



# Installation Guide Supplement

for use with

## Integrated Check Point® Products

Websense® Web Security  
Websense Web Filter



©1996–2010, Websense Inc.  
All rights reserved.  
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2010

Printed in the United States of America and Ireland.

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 6,606,659 and 6,947,985 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

## **Trademarks**

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, Windows Vista and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Check Point, FireWall-1, VPN-1, Check Point Edge, and VPN-1 Edge are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Sun, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Novell Directory Services is a registered trademark of, and eDirectory is a trademark of, Novell, Inc., in the United States and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

## **WinPcap**

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).

Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# Contents

<b>Chapter 1</b>	<b>Check Point Integration.....</b>	<b>5</b>
	Supported Check Point product versions .....	5
	How Websense filtering works with Check Point products.....	5
	Distributed environments .....	7
	Client computers and Check Point products .....	7
	Communicating with Websense software .....	7
	Enhanced UFP performance.....	8
	Installation .....	8
	Initial setup.....	9
	Upgrade .....	9
	Migrating between Check Point versions.....	10
<b>Chapter 2</b>	<b>Configuring Check Point Products.....</b>	<b>11</b>
	Creating a network object.....	12
	Creating an OPSEC application object.....	13
	Creating Resource Objects.....	16
	Defining rules.....	18
	Configuring enhanced UFP performance .....	21
	Websense configuration .....	21
	Check Point product configuration.....	22
	Early versions compatibility mode .....	22
	Enhanced UFP performance .....	23
<b>Appendix A</b>	<b>Troubleshooting .....</b>	<b>25</b>
<b>Appendix B</b>	<b>Configuring Communications.....</b>	<b>29</b>
	Establishing Secure Internal Communication .....	29
	Prerequisites .....	30
	Configuring the Check Point product to use SIC .....	31
	Configuring Websense software to use SIC .....	33
	Stopping and restarting the UFP Server .....	35
	Updating the OPSEC Application object .....	35
	Restoring Clear Communication .....	37
<b>Index .....</b>		<b>39</b>



# 1

## Check Point Integration

This supplement to the Websense Web Security and Websense Web Filter *Installation Guide (Installation Guide)* provides information specific to integrating Websense software with Check Point® products. For general installation instructions, refer to the *Installation Guide*.

An integration with a Check Point product works with Websense components as follows:

- ◆ **Filtering Service:** Interacts with the Check Point product and Network Agent to filter Internet requests.
- ◆ **Network Agent:** Manages Internet protocols that are not managed by the Check Point product.



### Important

Do *not* install Network Agent on the Check Point machine.

---

## Supported Check Point product versions

---

Websense Web Security and Websense Web Filter are compatible with the following Check Point products:

- ◆ FireWall-1 Feature Pack 1 or greater
- ◆ FireWall-1 NG AI
- ◆ FireWall-1 NGX
- ◆ Check Point Edge
- ◆ Check Point UTM-1™ Edge

## How Websense filtering works with Check Point products

---

Check Point products provide network security and a framework for content filtering. Websense software communicates with the Check Point product via URL Filtering Protocol (UFP). Websense software is implemented as a UFP Server, and

communicates with the Check Point product over TCP sockets. By default, Websense software listens on port 18182 for messages from the Check Point product.

To begin filtering:

- ◆ Client computers must point to the machine running the Check Point product as their default gateway. Typical networks implement this configuration for security reasons unrelated to filtering.
- ◆ The Check Point product must be configured to use a rule to analyze all HTTP requests, as well as FTP requests issued by a browser that proxies to the Check Point product. The rule must use the URI Specifications for HTTP.



**Note**

If Websense software must download the Master Database through a proxy server or firewall that requires authentication for any HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication.

---

When Websense software is integrated with a Check Point product, you define policies within TRITON - Web Security (the configuration interface for Websense software). These policies identify which of the Websense categories are blocked or permitted during different times and days. Within the Check Point product, you typically define a rule that directs the firewall to reject requests for sites in Websense categories whose action is set to block, limit by quota, or confirm. If a client selects an option to view a site with quota time on a block page, Websense software tells the Check Point product to permit the site.

When the Check Point product receives an Internet request for either an HTTP site or an FTP site requested by a browser that uses the firewall as a proxy, it queries Websense Filtering Service to determine if the site should be blocked or permitted.

Filtering Service checks the policy assigned to the client. Each policy designates specific time periods and lists the category filters that are in effect during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database to locate the category for the requested URL:

- ◆ If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- ◆ If the site is assigned to a permitted category, Filtering Service notifies the Check Point product that the site is not blocked, and the client is allowed to see the site.

---

## Distributed environments

---

When the SmartCenter™ server (FireWall-1 Management Server in FireWall-1) is separated from the Enforcement Module (FireWall-1 Module in FireWall-1), modify your Rule Base to allow the SmartCenter Server to communicate with Websense Filtering Service during setup. This allows the Check Point product to load the Websense dictionary, which contains the categories Blocked and Not Blocked.

All other communication is between Filtering Service and the Enforcement Module. See Check Point documentation for instructions on modifying the Rule Base.

**Note**

It is a best practice to install Websense components on a different machine than the Check Point product. If you choose to install Websense software and the Check Point product on the same machine, see the Websense Knowledge Base for configuration instructions. Search the Websense Knowledge Base (at [www.websense.com/SupportPortal/](http://www.websense.com/SupportPortal/)) for the terms *Installing Websense software on Check Point Firewall-1*.

---

---

## Client computers and Check Point products

---

Check Point products process HTTP requests transparently, so no Internet browser changes are required on client computers. You can have clients proxy to the firewall to enable user authentication within that firewall, or to enable filtering of FTP requests from a browser. See Check Point product documentation for instructions on handling FTP requests.

If clients use the firewall as a proxy, browsers on client computers must be configured to support proxy-based connections.

---

## Communicating with Websense software

---

Depending on which Check Point product is running, Websense software may communicate with the firewall through a secure connection or a clear connection.

- ◆ A secure connection requires that communication between the Check Point product and the Websense UFP Server is authenticated before any data is exchanged.
- ◆ A clear connection allows Websense software and the Check Point product to transfer data without restrictions.

The connection options for each supported Check Point product version are similar, but have some slight differences.

- ◆ **FireWall-1 NGX or FireWall-1 NG with Application Intelligence (AI):** clear connection is the default. An authenticated connection can be established, but is not recommended because of performance issues. In addition, a clear connection is required to use the Enhanced UFP Performance feature described in the next section.
- ◆ **FireWall-1 NG Feature Pack 1 or later:** clear connection is the default, but a Secure Internal Communication (SIC) trust connection can be configured within both Check Point and Websense software.

See [Chapter 2: Configuring Check Point Products](#) for the appropriate procedures to establish secure or clear communication with the Websense software.

