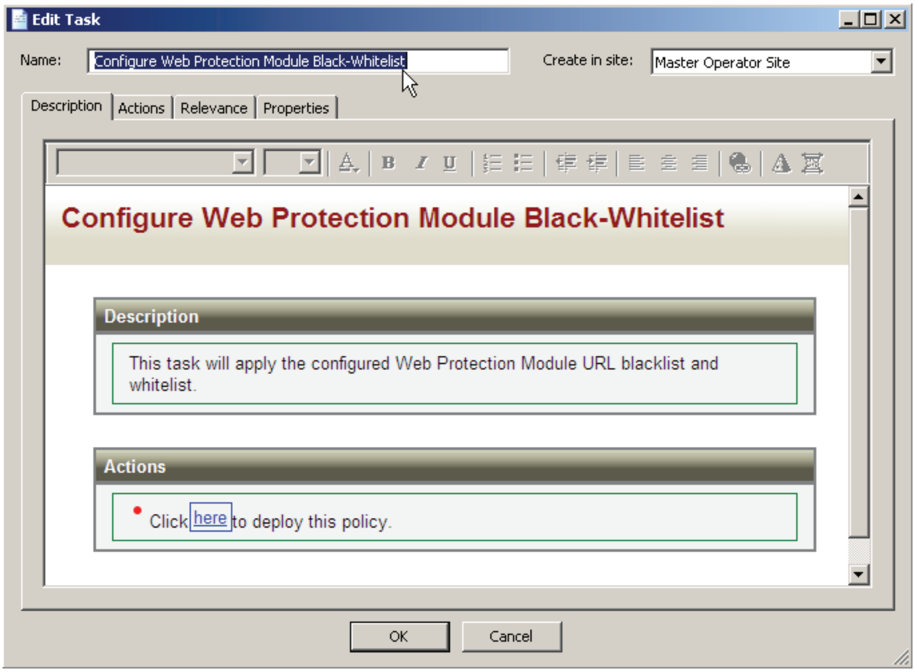
Note: You can block as many as 500 URLs per policy. If you wish to block more, create a different policy for each category of URLs you want to block.

Note: If you do not want to include a Whitelist in the policy, you can 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 and paste the URLs you want your users to be able to access without restriction. You can 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.

FIGURE 2-31. Edit Task window



Configure Web Protection Module Black-Whitelist

Description

This task will apply the configured Web Protection Module URL blacklist and whitelist.

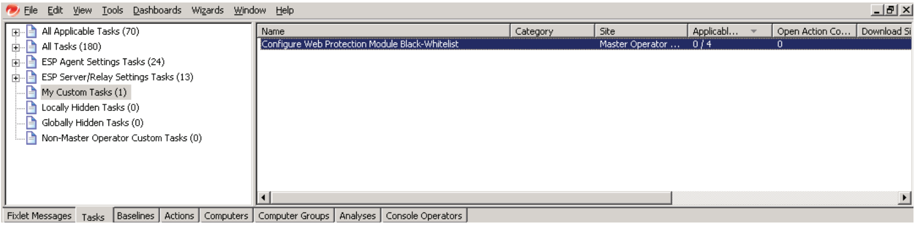
Actions

- Click here to deploy this policy.

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**.

11. In the Filter Panel, click **My Custom Tasks**. Your new Blacklist / Whitelist policy appears in the List Panel.

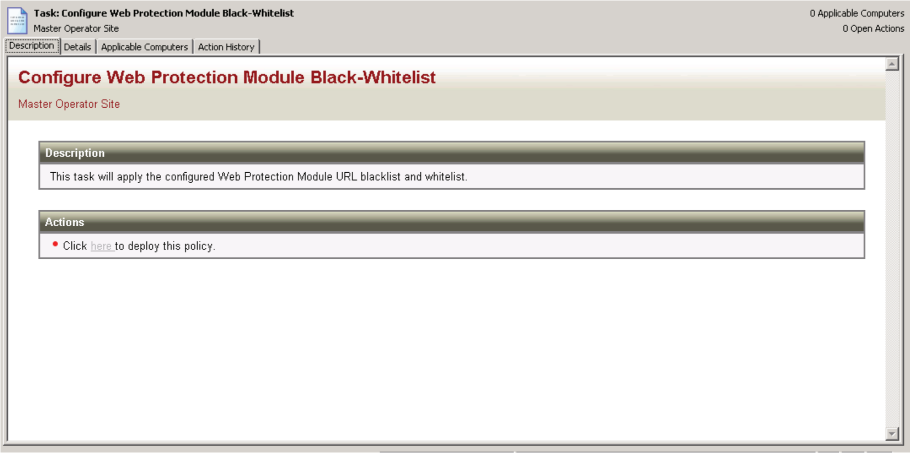
FIGURE 2-32. List Panel screen



Name	Category	Site	Applicabl...	Open Action Co...	Download Si
Configure Web Protection Module Black-Whitelist		Master Operator ...	0 / 4	0	

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

FIGURE 2-33. Task Pane screen



Task: Configure Web Protection Module Black-Whitelist
Master Operator Site

0 Applicable Computers
0 Open Actions

Configure Web Protection Module Black-Whitelist

Master Operator Site

Description

This task will apply the configured Web Protection Module URL blacklist and whitelist.

Actions

- Click here to deploy this policy.

13. Click the **here** link in the Actions window. The Take Action window appears.
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, and so on).
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 ESP 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 enabled in your browser. If you do not have this feature enabled, you will receive an error when you try to browse to a file. For more information, check the link that follows:

`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.

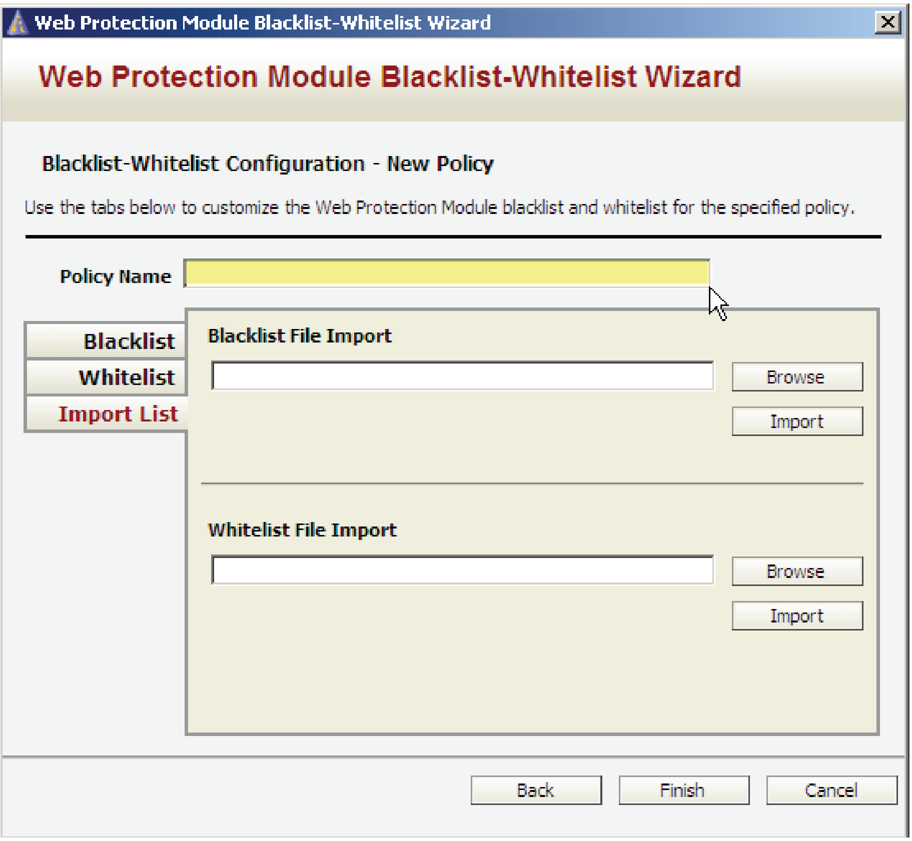
Note: If you do not want to include a Whitelist in the policy, you can skip this part of the process. The Web Protection Module allows you to create Blacklist / Whitelist policies with both list types (a Blacklist and a Whitelist), only a Blacklist, or only a Whitelist.

