BIGFIX

Web Protection Module

powered by TREND MICRO

Setup Guide

Version 1.0

March, 2010

Contents

Part 1 4

Preface 4
System Requirements 4
Installation 5
Checking for Incompatible Software 7

Part 2 9

Working with the Web Protection Module 9
Web Protection Module Agents 9
Deploying Web Protection Module Agents 9
Uninstalling Web Protection Module Agents 11
Configuring Log Maintenance 11
Working with Proxies 14
Configuring Proxy Settings 14
Encrypting a Proxy String 15
Configuring the Proxy 15
Disabling a Proxy Server 16
Web Reputation Technology 17
Disabling Web Reputation Technology 17
Enabling Web Reputation Technology 18
Configuring the Web Reputation Technology Security Level 19
Alert Notifications for Detected Threats 20
Enabling Alert Notifications 20
Disabling Alert Notifications 21
Uploading Logs 21

Part 3 23

Support 23
Technical Support 23

Part 1

Preface

The BigFix Web Protection Module joins its real-time visibility and control platform with your existing desktop security solution to prevent Web-based malware from infecting your users' computers. The 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 websites in real time. This guide will walk you through installation and configuration of the Web Protection Module, and will address proxy settings, web reputation technology, deploying WPM Agents, alert notifications, and uploading logs.

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 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

Installation

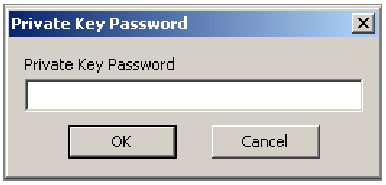
This procedure assumes that you have already installed the BigFix Unified Management Platform.

1. Obtain a masthead for the Web Protection Module site. Email licensing@bigfix.com 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*.

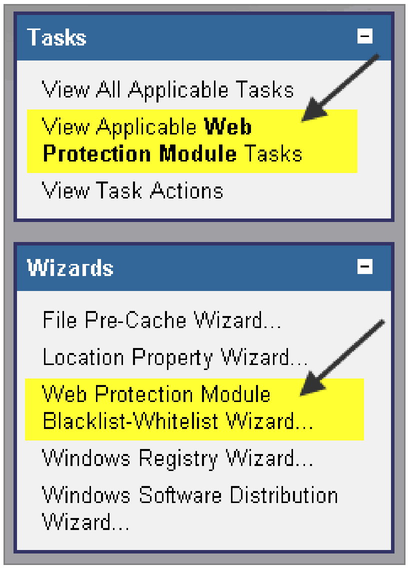
4. Enter your Private Key Password and click *OK*.



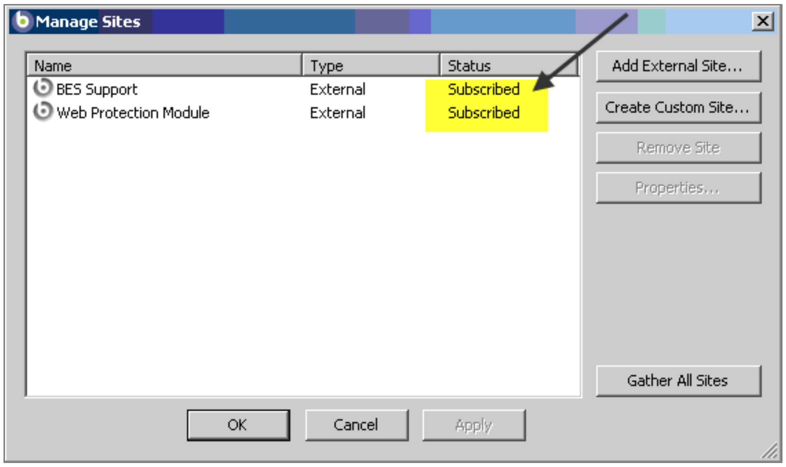
At this point, the Web Protection Module site begins the gathering process, in which it collects the Fixlets, Tasks, Analyses, and other components that will be used in the WPM solution.

When the gathering process is complete, the status will change to *Subscribed*. Refer to the BigFix Console Operator's Guide for more information about mastheads.

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.


Tasks
View All Applicable Tasks
View Applicable Web Protection Module Tasks
View Task Actions
Wizards
File Pre-Cache Wizard...
Location Property Wizard...
Web Protection Module Blacklist-Whitelist Wizard...
Windows Registry Wizard...
Windows Software Distribution Wizard...

In addition, the Web Protection Module site will display *Subscribed* status in the Manage Sites window.