## Enhanced UFP performance

---

The enhanced UFP performance feature increases the amount of traffic that Websense software and the Check Point product can filter while reducing CPU load.

Configuring enhanced UFP performance requires the proper settings in both Websense software and the Check Point product. See [Configuring enhanced UFP performance](#), page 21 for detailed configuration procedures.



### Note

To use enhanced UFP performance, Websense software and the Check Point product must be configured for clear communication.

---

## Installation

---

Refer to Chapter 2 of the *Installation Guide* for complete download and installation instructions for Websense software. Follow the installation instructions in the guide until prompted to select an integration option.

- ◆ If you are performing a custom installation:
  - The integration prompt is displayed only if Filtering Service is being installed on this machine.
  - Do not select Filtering Plug-in from the components list. No plug-in is needed for a Check Point integration.
- ◆ On the **Integration Option** screen, select **Integrated with another application or device**.
- ◆ On the **Select Integration** screen, select **Check Point**.

- ◆ If Network Agent is included in this installation, a warning advises against installing Network Agent on the same machine as the firewall. An exception allows Websense software and the firewall to be installed on an appliance with separate virtual processors to accommodate both products.
  - Select **Yes, install Network Agent** only if the machine has separate virtual processors.
- ◆ Follow the onscreen instructions in the Websense installation program to complete the installation.
- ◆ Follow the instructions in [Chapter 2: Configuring Check Point Products](#) to configure the firewall integration with Websense software.

## Initial setup

---

If Filtering Service is installed on a multihomed machine, or on the machine that is running the Check Point product (not recommended), identify Filtering Service by its IP address in your network so that Websense block messages can be sent to users.

See *Identifying Filtering Service by IP address* in the *Installation Guide* for instructions.

## Upgrade

---

Before upgrading Websense software, make sure your Check Point product is supported by the new version. See [Supported Check Point product versions, page 5](#).

Follow the instructions in the *Installation Guide* and *Installation Guide Supplement for Upgrading*.

Update the Check Point dictionary with new Websense settings, and update the Websense Resource Object in SmartCenter before you begin filtering with the new version of Websense software.

For more information, see [Chapter 2: Configuring Check Point Products](#) of this supplement.

## Migrating between Check Point versions

---

If you plan to upgrade your Check Point product (from FireWall-1 NG to FireWall-1 NGX, for example), do so *after* upgrading the Websense software.



### **Important**

Do not make any additional modifications to your Websense software until after you have upgraded your firewall product.

---

See the Websense Websense Web Security and Websense Web Filter *Installation Guide Supplement for Upgrading* for details.

See Check Point documentation for information on upgrading the Check Point software.

See [Chapter 2: Configuring Check Point Products](#) of this supplement for the necessary configuration procedures to ensure that your new version of the Check Point product can communicate with Websense software.

# 2

## Configuring Check Point Products

In addition to defining Websense filtering policies and assigning them to the appropriate clients, you must set up the Check Point product with the necessary objects and rules. In describing these objects and rules, this chapter assumes that you are familiar with general Check Point product concepts.

The following tasks must be completed before you begin to configure the Check Point product to communicate with Websense software:

- ◆ Both the Check Point product and either Websense Web Security or Websense Web Filter must be installed and running.
- ◆ In the Check Point product, create:
  - An object for the firewall itself, if it does not already exist (it typically is created by default upon installation of the Check Point product).
  - Objects that represent your network topology (as needed for filtering). See Check Point product documentation for more information on objects.

Configuring FireWall-1 NG, FireWall-1 NG with AI, and FireWall-1 NGX for Websense content filtering involves the following procedures:

- ◆ Create a network object for the machine running Websense Filtering Service. See [Creating a network object, page 12](#).
- ◆ Create an OPSEC™ application object for the Websense UFP Server. See [Creating an OPSEC application object, page 13](#).
- ◆ Create URI resource objects for the dictionary categories that Websense software sends to the Check Point product. See [Creating Resource Objects, page 16](#).
  - When creating the URI resource objects, you can configure both Websense software and the Check Point product to use Secure Internal Communication (SIC), rather than the default clear communication. See [Establishing Secure Internal Communication, page 29](#).
  - To return to clear communication, see [Restoring Clear Communication, page 37](#).
- ◆ Define rules that govern how the Check Point product behaves when it receives a response from Websense software. See [Defining rules, page 18](#).
- ◆ Optionally, you can configure the Check Point product for enhanced UFP performance. This applies only to FireWall-1 NG with Application Intelligence and FireWall-1 NGX. Make sure that you have configured the Check Point

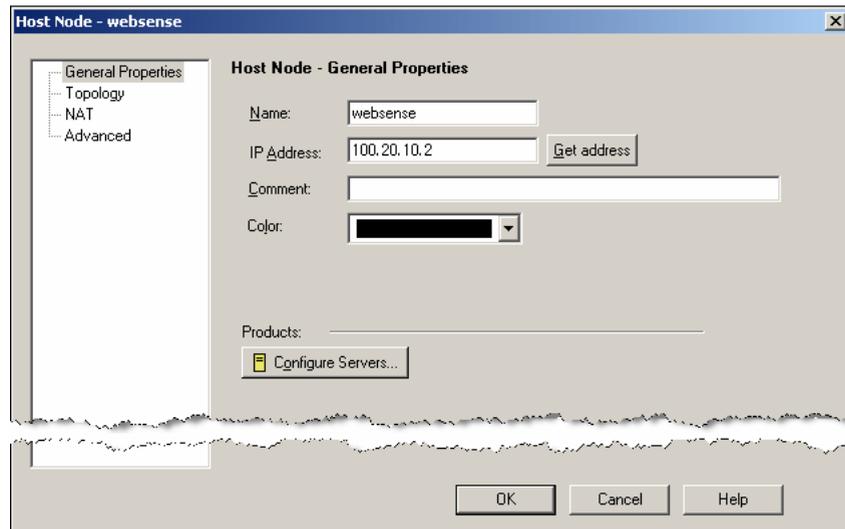
product for Websense content filtering before this procedure. See *Configuring enhanced UFP performance*, page 21.

**Note**

The procedures and illustrations in this chapter are based on FireWall-1 NGX. If FireWall-1 NG or FireWall-1 NG with Application Intelligence (AI) is running, you may notice slight differences in screens and field names.

## Creating a network object

1. Open a Check Point SmartConsole, such as SmartDashboard™ (*Policy Editor* in earlier versions). See your Check Point product documentation for detailed instructions on using SmartConsole.
2. If you have not already done so, create a network object (**Manage > Network Objects > New > Node > Host**) for the machine running Filtering Service.  
This object is required only if Websense software runs on a separate machine behind the firewall, as recommended.
3. Select **General Properties** in the left column. The following dialog box appears.