---

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 ESP Console menu bar. The Blacklist-Whitelist Wizard Policy Management window appears.
4. Click **New**. The Blacklist-Whitelist Configuration – New Policy window appears.

5. Click the **Import List** tab. The Import List pane appears.

FIGURE 2-34. Import List tab



Web Protection Module Blacklist-Whitelist Wizard

Web Protection Module Blacklist-Whitelist Wizard

Blacklist-Whitelist Configuration - New Policy

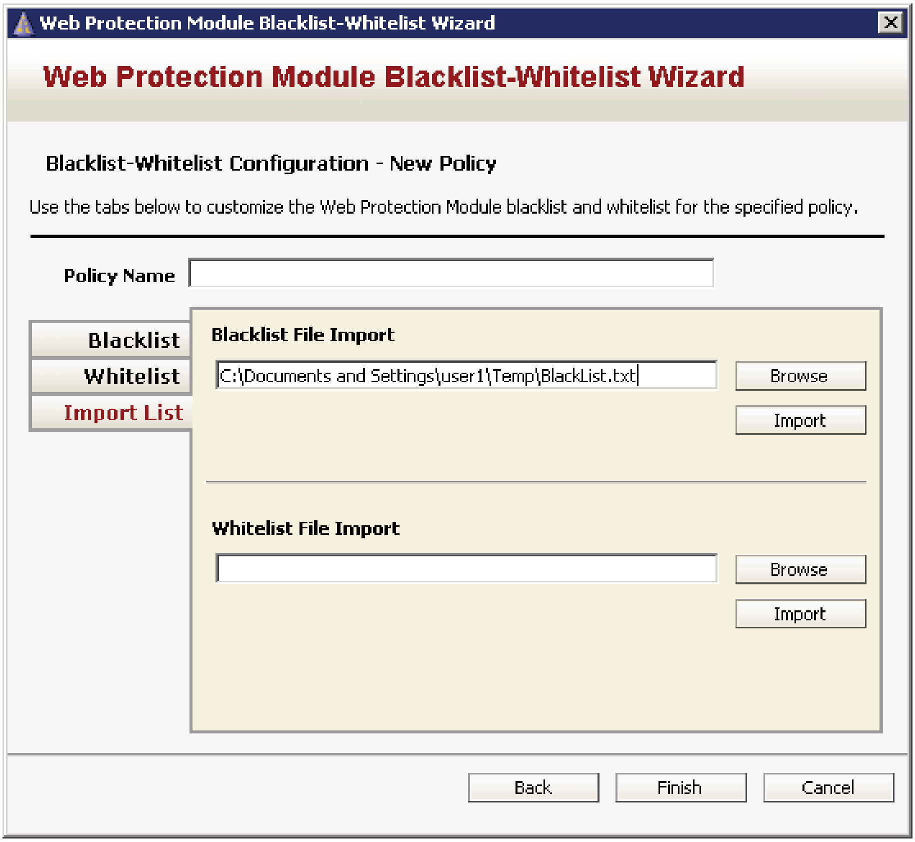
Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name

6. Enter the name for the new policy in the Policy Name field.
7. 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.
8. Use the Open window to navigate to the location where you have the text file.

9. Select the file and click **Open**. The path to the selected file appears in the Import pane.

FIGURE 2-35. Import List pane



Web Protection Module Blacklist-Whitelist Wizard

Web Protection Module Blacklist-Whitelist Wizard

Blacklist-Whitelist Configuration - New Policy

Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name

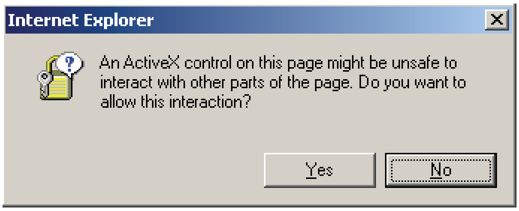
Blacklist File Import

C:\Documents and Settings\user1\Temp\BlackList.txt

Whitelist File Import

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

FIGURE 2-36. ActiveX Warning message

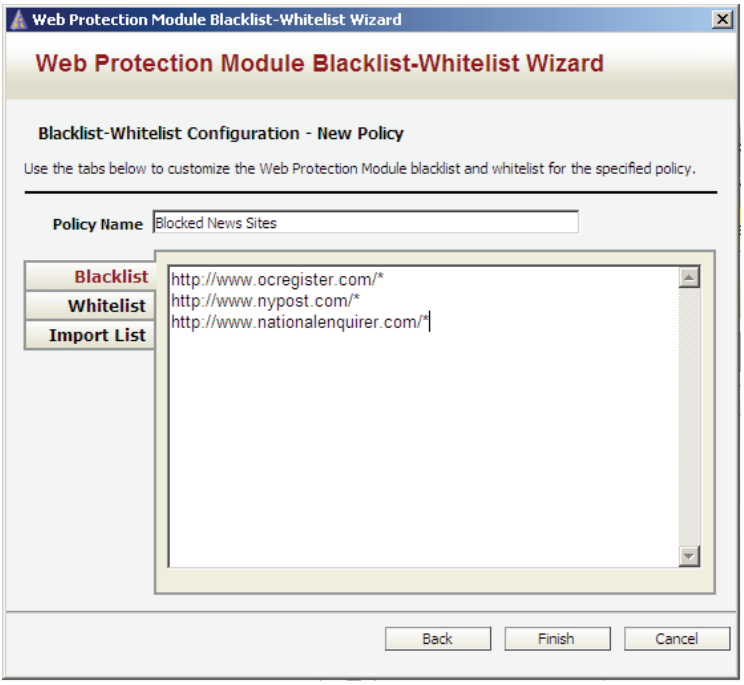


An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

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

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

FIGURE 2-37. Blacklist / Whitelist Wizard


Web Protection Module Blacklist-Whitelist Wizard
Web Protection Module Blacklist-Whitelist Wizard
Blacklist
Whitelist
Import List
Back
Finish
Cancel

Blacklist-Whitelist Configuration - New Policy

Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name: Blocked News Sites

```
http://www.ocregister.com/*
http://www.nypost.com/*
http://www.nationalenquirer.com/*
```

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 deploying the policy, see Steps 7-16 in the Creating and Deploying a New Blacklist / Whitelist Policy section.