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

Checking for Incompatible Software

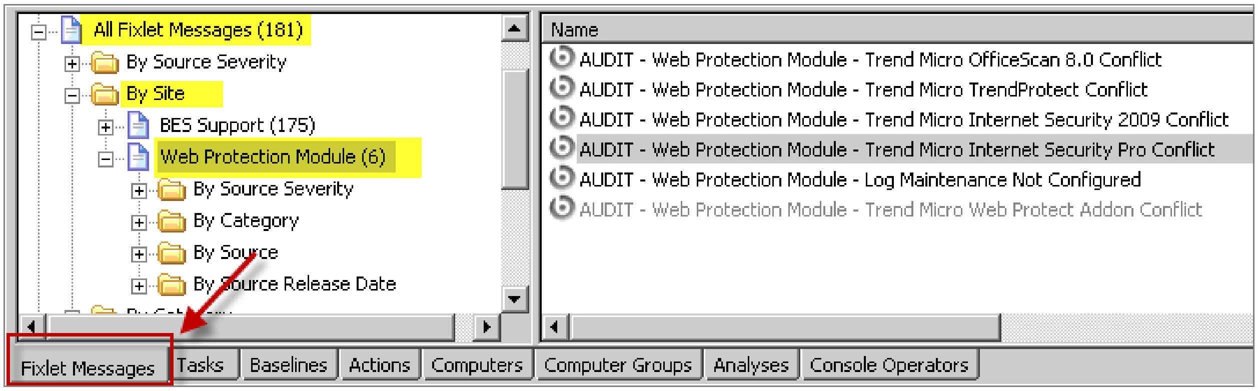
The Web Protection Module includes several AUDIT fixlets that automatically detect any of the following Trend Micro products:

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

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

1. Click the Fixlet Messages tab in the BigFix Console.

2. Select All Fixlet Messages > By Site > Web Protection Module.



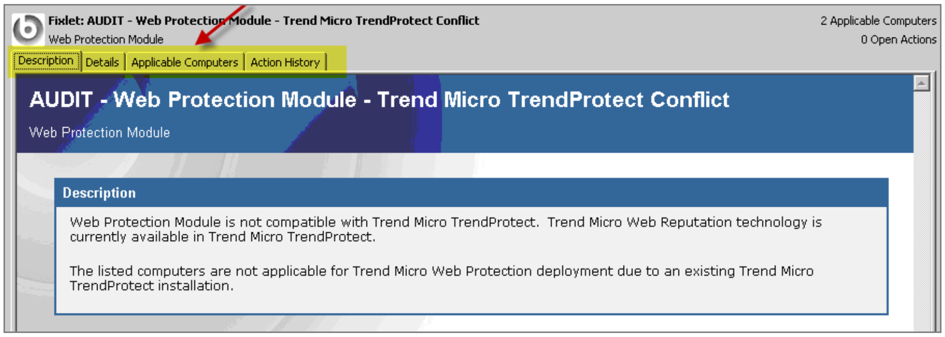
Name
AUDIT - Web Protection Module - Trend Micro OfficeScan 8.0 Conflict
AUDIT - Web Protection Module - Trend Micro TrendProtect Conflict
AUDIT - Web Protection Module - Trend Micro Internet Security 2009 Conflict
AUDIT - Web Protection Module - Trend Micro Internet Security Pro Conflict
AUDIT - Web Protection Module - Log Maintenance Not Configured
AUDIT - Web Protection Module - Trend Micro Web Protect Addon Conflict

3. Check to see if any of the following AUDIT fixlets appear in the list displayed on the rightl:

   - 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

4. If one of the AUDIT Fixlets appears, double-click it to display the Fixlet Message window. You will see the following tabs across the top of this window:

   - Description
   - Details
   - Applicable Computers
   - Action History



Fixlet: AUDIT - Web Protection Module - Trend Micro TrendProtect Conflict
Web Protection Module

2 Applicable Computers
0 Open Actions

AUDIT - Web Protection Module - Trend Micro TrendProtect Conflict

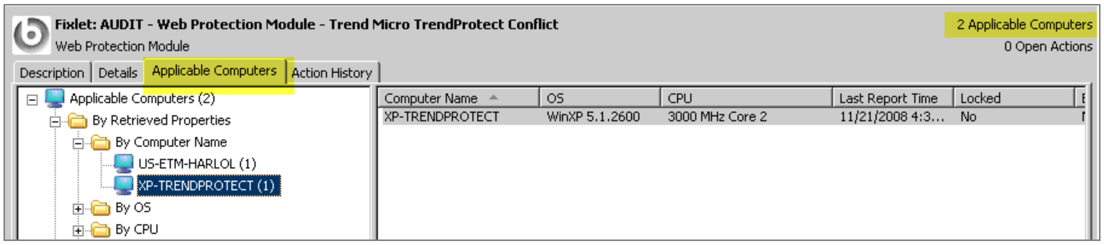
Web Protection Module

Description

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

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

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



Fixlet: AUDIT - Web Protection Module - Trend Micro TrendProtect Conflict
Web Protection Module

2 Applicable Computers
0 Open Actions

Computer Name	OS	CPU	Last Report Time	Locked	E
XP-TRENDPROTECT	WinXP 5.1.2600	3000 MHz Core 2	11/21/2008 4:3...	No	I