Host Node - General Properties

- Complete the items in the page:

Field	Description
<b>Name</b>	Enter a descriptive name for the network object representing the machine on which Filtering Service is running, such as <b>Websense</b> (make a note of this name for later use). Note: If your DNS is configured to resolve machines within your network, enter the Filtering Service machine's host name here. Then, for IP Address, you can click <b>Get address</b> to resolve the host name to its IP address automatically.
<b>IP Address</b>	Enter the IP address of the machine running Filtering Service. Note: If you entered a host name for Name, you can click <b>Get address</b> to find the machine's IP address automatically. See the description for Name, above, for more information.
<b>Comment</b>	Enter a description for this object.
<b>Color</b>	Select a color for displaying this object in SmartDashboard.

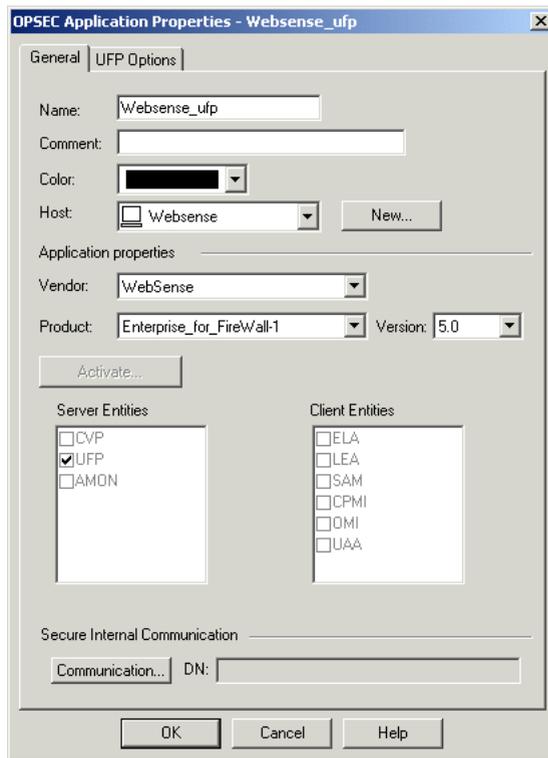
- Click **OK**.

## Creating an OPSEC application object

After you create the network object for the machine running Filtering Service, you must create an OPSEC application object for the Websense UFP Server. The UFP server was installed with the other components when you chose Check Point as your integration product during installation.

- Open SmartDashBoard, if it is not already open.
- Select **Manage > Servers and OPSEC Applications**.
- Click **New**, and then select **OPSEC Application** from the drop-down list.
- Select the **General** tab in the OPSEC Application Properties dialog box.

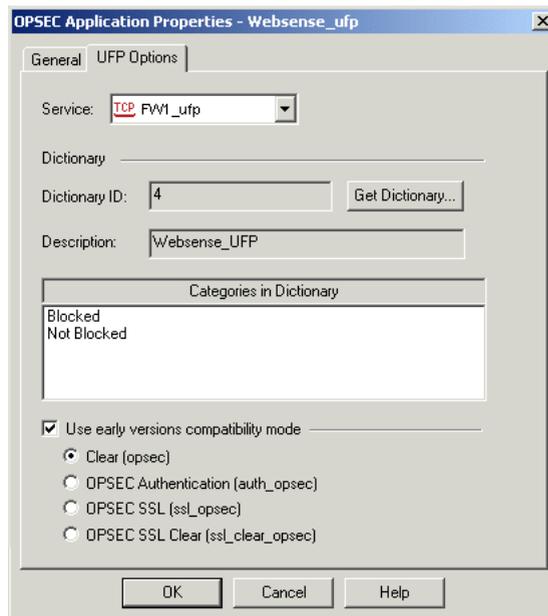
5. Complete the items on the tab:



OPSEC Application Properties – General tab

Field	Description
<b>Name</b>	Enter a descriptive name, such as <b>Websense_ufp</b> (make a note of this name for later use).
<b>Comment</b>	Enter a description for this object.
<b>Color</b>	Select a color for displaying this object in SmartDashboard.
<b>Host</b>	Select the network object created in the previous section. This object identifies the machine running Filtering Service. If you have not yet created this object, click <b>New</b> to create it. See <a href="#">Creating a network object</a> , page 12 for instructions.
<b>Vendor</b>	Select <b>Websense</b> .
<b>Product</b>	This value is not used in creating an object and does not need to be changed.
<b>Version</b>	This value is not used in creating an object and does not need to be changed.
<b>Server Entities</b>	<b>UFP</b> is checked automatically when you select Websense as the Vendor, and cannot be changed.

6. Select the **UFP Options** tab.



OPSEC Application Properties –  
UFP Options tab

7. Check the **Use early versions compatibility mode** option (**Backwards Compatibility** in earlier versions).
  - If Secure Internal Communication (SIC) is used, go to [Establishing Secure Internal Communication](#), page 29, to complete this section.
  - If SIC is not used, select **Clear (opsec)**.
8. Click **Get Dictionary**.

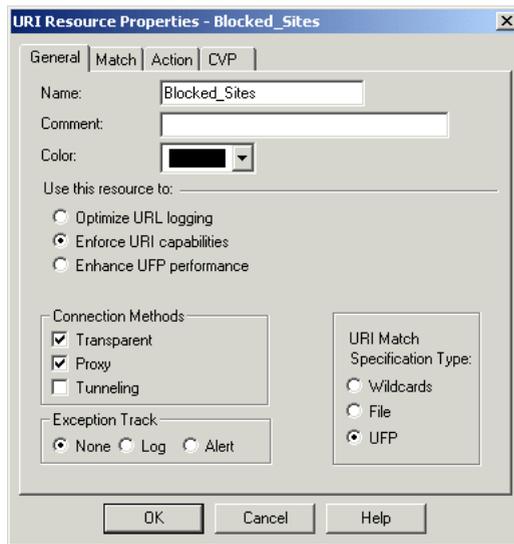
Websense software provides the Check Point product with a dictionary containing these categories: **Blocked** and **Not Blocked**. The full set of Websense categories is configured via TRITON - Web Security. See TRITON - Web Security Help for more information.

9. Click **OK**.
10. Close the OPSEC Applications dialog box.
11. Select **Policy > Install** to install the policy on the firewall.  
See the Check Point product documentation for more information.

## Creating Resource Objects

Create a Resource Object to define a Uniform Resource Identifier (URI) that uses the HTTP protocol. This URI identifies the Websense dictionary category *Blocked*.

1. Open SmartDashboard and select **Manage > Resources**.  
The Resources dialog box appears.
2. Click **New**, and choose **URI** from the submenu to display the URI Resource Properties dialog box.
3. Select the **General** tab, and complete the items in the tab.