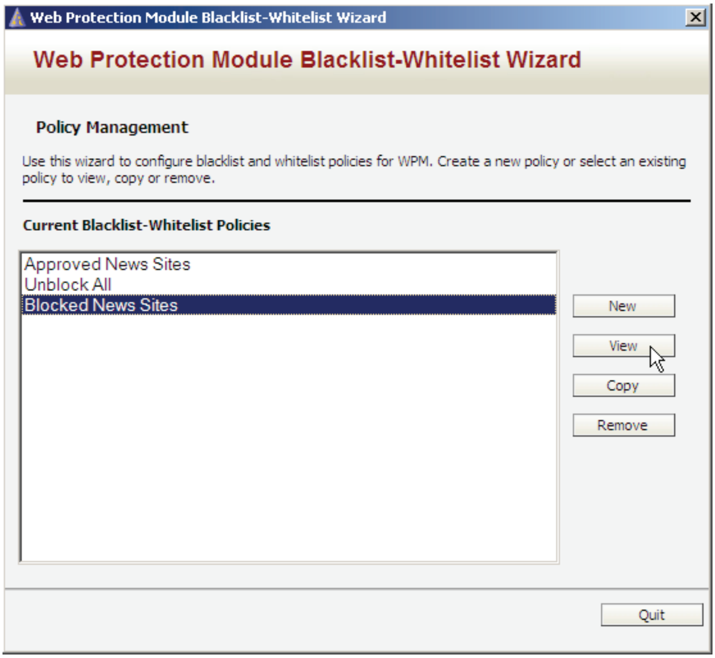
Viewing an Existing Policy

You can also view 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 ESP Console menu bar. The Blacklist-Whitelist Wizard Policy Management window appears:

FIGURE 2-38. Blacklist-Whitelist Wizard Policy Management window



Web Protection Module Blacklist-Whitelist Wizard

Web Protection Module Blacklist-Whitelist Wizard

Policy Management

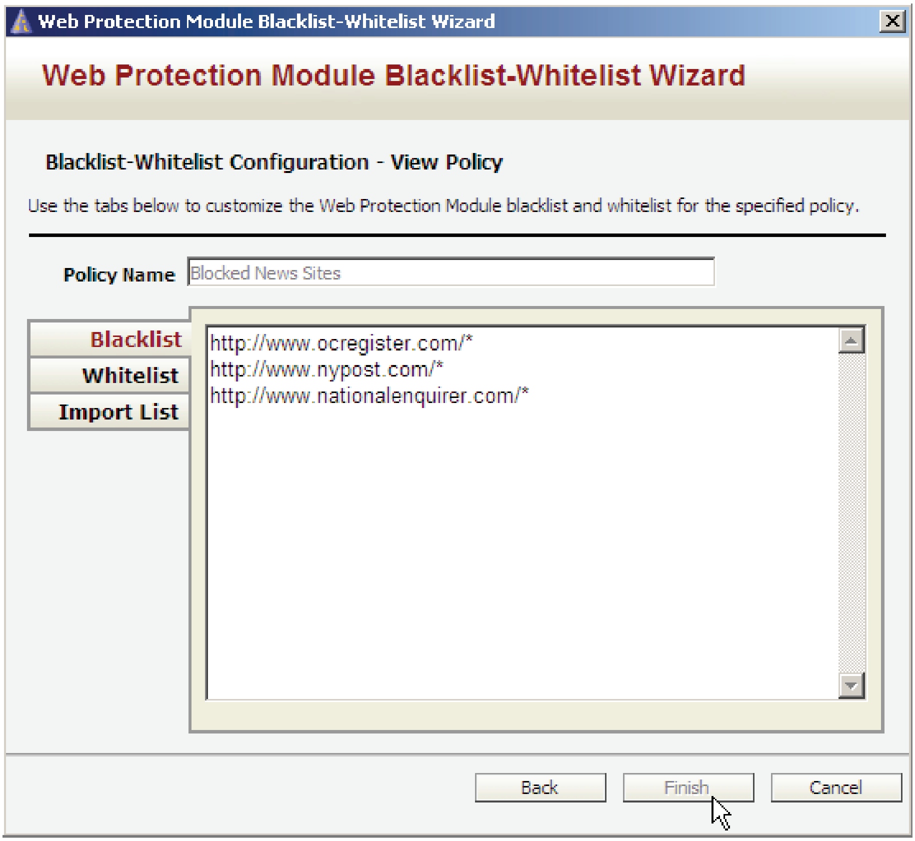
Use this wizard to configure blacklist and whitelist policies for WPM. Create a new policy or select an existing policy to view, copy or remove.

Current Blacklist-Whitelist Policies

Approved News Sites
Unblock All
Blocked News Sites

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

FIGURE 2-39. Blacklist-Whitelist Configuration – View Policy window


Web Protection Module Blacklist-Whitelist Wizard
Web Protection Module Blacklist-Whitelist Wizard
Blacklist-Whitelist Configuration - View Policy
Blacklist
Whitelist
Import List
Back
Finish
Cancel

Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name: Blocked News Sites

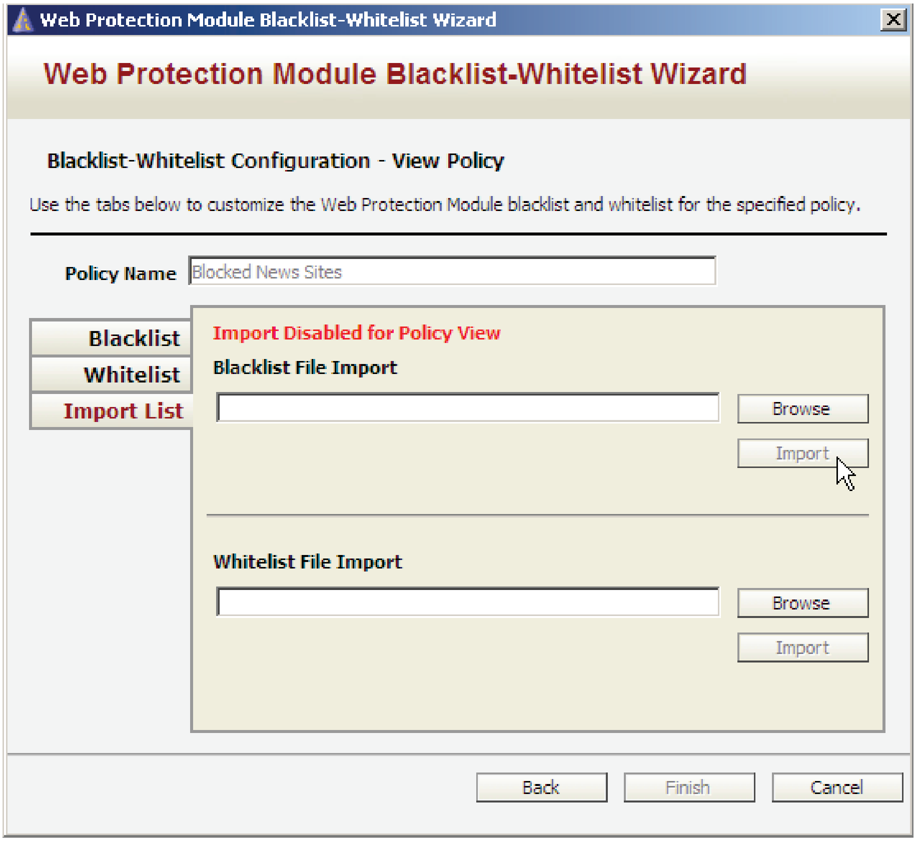
http://www.ocregister.com/*
http://www.nypost.com/*
http://www.nationalenquirer.com/*

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 you cannot make any changes.