6. Manually remove the incompatible software from the endpoint or endpoints, then reboot.

7. Access the Fixlet Messages tab again. The message should no longer appear in the list.

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

Part 2

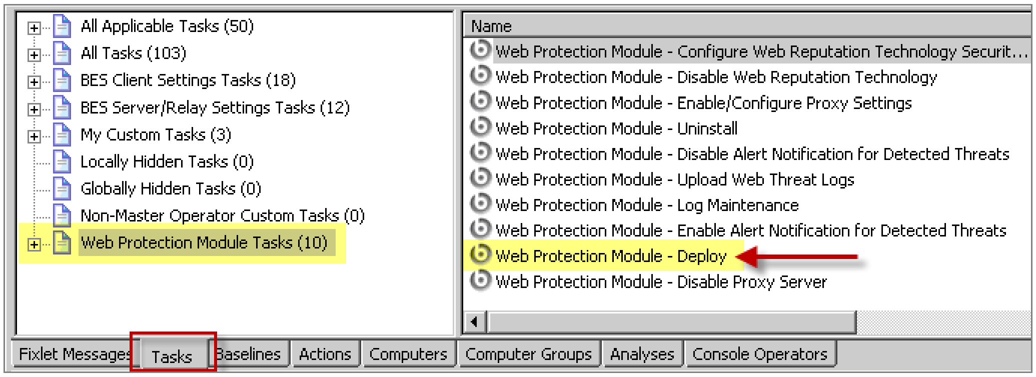
Working with the Web Protection Module

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

Web Protection Module Agents

Deploying Web Protection Module Agents

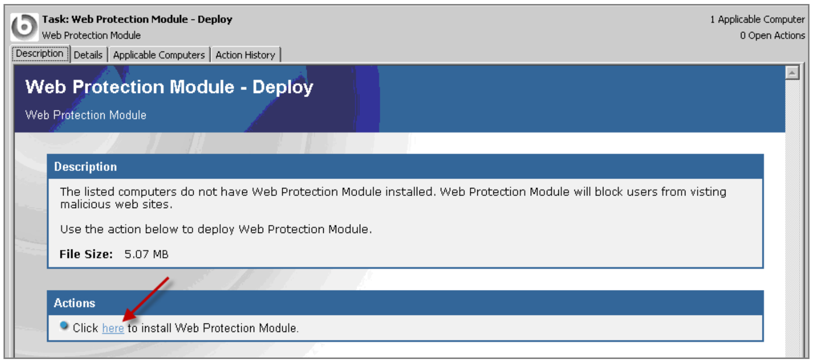
1. From the Tasks tab in the BigFix console, click on Web Protection Module Tasks to display the lists of tasks in the corresponding window on the right.



All Applicable Tasks (50)
All Tasks (103)
BES Client Settings Tasks (18)
BES Server/Relay Settings Tasks (12)
My Custom Tasks (3)
Locally Hidden Tasks (0)
Globally Hidden Tasks (0)
Non-Master Operator Custom Tasks (0)
Web Protection Module Tasks (10)

Name
Web Protection Module - Configure Web Reputation Technology Securit…
Web Protection Module - Disable Web Reputation Technology
Web Protection Module - Enable/Configure Proxy Settings
Web Protection Module - Uninstall
Web Protection Module - Disable Alert Notification for Detected Threats
Web Protection Module - Upload Web Threat Logs
Web Protection Module - Log Maintenance
Web Protection Module - Enable Alert Notification for Detected Threats
Web Protection Module - Deploy
Web Protection Module - Disable Proxy Server

2. From the list tasks, select *Web Protection Module – Deploy*. The Web Protection Module – Deploy Task window opens.



Task: Web Protection Module - Deploy
Web Protection Module

1 Applicable Computer
0 Open Actions

Web Protection Module - Deploy

Web Protection Module

Description

The listed computers do not have Web Protection Module installed. Web Protection Module will block users from visting malicious web sites.

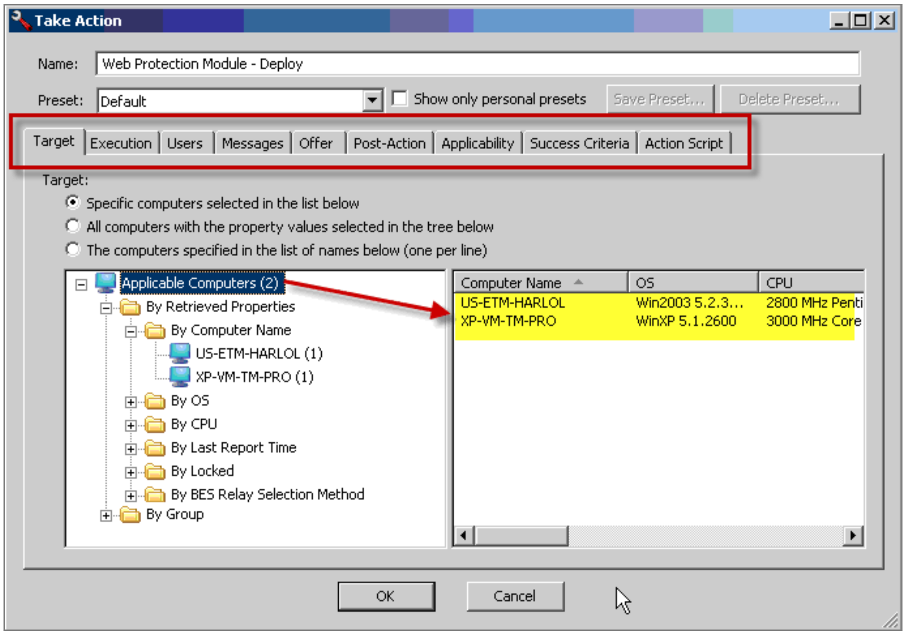
Use the action below to deploy Web Protection Module.