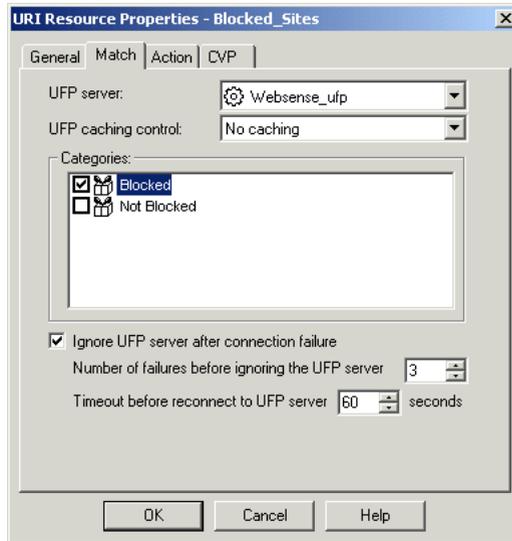


URI Resource Properties – General tab

Field	Description
<b>Name</b>	Enter a name for this URI Resource Object, such as <b>Blocked_Sites</b> .
<b>Comment</b>	Enter a description for this object.
<b>Color</b>	Select a color for this object's icon.
<b>Use this resource to</b>	Select <b>Enforce URI capabilities</b> . This option enables all other functionality of the URI resource, such as configuring CVP checking on the <b>CVP</b> tab. All basic parameters defining schemes, hosts, paths, and methods apply. The URL is checked for these parameters.
<b>Connection Methods</b>	Mark both the Transparent and the Proxy check boxes.

Field	Description
<b>Exception Track</b>	Select the desired method for tracking exceptions. See the Check Point product documentation for more information.
<b>URI Match Specification Type</b>	Select <b>UFP</b> .

4. Select the **Match** tab, and complete the items in the tab.



URI Resource Properties – Match tab

Field	Description
<b>UFP server</b>	Select the OPSEC Application object that was created for the Websense UFP Server in <a href="#">Creating an OPSEC application object</a> , page 13.
<b>UFP caching control</b>	Select a caching option. <b>No caching</b> is the recommended setting for most networks.
<b>Categories</b>	Mark the <b>Blocked</b> check box.
<b>Ignore UFP server after connection failure</b>	<ul style="list-style-type: none"> <li>Mark this check box to permit full HTTP and FTP access if Websense Filtering Service is not running or cannot be contacted. Dependent fields allow you to set the number of times the Check Point product tries to contact Websense software before ignoring it, and the length of time the Check Point product ignores Websense software before attempting to reconnect.</li> <li>Clear this check box to block all HTTP and FTP access when Filtering Service is not running.</li> </ul>

5. Click **OK**.

6. Close the Resources dialog box.
7. Select **Policy** > **Install** to install the policy on the firewall.  
See Check Point product documentation for more information.

## Defining rules

---

This section describes a content filtering scenario and its configuration. It includes information about the objects and rules that are needed to implement the suggested configuration.



### Note

The configuration described in this section assumes that all clients have a default route set to the firewall and do not proxy to the firewall.

This configuration also assumes that the recommended network configuration is being used: Websense software is running on a separate machine, behind the firewall, and caching is disabled.

---

In this scenario, the Check Point product denies access to any site that Websense software indicates is blocked, and allows access to any site that Websense software indicates is not blocked. The actual sites blocked may vary according to the computer making the request.

Use TRITON - Web Security to define policies that block the appropriate categories, and assign them to the desired computers or directory objects.

For example, you might modify the Default policy to use a category filter that blocks access to all categories except the Travel, and Business and Economy categories. This policy is applied to most computers.

A separate, more liberal policy could be defined for managers, which blocks only those categories considered a liability risk, such as Adult Material and Gambling. This policy, called Management, would be assigned to the computers used by top managers.

After the Websense policies are configured, you define rules in the Check Point product to prevent access to any site that Websense software indicates is blocked.

To set up this configuration in the Check Point product, you must create one URI Resource Object and one Network Object, and define two rules.

- ◆ Create a URI Resource Object for the Blocked category as described in [Creating Resource Objects, page 16](#).

In this example, the URI Resource Object is called Blocked\_Sites because Websense software is configured to block sites that are not required for business purposes.

- ◆ Create a Network Object that encompasses all machines on the internal network. This example assumes that everyone in the company is on the internal network. For this example, the Network Object is called `Internal_Network`.
- ◆ Add the rules to the Security Rules Base. The sequence of the rules is important, because the Check Point product evaluates the rules sequentially, from top to bottom.

**RULE 1:** Blocks access to undesirable Web sites. Add the new rule at an appropriate location in the Rule Base:

<b>Name</b>	(NGX only) Enter a descriptive name for the rule, such as <b>Websense Block</b>
<b>Source</b>	Add <code>Internal_Network</code>
<b>Destination</b>	Any (default)
<b>Service</b>	Add with Resource In the Service with Resource dialog box, select <b>HTTP</b> . Under <b>Resource</b> , select <b>Blocked_Sites</b> from the drop-down menu. This object was created in <a href="#">Creating Resource Objects, page 16</a> .
<b>Action</b>	Reject
<b>Track</b>	None
<b>Install On</b>	Policy Targets
<b>Time</b>	Any (default)
<b>Comment</b>	(NGX only) Enter a more detailed description of the rule.

**RULE 2:** The second rule allows access to all other Web sites. Add the second rule *after* Rule 1.

<b>Name</b>	(NGX only) Enter a descriptive name for the rule, such as <b>Websense Allow</b>
<b>Source</b>	Add <code>Internal_Network</code>
<b>Destination</b>	Any (default)
<b>Service</b>	Add/HTTP
<b>Action</b>	Accept
<b>Track</b>	None
<b>Install On</b>	Policy Targets
<b>Time</b>	Any (default)
<b>Comment</b>	(NGX only) Enter a more detailed description of the rule.

The following illustrations provide examples of Security Rule Base after the rules are defined.

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION
1	websense Block	Internal_Network	* Any	* Any Traffic	HTTP http->Blocked_Sites	reject
2	websense Allow	Internal_Network	* Any	* Any Traffic	TCP http	accept
3	Clean-up Rule	* Any	* Any	* Any Traffic	* Any	drop

ACTION	TRACK	INSTALL ON	TIME	COMMENT
reject	- None	* Policy Targets	* Any	Blocks websites that Websense categorizes as Blocked.
accept	- None	* Policy Targets	* Any	Allows access to all other websites.
drop	- None	* Policy Targets	* Any	

Security Rule Base – Deny Blocked Categories Policy

After defining the rules described above, **Verify** and **Install** the policy from the **Policy** menu. See Check Point product documentation for more information.



**Important**

For normal operation, set **Track** to **None** in the Websense rules. This disables logging in the Check Point product.