3. You can 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 **Back**. (In this case, the Import List feature is disabled).

FIGURE 2-40. View Policy page



Web Protection Module Blacklist-Whitelist Wizard

Web Protection Module Blacklist-Whitelist Wizard

Blacklist-Whitelist Configuration - View Policy

Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name: Blocked News Sites

Import Disabled for Policy View

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

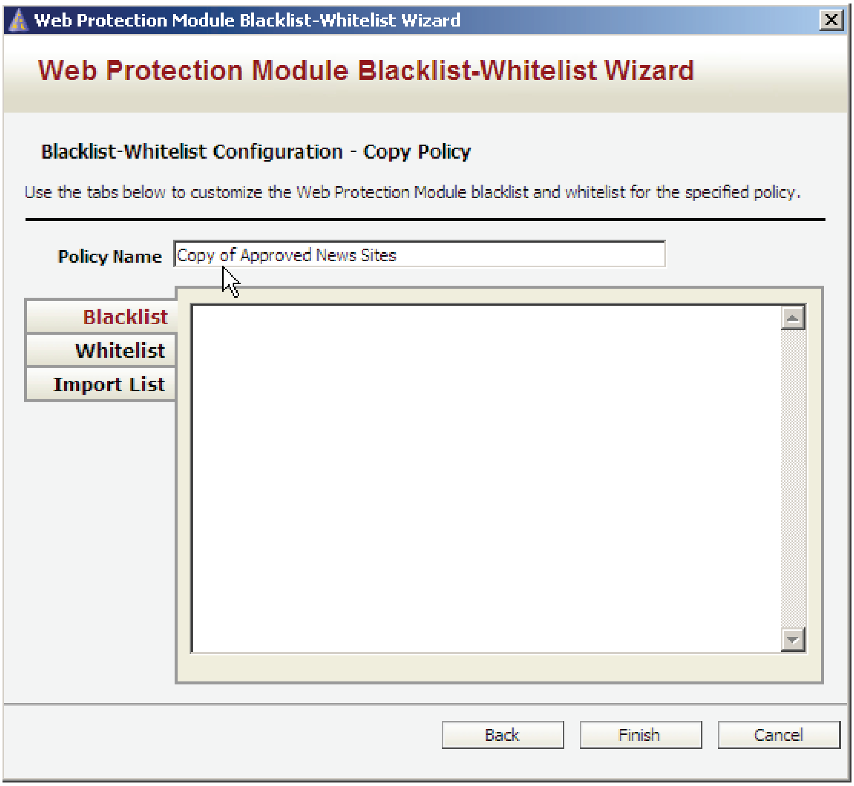
Copying and Editing a Policy

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 ESP Console menu bar. The Blacklist-Whitelist Wizard Policy Management window appears.
2. Select the name of the Blacklist / Whitelist policy you want to duplicate and click **Copy**. The Blacklist-Whitelist Configuration – Copy Policy window appears.

FIGURE 2-41. Blacklist-Whitelist Configuration – Copy Policy window



Web Protection Module Blacklist-Whitelist Wizard

Web Protection Module Blacklist-Whitelist Wizard

Blacklist-Whitelist Configuration - Copy Policy

Use the tabs below to customize the Web Protection Module blacklist and whitelist for the specified policy.

Policy Name: Copy of Approved News Sites

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 to start generating the relevant Custom Action.

Note: To see the process required to finish generating your Custom Action and deploying the policy, see Steps 7-16 in the Creating and Deploying a New Blacklist / Whitelist Policy section described previously.

Editing Custom Actions

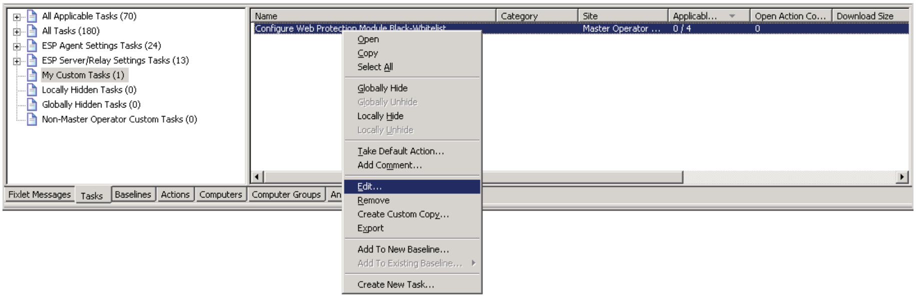
The Blacklist / Whitelist Wizard does NOT allow you to edit existing Blacklist / Whitelist policies. (You can only make modifications to new copies of policies, not the originals.) If necessary, however, you can edit the Custom Actions the Wizard generates.

You can 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 the Custom Task generation process or select it by right-clicking on the name of an existing Custom Task and selecting **Edit**.

FIGURE 2-42. Edit a Custom Task pull-down

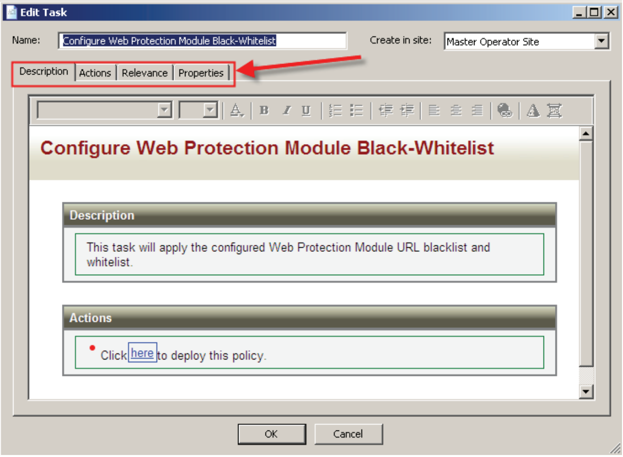


Name	Category	Site	Applicabl...	Open Action Co...	Download Size
Configure Web Protection Module Black-Whitelist		Master Operator ...	0 / 4	0	

The Edit Task window consists of four tabs:

- Description
- Actions
- Relevance
- Properties

FIGURE 2-43. Edit Task tabs



Edit Task

Name: Configure Web Protection Module Black-Whitelist

Create in site: Master Operator Site

Configure Web Protection Module Black-Whitelist

Description

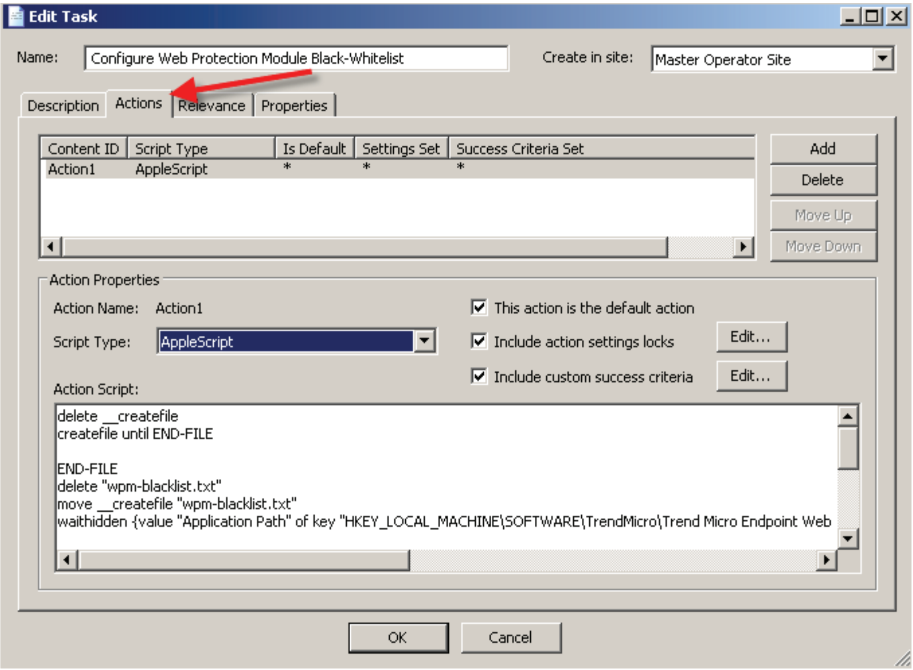
This task will apply the configured Web Protection Module URL blacklist and whitelist.

Actions

- Click here to deploy this policy.

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.

FIGURE 2-44. Actions tab



Edit Task

Name: Configure Web Protection Module Black-Whitelist

Create in site: Master Operator Site

Content ID	Script Type	Is Default	Settings Set	Success Criteria Set
Action1	AppleScript	*	*	*

Action Properties

Action Name: Action1

Script Type: AppleScript

☑ This action is the default action

☑ Include action settings locks

☑ Include custom success criteria

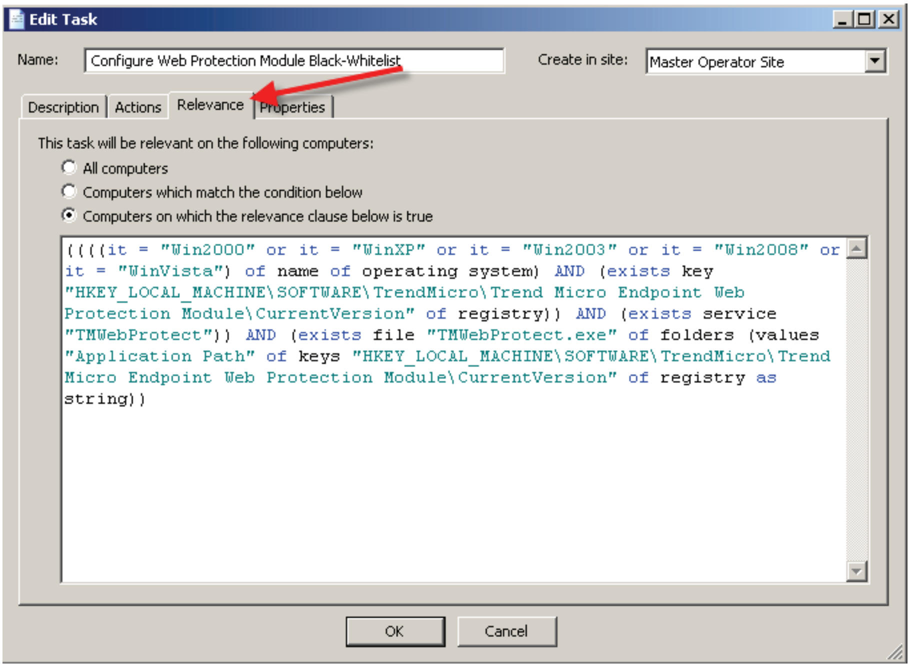
Action Script:

```
delete __createfile
createfile until END-FILE

END-FILE
delete "wpm-blacklist.txt"
move __createfile "wpm-blacklist.txt"
waithidden {value "Application Path" of key "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Trend Micro Endpoint Web
```

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

FIGURE 2-45. Relevance tab



Name: Configure Web Protection Module Black-Whitelist

Create in site: Master Operator Site

This task will be relevant on the following computers:

○ All computers

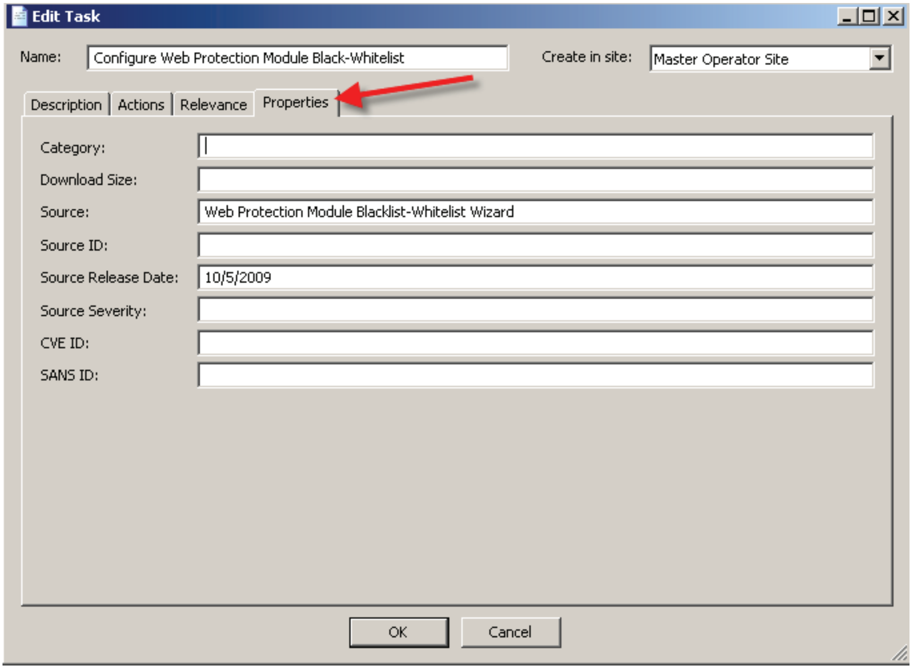
○ Computers which match the condition below

● Computers on which the relevance clause below is true

```
((((it = "Win2000" or it = "WinXP" or it = "Win2003" or it = "Win2008" or
it = "WinVista") of name of operating system) AND (exists key
"HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Trend Micro Endpoint Web
Protection Module\CurrentVersion" of registry)) AND (exists service
"TMWebProtect")) AND (exists file "TMWebProtect.exe" of folders (values
"Application Path" of keys "HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Trend
Micro Endpoint Web Protection Module\CurrentVersion" of registry as
string))
```

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

FIGURE 2-46. Properties tab



Edit Task

Name: Configure Web Protection Module Black-Whitelist

Create in site: Master Operator Site

Category:

Download Size:

Source: Web Protection Module Blacklist-Whitelist Wizard

Source ID:

Source Release Date: 10/5/2009

Source Severity:

CVE ID:

SANS ID:

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

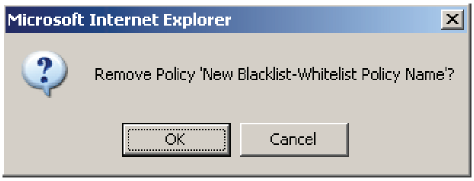
Complete the steps that follow to delete an existing Blacklist / Whitelist policy from the Wizard's Policy Management list.