File Size: 5.07 MB

Actions

- Click here to install Web Protection Module.

3. Click where indicated in the Actions box to begin the installation process. The Take Action dialog opens.



Take Action

Name: Web Protection Module - Deploy

Preset: Default ☐ Show only personal presets

Target:

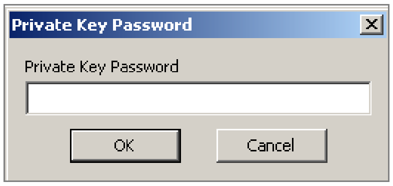
● Specific computers selected in the list below
○ All computers with the property values selected in the tree below
○ The computers specified in the list of names below (one per line)

Computer Name	OS	CPU
US-ETM-HARLOL	Win2003 5.2.3...	2800 MHz Penti
XP-VM-TM-PRO	WinXP 5.1.2600	3000 MHz Core

4. In the Take Action window, select the computer(s) to which you would like to deploy the Web Protection Module agent. Set any desired options, such as scheduling, with the available tabs in the Take Action window. For more information about setting options in the Take Action window, consult the BigFix Console Operators Guide.

5. Click *OK* when finished. The Private Key Password window appears.

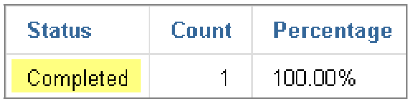
6. Enter your Private Key Password and click *OK*.



Private Key Password

Private Key Password

An Action window appears in which you can track the progress of your deployment. When it is finished, the status shows “Completed.”



Status	Count	Percentage
Completed	1	100.00%

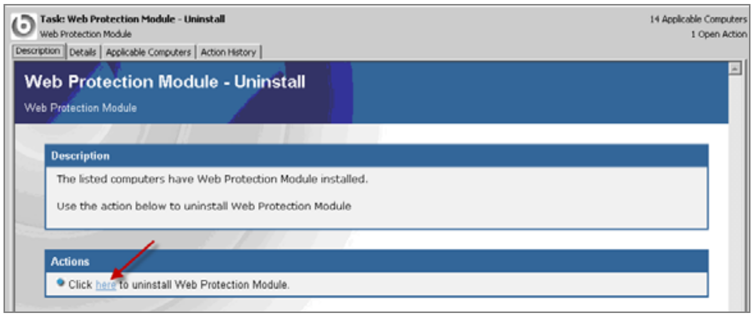
Note: BigFix recommends configuring new Web Protection Module Agents to prevent them from accumulating overly-large URL log files. (By default, BES does not deploy new Agents with log maintenance configured.)

Uninstalling Web Protection Module Agents

To uninstall Web Protection Module Agents:

1. From the Tasks tab in the BigFix Console, click Web Protection Module Tasks.

2. In the List Panel, select *Web Protection Module – Uninst*all. The Web Protection Module – Uninstall Task window will open.



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

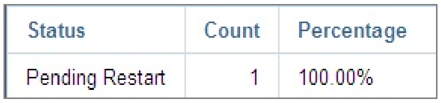
Actions

- Click here to uninstall Web Protection Module.

3. Click where indicated in the Actions box. The Take Action window opens.

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 will display as “Pending Restart.”



Status	Count	Percentage
Pending Restart	1	100.00%

Configuring Log Maintenance

The Web Protection Module 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 Module Agent (urlthreats.txt)

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

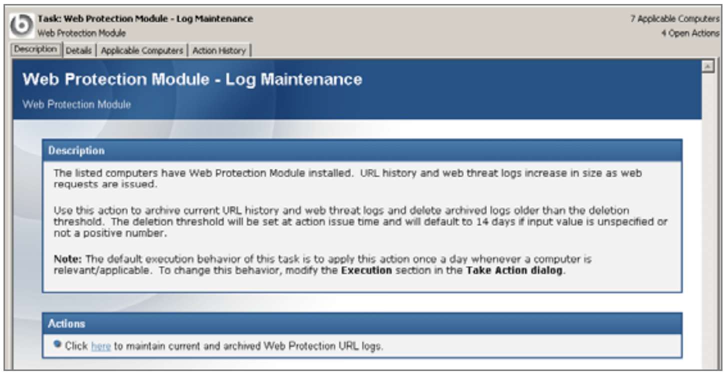
Use the Web Protection Module – Log Maintenance task to set the maximum amount of time (in days) that the Web Protection Agent will maintain these logs on the endpoint.

Note: BigFix 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 BES 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 tab in the Console, click Web Protection Module Tasks.

2. In the List Panel, click *Web Protection Module– Log Maintenance*. The Web Protection Module – Log Maintenance task window opens.



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.

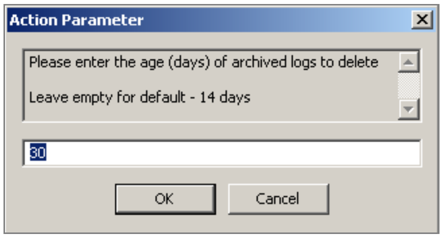
Use this action to archive current URL history and web threat logs and delete archived logs older than the deletion threshold. The deletion threshold will be set at action issue time and will default to 14 days if input value is unspecified or not a positive number.