When logging is enabled for these rules, the log files become very large, and adversely impact performance. Configure other options in the **Track** field only when you are testing and troubleshooting.

When the Check Point product receives an HTTP request, it sends Websense software the address of the requested site, as well as the IP address of the computer requesting the site.

For example, the CNN Web site is requested by a top manager. Websense software categorizes the site as News and Media. Websense software indicates that the site is Not Blocked under the Management policy that you defined in TRITON - Web Security. The Check Point product allows the site according to Rule 2.

If the CNN site was requested from an accounting clerk’s computer, Websense software indicates that the site is Blocked because that computer is governed by the Websense Default policy, which blocks the News and Media category. The Check Point product denies the request according to Rule 1, and a Block Page is displayed on the clerk’s computer.

Any time a computer requests a site not categorized by the Websense Master Database, Websense software indicates that the site is not in the database. The Check Point product allows access to the site according to Rule 2.

## Configuring enhanced UFP performance

Enhanced UFP performance improves the performance of the UFP Server by increasing the amount of traffic that Websense software and the Check Point product can filter while reducing CPU load.

Configuring enhanced UFP performance requires the proper settings in Websense Web Security or Websense Web Filter, and in the Check Point product. In order to use enhanced UFP Performance, clear communication is required between Websense software and the Check Point product.



### Note

Before performing the following procedures, make sure you have configured the Check Point product for content filtering with Websense software, as described earlier in this chapter.

## Websense configuration

Before configuring the Check Point product for enhanced UFP performance, open the **ufp.conf** file and make sure Websense software is configured for clear communication:

1. On the Websense Filtering Service machine, navigate to the directory where the Check Point integration files are installed. The default directories are:
  - **Windows:** C:\Program Files\Websense\bin
  - **Linux:** /opt/Websense/bin

2. Open the **ufp.conf** file in any text editor.

The file must contain the following line to be configured for clear communication:

```
ufp_server port 18182
```

Additional lines that appear in this file are used for Secure Internal Communication, and must be commented out using the comment symbol (#):

```
#ufp_server auth_port 18182
#opsec_sic_policy_file ufp_sic.conf
#opsec_sic_name "place_holder_for_opsec_SIC_name"
#opsec_sslca_file opsec.p12
```

3. Edit the file, if necessary, to match the commands in the previous step.
4. Save and close the **ufp.conf** file.
5. Stop and restart the Websense UFP Server:

- **Windows:** Use the Windows Services dialog box.
- **Linux:** Use the **./WebsenseAdmin restart** command.

See the *Installation Guide* for instructions on stopping and restarting Websense services. See also [Stopping and restarting the UFP Server](#), page 35.

## Check Point product configuration

To configure for enhanced UFP performance in the Check Point product:

- ◆ Configure the OPSEC Application object for the Websense UFP Server to operate in *early versions compatibility mode* (previously known as *backwards compatibility mode*) for clear communication.

Clear communication is the default for FireWall-1 NG with AI and FireWall-1 NGX. See [Early versions compatibility mode](#).

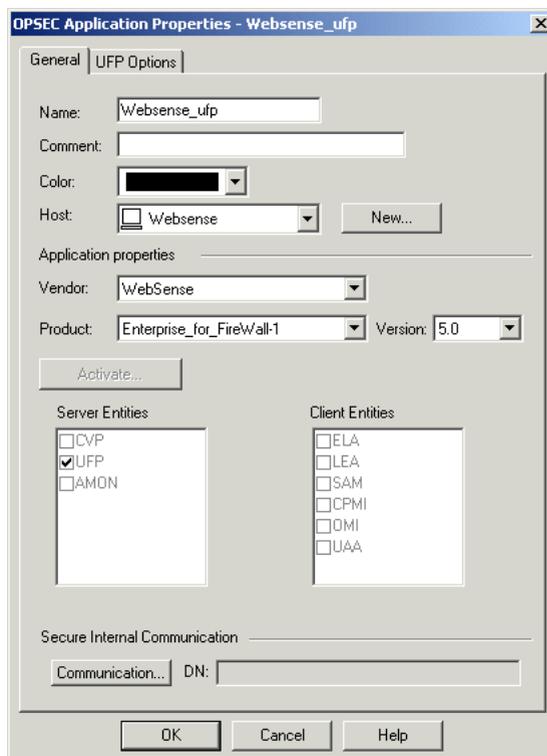
- ◆ Configure the URI Resource Object that identifies the Websense dictionary category Blocked for enhanced UFP performance. See [Enhanced UFP performance, page 23](#).

### Early versions compatibility mode

Follow these steps to configure the previously created OPSEC Application object for the Websense UFP Server to operate in early versions compatibility mode (clear communication) for enhanced UFP performance.

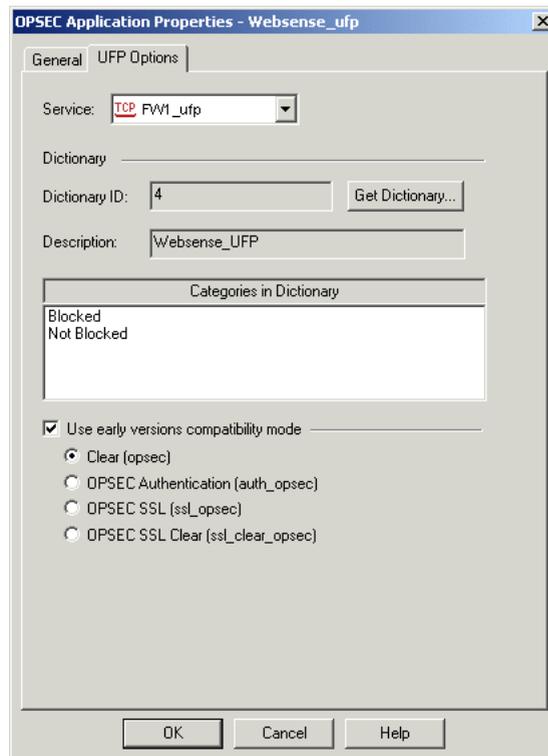
1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
2. Double-click on the OPSEC Application object you created for the Websense UFP Server in [Creating an OPSEC application object, page 13](#).

The OPSEC Application Properties dialog box for this object appears.