To delete a policy:

1. Click **Wizards > Web Protection Module Blacklist-Whitelist Wizard** to access the Web Protection Module Blacklist-Whitelist Wizard from the ESP 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.

FIGURE 2-47. Remove window



Microsoft Internet Explorer

Remove Policy 'New Blacklist-Whitelist Policy Name'?

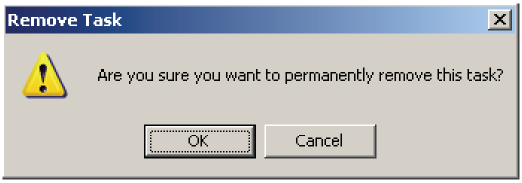
3. Click **OK**. The Web Protection Module removes the policy from the Blacklist-Whitelist Wizard Policy Management window.
4. Click **Quit** to exit the Wizard.

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, complete the steps that follow.

---

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.

FIGURE 2-48. Remove Task window



Remove Task

Are you sure you want to permanently remove this task?

7. Click **OK**. The Private Key Password window appears.
8. Enter your Private Key Password and click **OK**. ESP 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, Trend Micro 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:

TABLE 2-2.

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

TABLE 2-2.

FIELD NAME	FIELD DESCRIPTION
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:

TABLE 2-3.

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

The following section describes how to view and analyze client information.

To view a client information analyses:

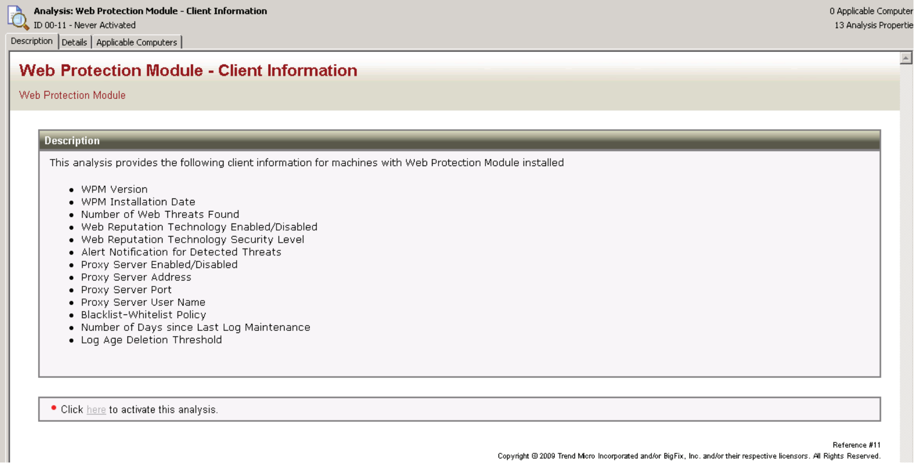
1. Click the **Analyses** tab. The List Panel changes to show all available analyses.
2. Click **All Applicable Analyses**.
3. Click the "+" sign and then click **By Site**.
4. Click **Web Protection Module**.

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.

FIGURE 2-49. Web Protection Module – Client Information window



Analysis: Web Protection Module - Client Information
ID 00-11 - Never Activated

0 Applicable Computer
13 Analysis Propertie

Web Protection Module - Client Information

Web Protection Module

Description

This analysis provides the following client information for machines with Web Protection Module installed

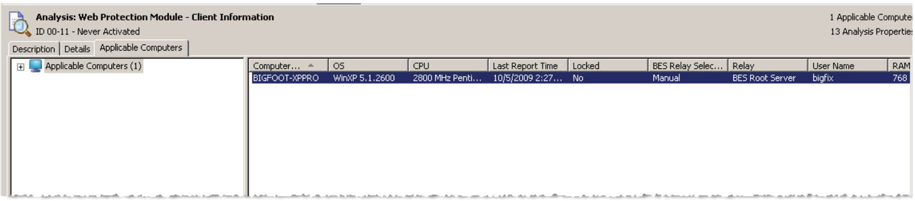
- WPM Version
- WPM Installation Date
- Number of Web Threats Found
- Web Reputation Technology Enabled/Disabled
- Web Reputation Technology Security Level
- Alert Notification for Detected Threats
- Proxy Server Enabled/Disabled
- Proxy Server Address
- Proxy Server Port
- Proxy Server User Name
- Blacklist-Whitelist Policy
- Number of Days since Last Log Maintenance
- Log Age Deletion Threshold

• Click here to activate this analysis.

Reference #11
Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

6. To view the details about each property, click the **Applicable Computers** tab.

FIGURE 2-50. Applicable Computers tab



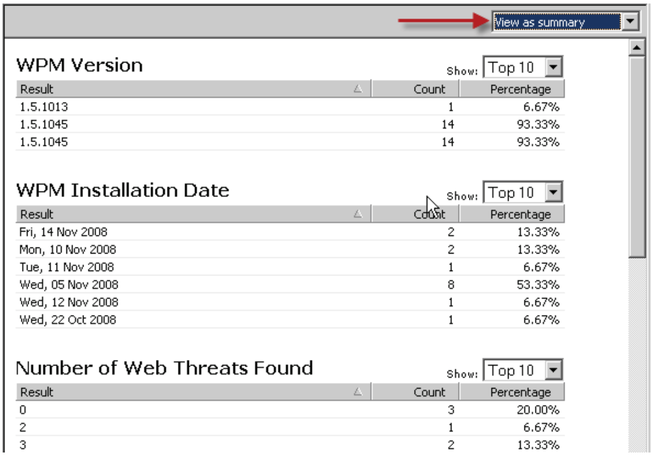
Analysis: Web Protection Module - Client Information
ID 00-11 - Never Activated

1 Applicable Compute
13 Analysis Propertie

Computer...	OS	CPU	Last Report Time	Locked	BES Relay Selec...	Relay	User Name	RAM
BIGFOOT-XPPRO	WinXP 5.1.2600	2800 MHz Penti...	10/5/2009 2:27...	No	Manual	BES Root Server	bigfix	768

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.