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.

3. Click where indicated in the Actions window. An Action Parameter window opens. This window allows you to set the number of days the Web Protection Module Agent maintains logs on the selected endpoints.



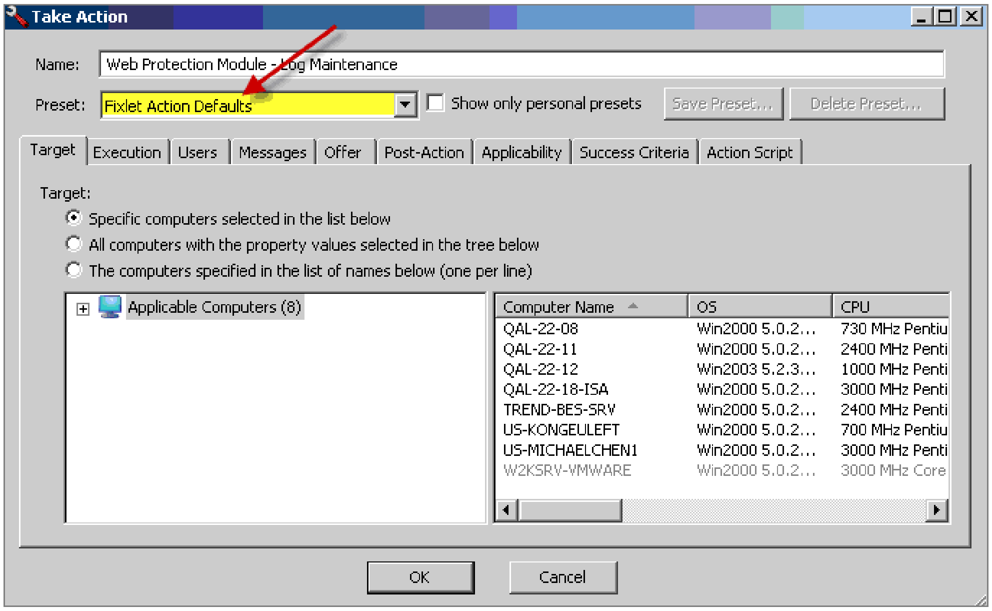
Please enter the age (days) of archived logs to delete

Leave empty for default - 14 days

30

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.

   The Take Action window opens and displays “Fixlet Action Defaults” in the Action Preset drop down box.



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)

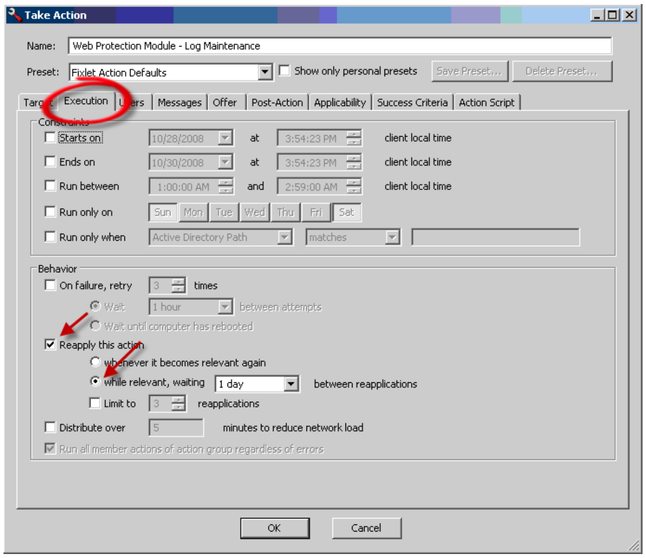
⊞ Applicable Computers (8)

Computer Name	OS	CPU
QAL-22-08	Win2000 5.0.2...	730 MHz Pentiu
QAL-22-11	Win2000 5.0.2...	2400 MHz Penti
QAL-22-12	Win2003 5.2.3...	1000 MHz Penti
QAL-22-18-ISA	Win2000 5.0.2...	3000 MHz Penti
TREND-BES-SRV	Win2000 5.0.2...	2400 MHz Penti
US-KONGEULEFT	Win2000 5.0.2...	700 MHz Pentiu
US-MICHAELCHEN1	Win2000 5.0.2...	3000 MHz Penti
W2KSRV-VMWARE	Win2000 5.0.2...	3000 MHz Core

5. **Important:** On the *Target* 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



Name: Web Protection Module - Log Maintenance

Preset: Fixlet Action Defaults

□ Show only personal presets

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

□ 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

If desired, you may 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.

7. Click *OK* at the bottom of the screen. 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 locate any older log maintenance actions under the *Actions* tab and stop them. Then repeat steps 1-9 above.