OPSEC Application Properties –  
General tab

3. Select the **UFP Options** tab.



OPSEC Application Properties – UFP Options tab,  
configured for enhanced UFP performance

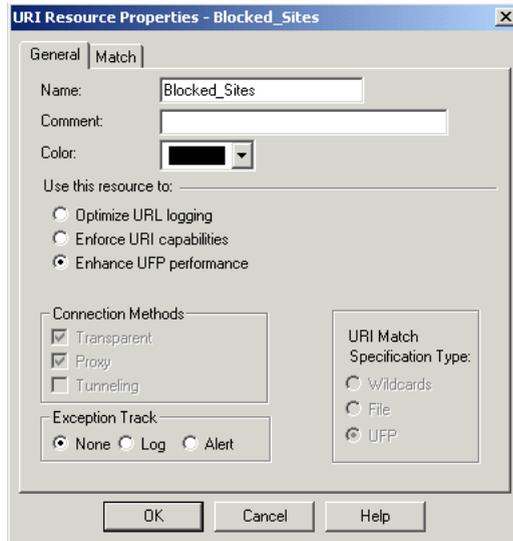
4. Select **Use early versions compatibility mode (Backwards Compatibility)** in earlier versions).
5. Select **Clear (opsec)**.
6. Click **OK**.
7. Close the Servers and OPSEC Applications dialog box.
8. Select **Policy > Install** to install the policy on the firewall. See Check Point product documentation for more information.

## Enhanced UFP performance

To configure the previously created URI Resource Object that identifies the Websense dictionary category Blocked for enhanced UFP performance:

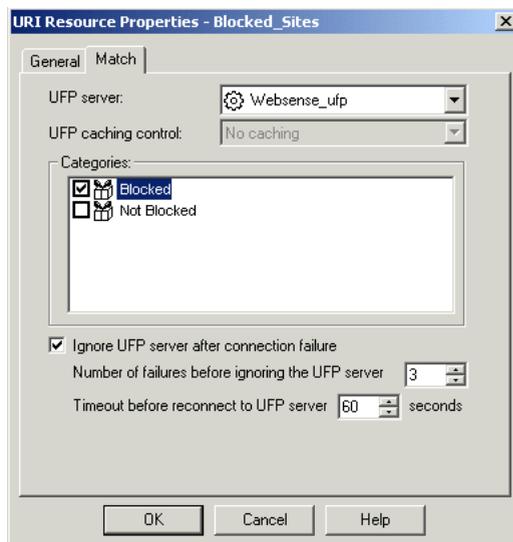
1. Open the SmartDashboard, and select **Manage > Resources**.  
The Resources dialog box appears.
2. Double-click on the Resource Object you created for the Websense dictionary category Blocked in *Creating Resource Objects*, page 16.

The URI Resource Properties dialog box for this resource appears.



URI Resource Properties – General tab, configured for enhanced UFP performance

3. In the **General** tab, select **Enhance UFP performance**.
4. Select the **Match** tab.



URI Resource Properties – Match tab, configured for enhanced UFP performance

5. Reselect the OPSEC Application object for the Websense UFP Server in the **UFP server** field. In this example, the object is named **Websense\_ufp**.
6. Clear and then mark the **Blocked** category, and click **OK**.
7. Close the Resources dialog box.
8. Select **Policy > Install** to install the policy on the firewall. See the Check Point product documentation for more information.

# A

## Troubleshooting

### Where can I find download and error messages?

Websense software creates **Websense.log** and **ufpserver.log** files when errors occur. These files are located in the Websense **bin** directory, (C:\Program Files\Websense\bin or /opt/Websense/bin, by default.)

These log files record error messages and other messages pertaining to database downloads. **Websense.log** is located only on the machine running Policy Server.

### The Master Database does not download

In addition to the subscription and access problems discussed in the Websense *Installation Guide*, a rule in the firewall could be blocking the download. Create a rule in the Check Point product at the top of the rule base that allows all traffic (outbound) from the Websense Filtering Service machine. If this test succeeds, move the rule down systematically until the problematic rule is found.

### Websense dictionary does not load in the Check Point product

The Get Dictionary process occurs between the Check Point SmartCenter Server and Websense Filtering Service. If the SmartCenter Server is not installed on the same machine as the Check Point Enforcement Module, you may need to configure the Check Point product to allow communication between the machines running the SmartCenter Server and Filtering Service. See *Distributed environments*, page 7, for more information.

Three causes are listed below as to why the dictionary might not load within the Check Point product.

#### Port mismatch

If the FW1\_ufp Service defined in the Check Point product uses a different port than Filtering Service filtering port (default 18182), Websense software cannot communicate with the Check Point product. As a result, the Check Point product cannot retrieve the Websense dictionary entries.

Check for mismatched port entries in the following locations:

- ◆ Check the FW1\_ufp Service definition in the Check Point product.
  1. From the Check Point client, choose **Manage > Services**.
  2. Select **FW1\_ufp** from the list of services.
  3. Click **Edit**.  
The TCP Services Properties dialog box appears.
  4. Make sure the port number displayed is the same as the port number defined for the filtering port when you installed Filtering Service.
- ◆ Open the **ufp.conf** file in a text editor. The file is located by default in the C:\Program Files\WebSense\bin\FW1 or /opt/WebSense/bin/FW1 directory. Check the port value to make sure it matches the port setting for the FW1\_ufp Service in the Check Point product.
- ◆ In the Check Point product, the filtering port specified in the **fwopsec.conf** file must match the port number set for the FW1\_ufp Service and the port defined in the WebSense **ufp.conf** file.



**Note**

If the SmartCenter Server and the Enforcement Module are installed on separate machines, both contain an **fwopsec.conf** file. You must reconcile the filtering port number in each of these files.

---

## Communication mismatch

If the WebSense dictionary does not load, check your communication settings. The method of communication selected in the OPSEC Application object must be consistent with that defined in the **ufp.conf** file (SIC or clear communication).

For example, if you have selected *early version compatibility* mode in the OPSEC Application Properties dialog box (see [Early versions compatibility mode, page 22](#)), the first line in the **ufp.conf** file must be:

```
ufp_server port 18182
```

If you have selected SIC, the first line in the **ufp.conf** file must be:

```
ufp_server auth_port 18182
```

## Policy properties

Although it is enabled by default, some environments need to disable the **Accept Outgoing Packet Originating from Gateway** setting in the Check Point product's policy properties. Since the firewall cannot send any traffic in this environment, it cannot request the dictionary.

To enable the dictionary request, add the following rule to the Rule Base anywhere before the cleanup rule:

<b>Source</b>	Check Point product workstation object
<b>Destination</b>	Any, or the Filtering Service workstation object
<b>Service</b>	FW1_ufp
<b>Action</b>	Accept
<b>Track</b>	Long (or any desired setting)
<b>Install On</b>	SRC ( <i>Required</i> )
<b>Time</b>	Any

## SIC trust configuration in FireWall-1 NG

When you click **Get Dictionary** in the **Match** tab of the URI Definition dialog box, FireWall-1 NG (Feature Pack 1 or later) contacts Websense Filtering Service via SIC trust to retrieve a list of categories for use in Check Point rules. If the SIC trust was not configured correctly, this contact fails and no categories can be retrieved.

To set up the SIC trust, see [Establishing Secure Internal Communication](#), page 29.