FIGURE 2-51. View as Summary option



WPM Version

Show: Top 10

Result	Count	Percentage
1.5.1013	1	6.67%
1.5.1045	14	93.33%
1.5.1045	14	93.33%

WPM Installation Date

Show: Top 10

Result	Count	Percentage
Fri, 14 Nov 2008	2	13.33%
Mon, 10 Nov 2008	2	13.33%
Tue, 11 Nov 2008	1	6.67%
Wed, 05 Nov 2008	8	53.33%
Wed, 12 Nov 2008	1	6.67%
Wed, 22 Oct 2008	1	6.67%

Number of Web Threats Found

Show: Top 10

Result	Count	Percentage
0	3	20.00%
2	1	6.67%
3	2	13.33%

7. If you wish to deactivate the analysis, return to the click **here** link in the Action window.

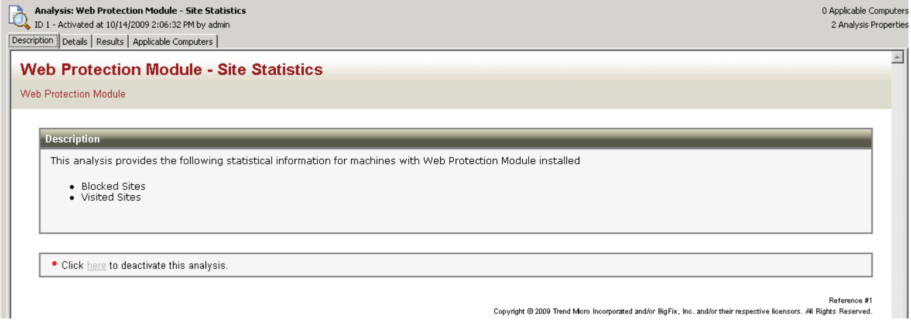
Viewing the Site Statistics Analysis

You can also view the site statistics analysis.

To view the site statistics analysis:

1. Click the **Analyses** tab.
2. The List Panel shows all available analyses.
3. Click **All Applicable Analyses**.
4. Click the "**+**" sign and then click **By Site**.
5. Click **Web Protection Module**. The Web Protection Module presents you with a list of both available analyses.
6. 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

FIGURE 2-52. Web Protection Agent properties



Analysis: Web Protection Module - Site Statistics
ID 1 - Activated at 10/14/2009 2:06:32 PM by admin

0 Applicable Computers
2 Analysis Properties

Web Protection Module - Site Statistics

Web Protection Module

Description

This analysis provides the following statistical information for machines with Web Protection Module installed

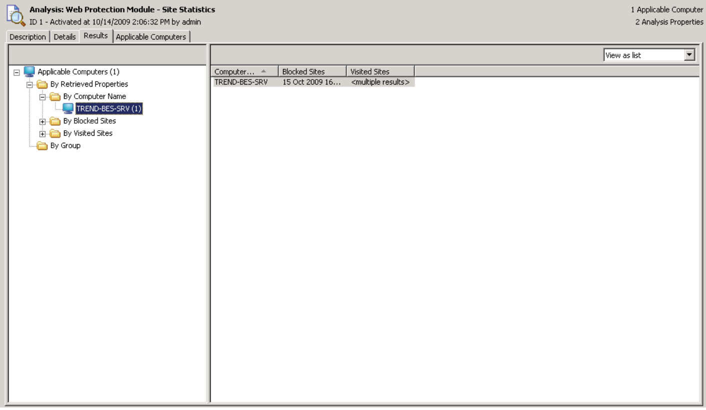
- Blocked Sites
- Visited Sites

- Click here to deactivate this analysis.

Reference #1
Copyright © 2009 Trend Micro Incorporated and/or BigFix, Inc. and/or their respective licensors. All Rights Reserved.

7. To view the details of each property, click the **Results** tab.

FIGURE 2-53. Results tab



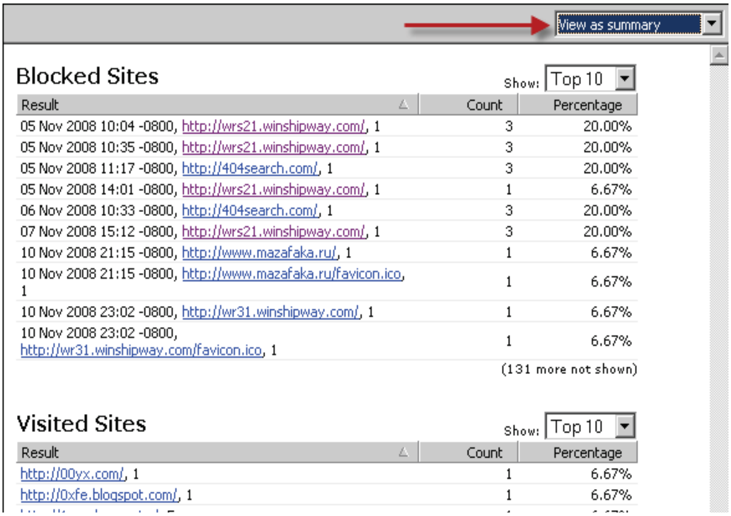
Analysis: Web Protection Module - Site Statistics
ID 1 - Activated at 10/14/2009 2:06:32 PM by admin

1 Applicable Computer
2 Analysis Properties

Computer...	Blocked Sites	Visited Sites
TREND-BES-SRV	15 Oct 2009 16...	<multiple results>

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.

FIGURE 2-54. Blocked/Visited Sites page



Blocked Sites

Show: Top 10

Result	Count	Percentage
05 Nov 2008 10:04 -0800, http://wrs21.winshipway.com/, 1	3	20.00%
05 Nov 2008 10:35 -0800, http://wrs21.winshipway.com/, 1	3	20.00%
05 Nov 2008 11:17 -0800, http://404search.com/, 1	3	20.00%
05 Nov 2008 14:01 -0800, http://wrs21.winshipway.com/, 1	1	6.67%
06 Nov 2008 10:33 -0800, http://404search.com/, 1	3	20.00%
07 Nov 2008 15:12 -0800, http://wrs21.winshipway.com/, 1	3	20.00%
10 Nov 2008 21:15 -0800, http://www.mazafaka.ru/, 1	1	6.67%
10 Nov 2008 21:15 -0800, http://www.mazafaka.ru/favicon.ico, 1	1	6.67%
10 Nov 2008 23:02 -0800, http://wr31.winshipway.com/, 1	1	6.67%
10 Nov 2008 23:02 -0800, http://wr31.winshipway.com/favicon.ico, 1	1	6.67%

(131 more not shown)

Visited Sites

Show: Top 10

Result	Count	Percentage
http://00yx.com/, 1	1	6.67%
http://0xfe.blogspot.com/, 1	1	6.67%

8. To deactivate the analysis, return to the click the **here** link in the Action window.

The Web Protection Module Dashboard

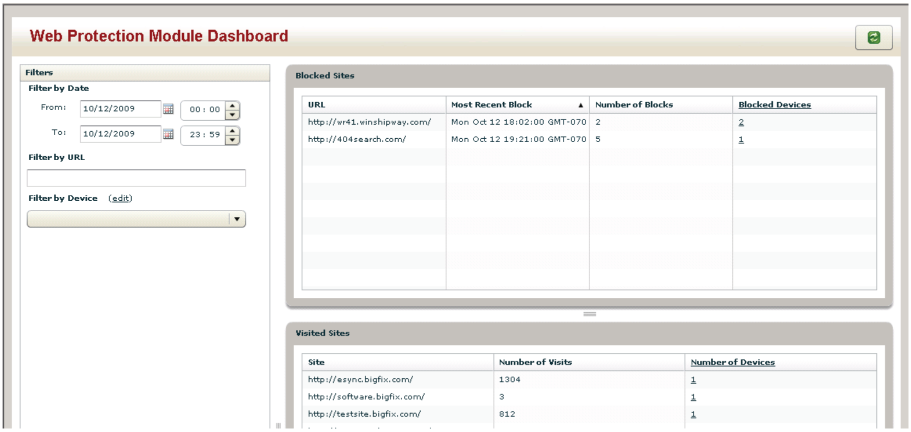
The Web Protection Module provides a dashboard that enables you to view statistics about the Web sites users' access and the number of threats that it blocks.