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

Working with Proxies

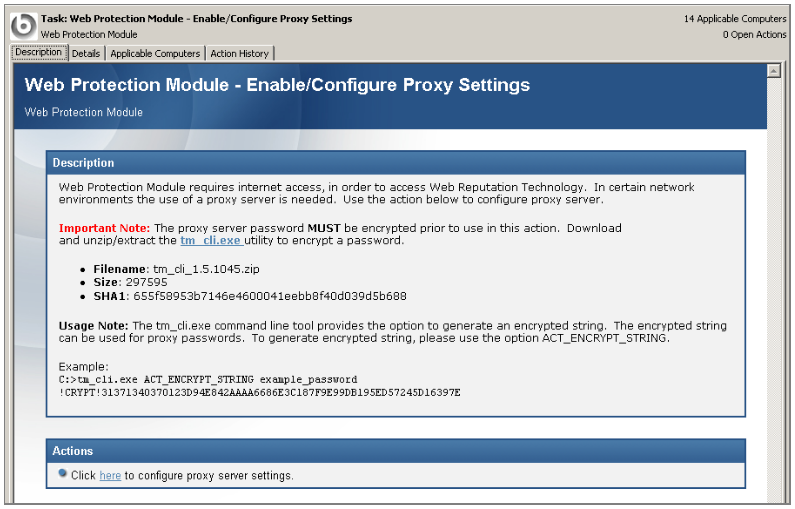
Configuring Proxy Settings

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

To configure one or more Agent’s proxy settings:

1. From the Tasks tab in the Console, click *Web Protection Module Tasks*.

2. In the List Panel, click *Web Protection Module – Enable/Configure Proxy Settings*. The Web Protection Module – Enable/Configure Proxy Settings task window opens.



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.

If your proxy requires a password, follow 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.

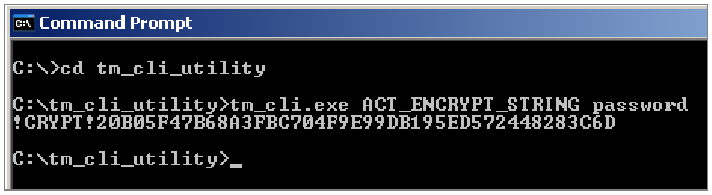
1. Click the **tm_cli.exe** link in the *Web Protection Module – Enable/Configure Proxy Settings* document page to download a zipped version of the password encryption utility.

2. 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.

3. Open a DOS Command window and use the cd command to navigate to your target_directory.

4. Enter the following command where the password you want to encrypt appears in italics:

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

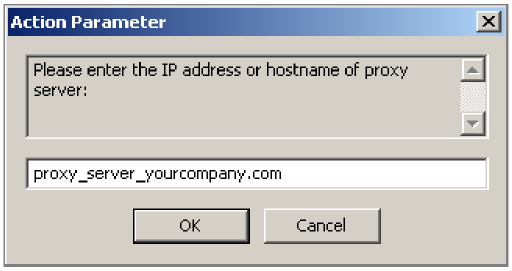


```
C:\>cd tm_cli_utility

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

C:\tm_cli_utility>_
```

5. 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

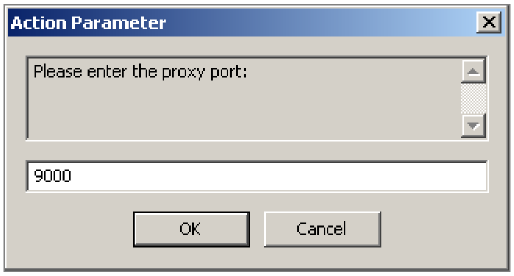
1. Access the Web Protection Module – Enable/Configure Proxy Settings document page and click where indicated in the Actions window. The first of four Action Parameter windows appears.



Please enter the IP address or hostname of proxy server:

proxy_server_yourcompany.com

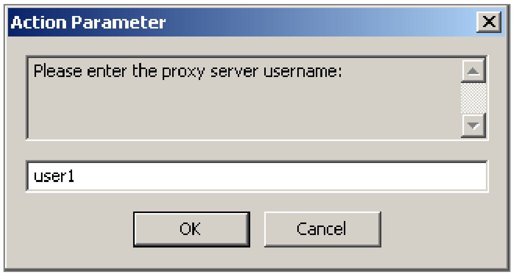
2. Enter the IP address or hostname of the Web proxy you wish to use and click *OK*. A second window appears, prompting you for the number of the proxy server port you wish to use.



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.

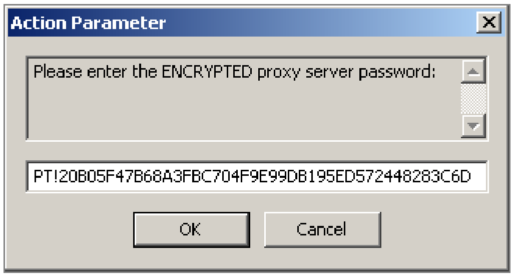


Action Parameter

Please enter the proxy server username:

user1

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



Action Parameter

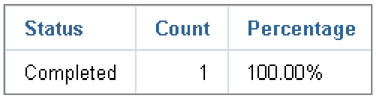
Please enter the ENCRYPTED proxy server password:

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 that you wish 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."