If you established the SIC trust, but still cannot get the dictionary, you can re-establish the trust.

1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.  
The Servers and OPSEC Applications dialog box appears.
2. Select the Websense UFP Server object in the list, and click **Edit**.  
The OPSEC Application Properties dialog box appears.
3. Click **Communication**.  
The Communications dialog box appears.
4. Click **Reset** to remove the SIC trust initialized previously, then click **Yes** in the confirmation dialog box that appears.
5. Click **Close** in the Communications dialog box.
6. Click **OK** to close the OPSEC Application Properties dialog box.
7. Click **Close** to close the Servers and OPSEC Applications dialog box.
8. Select **Policy > Install** to install the policy on the firewall.

9. Create the SIC trust again as described under *Establishing Secure Internal Communication*, page 29.



**Note**

*Do not* create a new OPSEC Application object for the Websense UFP Server; edit the object that already exists.

---

## No filtering occurs after enabling enhanced UFP performance

Users who have configured FireWall-1 NG with AI for enhanced UFP performance may not be able to filter Internet requests. This is a Check Point licensing issue and not a configuration problem. A license from an older version of NG cannot work with the newer version of NG with AI. Contact Check Point to update your license for your version of FireWall-1 NG with AI.

## FTP requests are not being blocked as expected

Websense software cannot block FTP requests when the Check Point product is configured to act as a proxy server.

The FTP request is sent as **ftp://**. The Check Point product then sends the packet to the Websense software with an **http://** header. Websense software performs a lookup against HTTP categories instead of performing a protocol lookup, and the FTP request is blocked or permitted according to the category assigned to the HTTP version of the same URL.

It is recommended that you use the capability of the Check Point product to block the FTP protocol.

1. In the Check Point product, create a rule that blocks on the FTP service. See Check Point product documentation for more information.
2. Place this rule above the Websense rule.
3. Save the policy.

Users receive the Check Point block page instead of the Websense block page.



**Note**

In this case, it is not necessary to set the FTP protocol to be blocked in TRITON - Web Security.

---

# B

## Configuring Communications

Secure Internal Communication (SIC) may be needed when you integrate a Check Point product with Websense software. Following are instructions for enabling this communication method, as well as instructions for disabling this communication method (see [Restoring Clear Communication](#), page 37).

### Establishing Secure Internal Communication

---

If Websense software is integrated with a FireWall-1 NG version, you can configure both programs to use Secure Internal Communication (SIC). A secure connection requires that communication between the Check Point product and the Websense UFP Server be authenticated before any data is exchanged.



---

#### Note

The use of SIC with Websense software creates performance problems and is not recommended for networks with more than 100 users.

---

After installing Filtering Service, establish an SIC trust between the Check Point product and Websense software:

- ◆ Configure the OPSEC Application object for the Websense UFP Server within the Check Point product to use Secure Internal Communication. See [Configuring the Check Point product to use SIC](#), page 31.
- ◆ Configure Websense software to use Secure Internal Communication. See [Configuring Websense software to use SIC](#), page 33.
- ◆ Update the OPSEC Application object within the Check Point product to receive secure communications from Websense software. See [Updating the OPSEC Application object](#), page 35.

## Prerequisites

The following must be completed before you begin to configure the Check Point product to communicate with Websense software, as described in Chapter 2 of this Supplement.

- ◆ Both the Check Point product and Websense software must already be installed and running.
- ◆ In the Check Point product, create the following objects:
  - An object for the firewall. Consult Check Point product documentation for instructions.
  - Network Objects that represent your network topology (as needed for your filtering goals) must exist. Consult Check Point product documentation for instructions.
  - You must create the OPSEC Application object for the Websense UFP Server before Websense software can establish SIC. If you have not already done this, see the procedures in [Creating an OPSEC application object, page 13](#).



### Note

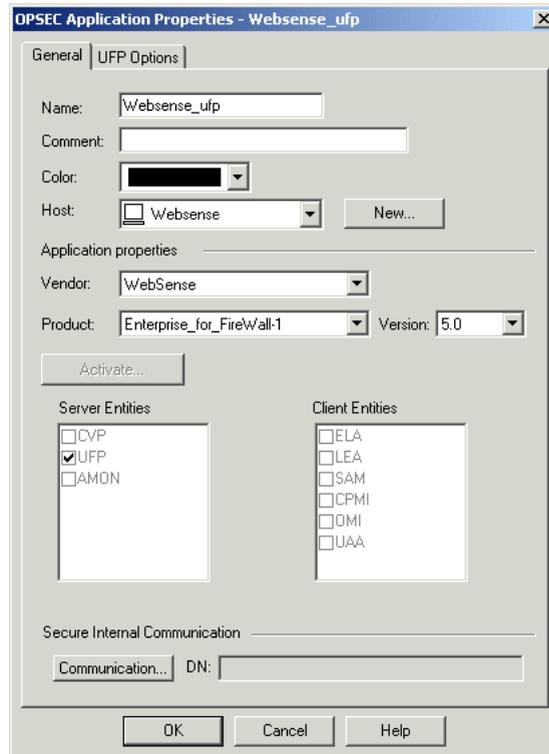
Do **not** perform the procedures in this section if you are using an earlier version of FireWall-1 (before FireWall-1 NG Feature Pack 1).

---

## Configuring the Check Point product to use SIC

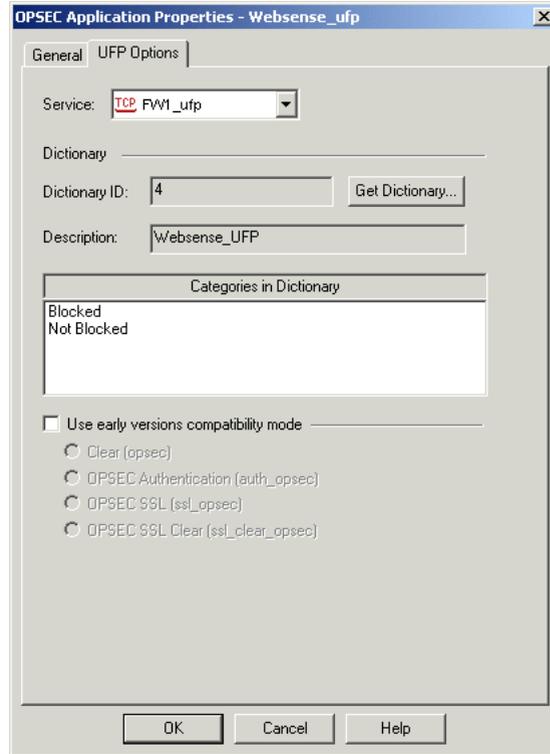
1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
2. Double-click the OPSEC Application object you created for the Websense UFP Server in *Creating an OPSEC application object*, page 13.