You can access the Dashboard in one of two ways:

1. To access the Dashboard from the ESP Console, select **Dashboards > 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.

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.

FIGURE 2-55. Web Protection Module Dashboard page



Web Protection Module Dashboard

Filters

Filter by Date

From: 10/12/2009 00 : 00

To: 10/12/2009 23 : 59

Filter by URL

Filter by Device (edit)

Blocked Sites

URL	Most Recent Block ▲	Number of Blocks	Blocked Devices
http://wr41.winshipway.com/	Mon Oct 12 18:02:00 GMT-070	2	2
http://404search.com/	Mon Oct 12 19:21:00 GMT-070	5	1

Visited Sites

Site	Number of Visits	Number of Devices
http://esync.bigfix.com/	1304	1
http://software.bigfix.com/	3	1
http://testsite.bigfix.com/	812	1

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 the information that is currently on each endpoint. If you have both a Log Maintenance and a corresponding Log Upload policy in place (which Trend Micro recommends as a best practice), historical information older than your specified aging threshold is archived on the ESP server.

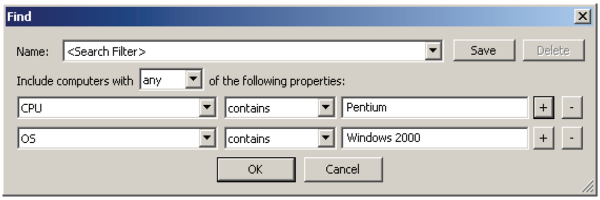
Note: To see historical information for blocked and visited sites, review the log entries in the following directory:

```
<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. After you set them, these settings enable you to do the following:

TABLE 2-4.

FILTER CATEGORY	DESCRIPTION
Filter by Date	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 a 24-hour format beginning at 00:00 hours and ending at 23:59 hours. To change the date range, you can either: • Choose each day by picking it from a calendar that you display by clicking the Calendar icon. • Enter each date manually. To change the time, you can either: • Use the arrow keys to select the appropriate hours and minutes. • Enter the times manually.
Filter by URL	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.
Filter by Device	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 ESP Console's Find feature to search for endpoints containing the specified property or properties (for example, OS, subnet, computer name, and so on). To access the Find feature, click **(edit)**. The following illustration depicts this window:  Find Name: <Search Filter> Include computers with any of the following properties: CPU contains Pentium OS contains Windows 2000

- **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

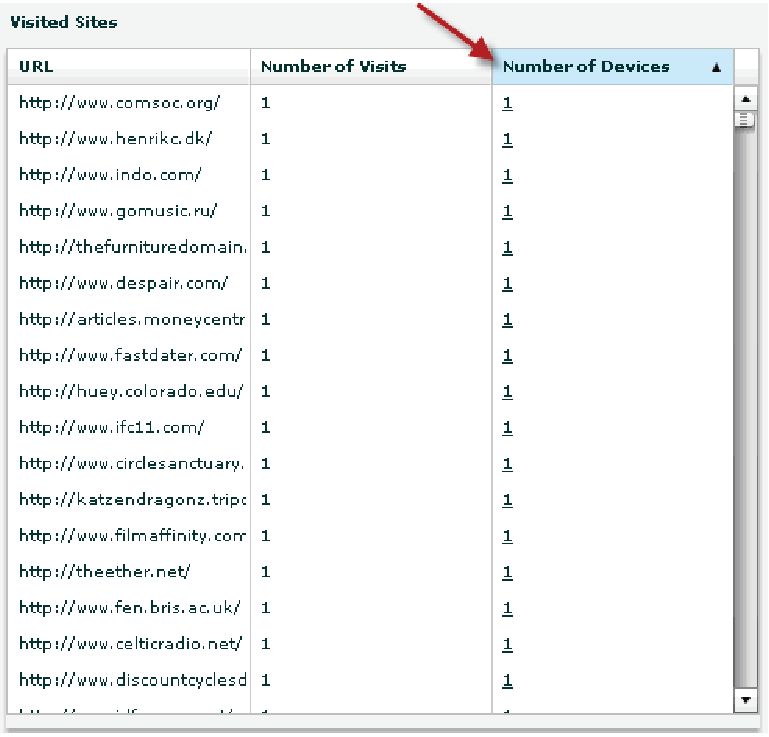
You can also resize the display according to your needs by moving one of the "handle" icons. Additionally, a **Refresh** button is available to clear any modified selections and reload the default values.

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.

FIGURE 2-56. Visited Sites page

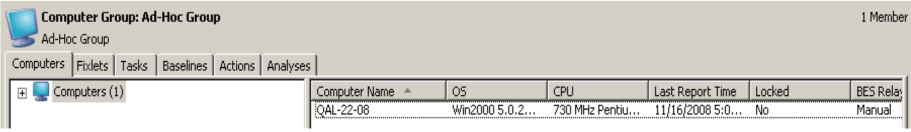


Visited Sites

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
http://www.fastdater.com/	1	1
http://huey.colorado.edu/	1	1
http://www.ifc11.com/	1	1
http://www.circlesanctuary.	1	1
http://katzendragonz.tripc	1	1
http://www.filmaffinity.com	1	1
http://theether.net/	1	1
http://www.fen.bris.ac.uk/	1	1
http://www.celticradio.net/	1	1
http://www.discountcyclesd	1	1

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

FIGURE 2-57. Ad-Hoc Listings



Computer Group: Ad-Hoc Group
Ad-Hoc Group

1 Member

Computer Name ▲	OS	CPU	Last Report Time	Locked	BES Relay
QAL-22-08	Win2000 5.0.2...	730 MHz Pentiu...	11/16/2008 5:0...	No	Manual

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 ESP 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 uploads copies of the logs the next time it is connected to the network.

Can the user disable the Web Protection Module Agent?

Only when the user has administrative rights to their computer.

Support

Search the Trend Micro User Forums for discussion threads and community-based support on a wide variety of topics.

For questions or troubleshooting issues, search the list of available articles in the Trend Micro Knowledge Base at `http://support.trendmicro.com`.

Get technical assistance from Trend Micro's support team from anywhere in the world:

United States

(866) 752-6208

International

(661) 367-2202

`support.trendmicro.com`