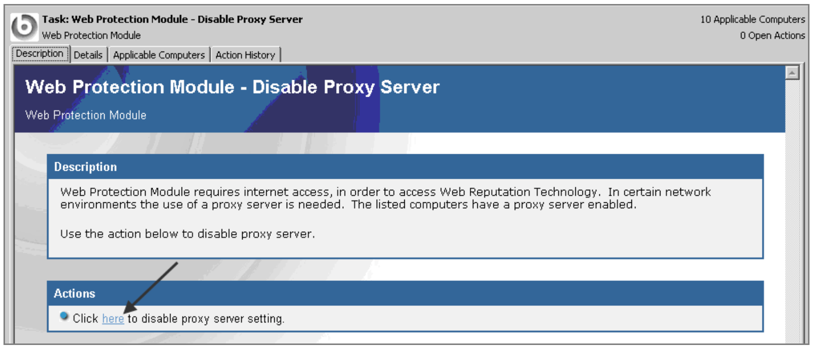
Status	Count	Percentage
Completed	1	100.00%

Disabling a Proxy Server

To disable one or more Agent's proxy settings:

1. From the Tasks tab in the Console, click *Web Protection Module Tasks*.

2. In the List Panel, click *Web Protection Module – Disable Proxy Server*. The Web Protection Module – Disable Proxy Server task window opens.



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.

3. Click where indicated in the Actions box. The Take Action window opens.

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 BES 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.

Web Reputation Technology

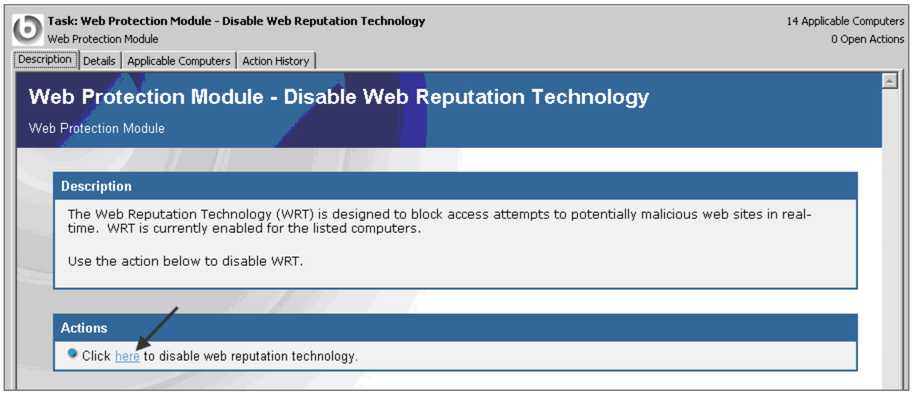
Web Reputation Technology (WRT) uses a “reputation score” calculated by heuristics and an “in-the-cloud” database of known threats to detect and block security risks in outbound Web requests. WRT is activated by default when you install the Web Protection Agent on a computer.

Disabling Web Reputation Technology

To disable WRT:

1. From the Tasks tab, click *View Applicable Web Protection Module Tasks.*

2. In the list of tasks, click *Web Protection Module – Disable Web Reputation Technology*. The Web Protection Module – Disable Web Reputation Technology task window opens.



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.

3. Click where indicated in the Actions box. The Take Action window opens.

4. Select the computer or computers in the window and click *OK*. The Private Key Password window appears.

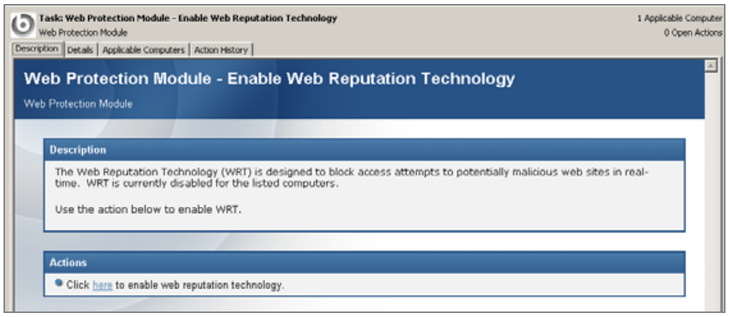
5. Enter your Private Key Password and click *OK*. An Action window appears in which you can track the progress of your change. When it is finished, the status shows "Completed."

Enabling Web Reputation Technology

If you need to enable (WRT) for one or more endpoints, follow the steps below:

1. From the Tasks tab, click *View Applicable Web Protection Module Tasks*.

2. In the List Panel, click *Web Protection Module – Enable Web Reputation Technology*. The Web Protection Module – Enable Web Reputation Technology task window opens.



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.

3. Click where indicated in the Actions window. The Take Action window opens.

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

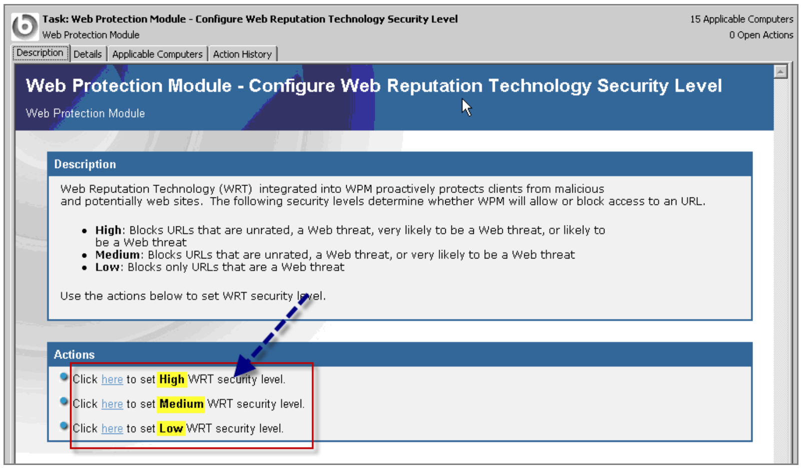
The Web Protection Module enables you to set security levels for your endpoints. You can choose one of the following settings for each endpoint or group of endpoints:

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 tab, click *View Applicable Web Protection Module Tasks*.

