



Malware Prevention Module

Getting Started Guide

Revision 1.0.1

Warning and Disclaimer

This document is designed to provide information about the configuration and installation of **CensorNet Professional (CNPRO)** and its various modules and extensions. Every effort has been made to make this document as complete and accurate as possible, but no warranty or fitness is implied.

CensorNet Ltd does not accept any liability for poorly designed or malfunctioning networks.

Table of Contents

Table of Contents.....	2
Introduction	3
Requirements.....	3
Installation	3
Using the Malware Prevention Module.....	4
Default Settings.....	5
Testing the Malware Prevention Module	6
Technical Support	7

Introduction

The Malware Prevention module is an extension to the CSRV Database which provides a set of new categories in the Content Classifier section of the Policy Manager. The categories add millions of executable files found on the Internet which have been scanned for malware and categorised according to whether they are clean or contain malware. With this module it is possible to block malware sites or block sites that do not contain malware (for example, legitimate download and file sharing web sites – sites that contain executables).

Requirements

- CensorNet Professional 1.4.11 or above.
- An up-to-date download of the URL database (CSRV) – please check the System Overview page for “Database Update Complete” message.

Installation

Installation is automatic.

Once you have ordered the Malware Prevention add-on module it will be added to your CSRV account within 24 hours and on the next update (configured under *Filters* > *URL Database Download*) the Malware Categories will be downloaded and processed.

Using the Malware Prevention Module

The new categories will appear under the *Add-Ons* top level category when you create or update a policy.

The new categories are as follows:-

Category Name	Description
Malware Domain, English	Malware was found on the entire domain, category is applied at domain level.
Malware Object, English	Indicates Malware was found in specific executable, but not in sufficient numbers to classify the entire domain. Rating is applied at object level.
Potential Malware, English	Domain was scanned and some Malware was found, however, not in sufficient quantities to classify the entire domain.
No Malware Domain, English	Entire domain was scanned, no Malware was found in any of the executables. Rating is applied at domain level.
No Malware Object, English	Specific executable was scanned and no Malware was found. Rating is applied at object level.

After the Malware Prevention module has been activated and the CSRV database has updated successfully, the new module will appear as follows when you create or update a policy:-

Categories	Allow	Ignore	Block
<input checked="" type="checkbox"/> Commercial	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> Education	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> General Interest	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> Government	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> Internet	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> Generic	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Add-Ons	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Malware	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Malware Domain, English	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Malware Object, English	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Potential Malware, English	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> No Malware Domain, English	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input type="checkbox"/> No Malware Object, English	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Default Settings

By default the Malware category will be set to Ignore. This means that any web sites containing malware will not be matched against the new categories.

The following screenshot shows the recommended default settings for the Malware category:-

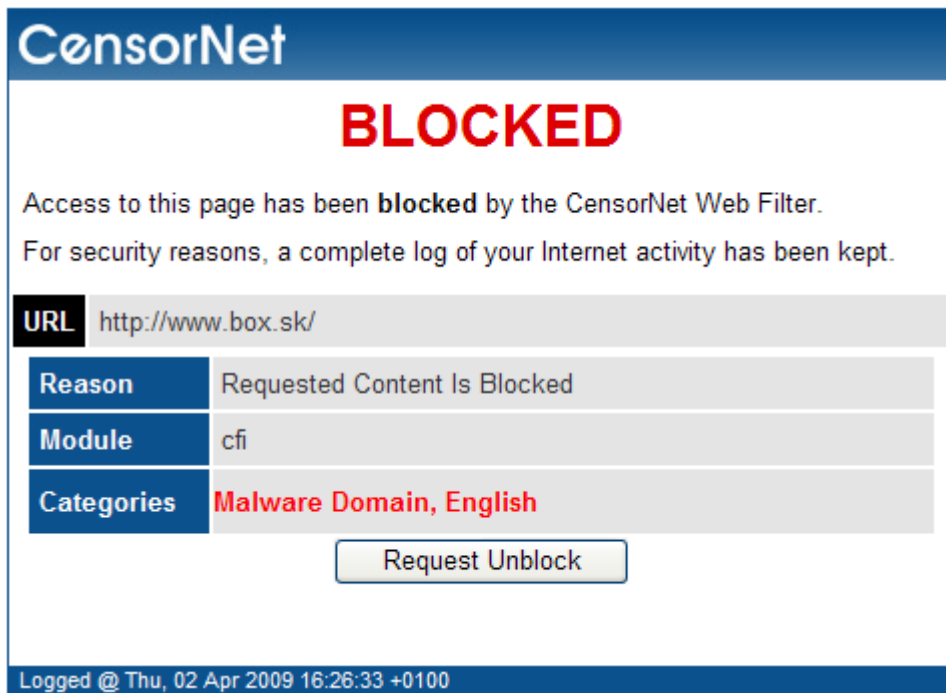
Categories	Allow	Ignore	Block
<input checked="" type="checkbox"/> Commercial	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Education	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> General Interest	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Government	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Generic	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Add-Ons	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Malware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Malware Domain, English	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Malware Object, English	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> Potential Malware, English	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input type="checkbox"/> No Malware Domain, English	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> No Malware Object, English	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

This will **block** known sites that contain malware and **allow** legitimate sites that contain executables that are clean.

Testing the Malware Prevention Module

The easiest way to test the Malware Prevention module is to edit the default policy and enable the Malware category as described in "Default Settings" above.

Whilst logged in as a username that will receive the default policy, attempt to visit www.box.sk and you should see this message in your web browser:-



Next, go to the "Who's Blocked" report in CensorNet Professional Web control panel under Reports > Who's Blocked and click on the username or workstation you used to visit the web site. In the report, you should see the visit to www.box.sk classified as Malware, English:-

Web Site	U	Workstation	Visited At	Duration	Allowed	Ignored	Blocked
www.box.sk		TIML	2009-04-02 16:26:33+01	00:00:00	0	0	2
/		TIML	2009-04-02 16:26:33+01	-			Malware Domain, English
/favicon.ico		TIML	2009-04-02 16:26:33+01	-			Malware Domain, English
www.cracklib.net		TIML	2009-04-02 16:25:32+01	00:00:05	0	5	0
www.megagames.com		TIML	2009-04-02 16:25:22+01	00:00:00	0	0	2

Technical Support

If you require help installing, configuring or activating CensorNet Professional please contact our Technical Support department in the following ways.

Live Support <http://www.censornet.com/support>

Telephone 0845 230 9592

E-mail support@censornet.com