2. In the List Panel, click *Web Protection Module – Configure Web Reputation Technology Security Level*. The Web Protection Module – Configure Web Reputation Technology Security Level Task window opens.



Task: Web Protection Module - Configure Web Reputation Technology Security Level
Web Protection Module

15 Applicable Computers
0 Open Actions

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.

3. In the Actions box, click the link corresponding to the security level you want to set. The Take Action window opens.

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.”

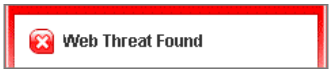
Alert Notifications for Detected Threats

Enabling Alert Notifications

This feature is turned off by default when you install the Web Protection Agent on a computer.

The Web Protection Module 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 below that appears for 30 seconds in the lower left corner of the screen whenever the Agent detects a threat.



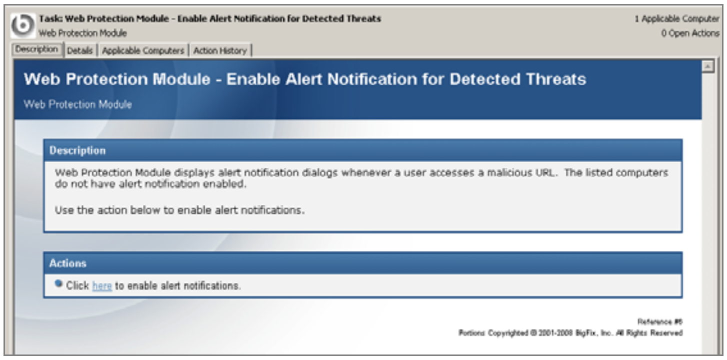
Web Threat Found

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 tab, click *View Applicable Web Protection Module Tasks*.

2. In the List Panel, click *Web Protection Module – Enable Alert Notification for Detected Threats*. The Web Protection Module – Enable Alert Notifications for Detected Threats task window opens.



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
Portions Copyrighted © 2001-2008 BigFix, Inc. All Rights Reserved

3. Click where indicated in the Actions window. The Take Action window opens.

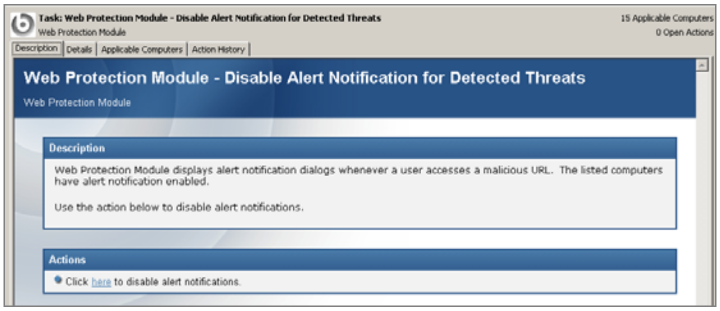
4. Select the computer or computers in the window and click *OK*. The Private Key Password window appears.

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 Notifications

To disable alert notification:

1. Using the same process as above, click the Tasks tab and click the *Web Protection Module – Disable Alert Notification for Detected Threats* link. The Web Protection Module – Disable Alert Notifications for Detected Threats task opens.



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

15 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.

2. Click where indicated in the Actions window to disable alert notifications. The Take Action window opens.

3. 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.

4. 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 BES server. This task is particularly useful for archiving or using a third-party tool to perform analyses on your endpoint logs.

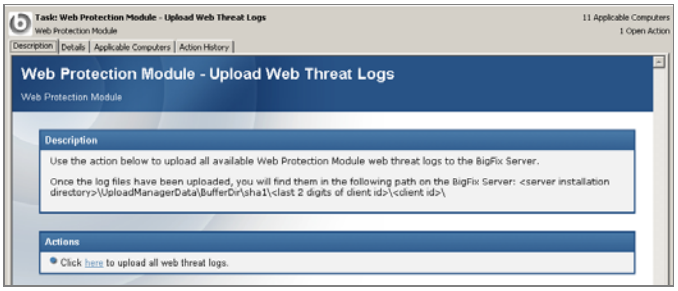
When you use this task, the Web Protection Module Agent uploads copies of the logs to the following directory on the BES server and deletes them from the endpoint:

```
<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 BES server:

1. From the Tasks tab, click *View Applicable Web Protection Module Tasks*.

2. In the List Panel, click *Web Protection Module– Upload Web Threat Logs*. The Web Protection Module – Upload Web Threat Logs task window opens.



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.

3. Click where indicated in the Actions window to upload logs. The Take Action window opens.

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.”

Part 3

Support

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