The OPSEC Application Properties dialog box for this object appears.



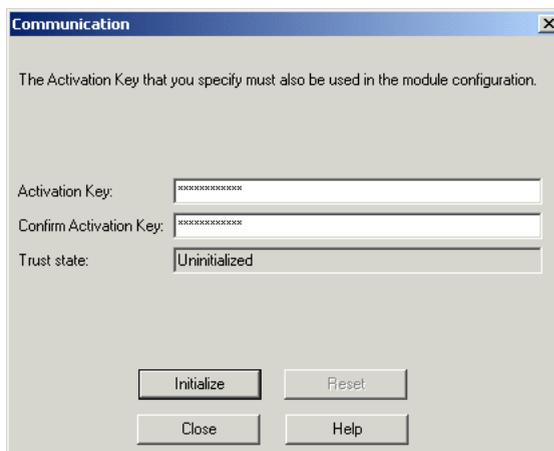
OPSEC Application Properties – General tab

3. If clear communication (for early version compatibility mode) is enabled, disable it:
  - a. Go to the **UFP Options** tab of the OPSEC Application Properties dialog box for this object.



- b. Make sure the **Use early versions compatibility mode** check box is *not* selected. (This field was called **Use backwards compatibility mode** in earlier versions.)
4. Click **Communication**.

The Communication dialog box appears.



Communication Dialog Box

5. Enter and confirm an **Activation Key** (password) for communication between Websense Filtering Service and the Check Point product. (Make a note of this password for later use.)
6. Click **Initialize**.  
The **Trust state** field must show **Initialized but trust not established**.
7. Click **Close** to return to the OPSEC Application Properties dialog box.
8. Click **OK**.
9. Close the Servers and OPSEC Applications dialog box.
10. Select **Policy > Install** to install the policy on the firewall. See the Check Point product documentation for more information.

## Configuring Websense software to use SIC

Use this procedure to obtain a SIC certificate from the Check Point product, and configure Websense software to use it. After you complete this procedure, Websense software sends this certificate each time it communicates with the Check Point product.

1. Open a command prompt on the Websense Filtering Service machine and navigate to the directory containing the Check Point integration files (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).
2. Enter the following command:

```
opsec_pull_cert -h <host> -n <object> -p <password> -o <path>
```

The table below explains the variables for this command.

Variable	Description
<host>	The IP address or machine name of the computer on which the SmartCenter Server (Management Server in earlier versions) is installed. This IP address may be the same machine as the Enforcement (FireWall) Module or a different machine.
<object>	The name of the OPSEC Application object created for the Websense UFP Server.
<password>	The activation key that you entered for the named OPSEC Application object. See <a href="#">Configuring the Check Point product to use SIC</a> , page 31.
<path>	Path to the output certificate file, <b>opsec.p12</b> . This variable must be expressed as a complete path. <ul style="list-style-type: none"> <li>• If the OPSECDIR variable already exists, the default path is <b>\$OPSECDIR/opsec.p12</b>.</li> <li>• If the OPSECDIR variable does not exist, the opsec.p12 file is created in the same folder as the <b>opsec_pull_cert.exe</b> file (Websense\bin or Websense/bin/FW1).</li> </ul>

This command contacts the firewall and downloads the Secure Internal Communication certificate that authorizes Websense software to communicate with the Check Point product, and saves the certificate in a file, **opsec.p12**.

The command line displays information similar to the following example:

```
opsec_pull_cert -h 10.201.254.245 -n Websense_UFP -p
firewall -o "C:\Program Files\Websense\bin\opsec.p12"
The full entity sic name is:
CN=Websense_UFP,0=fw1_server..dwz26v
Certificate was created successfully and written to
"opsec.p12".
```

3. Write down the SIC name displayed by the `opsec_pull_cert` command.

In the example above, the SIC name is:

```
CN=Websense_UFP,0=fw1_server..dwz26v
```

4. Open the **ufp.conf** file, located by default in the `C:\Program Files\Websense\bin` or `/opt/Websense/bin` directory.

The default file contains the following syntax:

```
ufp_server port 18182
#ufp_server auth_port 18182
#opsec_sic_policy_file ufp_sic.conf
#opsec_sic_name "place_holder_for_opsec_SIC_name"
#opsec_sslca_file opsec.p12
```

The first line is used for clear communication.

The remaining lines are used for SIC. If the file does not contain the lines for SIC shown above, enter them.

5. To enable secure communication, comment out the first line and remove the comment symbol (#) from the remaining four lines.

```
#ufp_server port 18182
ufp_server auth_port 18182
opsec_sic_policy_file ufp_sic.conf
opsec_sic_name "place_holder_for_opsec_SIC_name"
opsec_sslca_file opsec.p12
```

6. On the **opsec\_sic\_name** line, replace the placeholder with the SIC name recorded in [Step 3](#).

The name must be enclosed in quotation marks. For example:

```
opsec_sic_name "CN=Websense_UFP,0=fw1_server..dwz26v"
```

The completed file:

```
#ufp_server port 18182
ufp_server auth_port 18182
opsec_sic_policy_file ufp_sic.conf
opsec_sic_name "CN=Websense_UFP,0=fw1_server..dwz26v"
opsec_sslca_file opsec.p12
```

7. Save and close the file.

8. Stop and restart the Websense UFP Server:
  - **Windows:** Use the Windows Services dialog box.
  - **Linux:** Use the `./WebsenseAdmin restart` command.

See the *Installation Guide* for instructions on stopping and restarting Websense services. See also [Stopping and restarting the UFP Server](#), below.

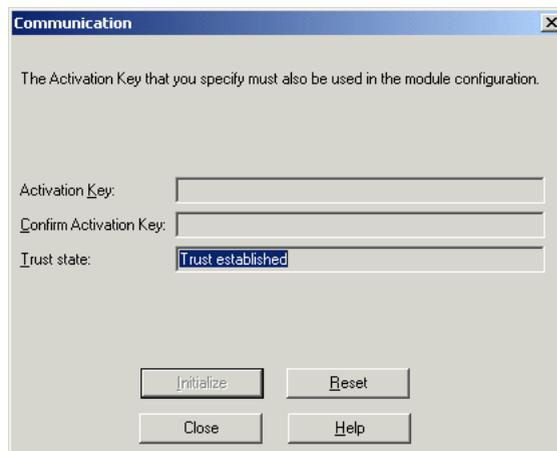
## Stopping and restarting the UFP Server

Filtering Service must be running for the Websense UFP Server to function. When the Filtering Service is stopped, the UFP Server is automatically shut down. The UFP Server must be restarted manually. If the UFP Server is started first, it automatically starts the Filtering Service. Stopping or starting the UFP Server while the Filtering Service is running has no effect on the Filtering Service.

## Updating the OPSEC Application object

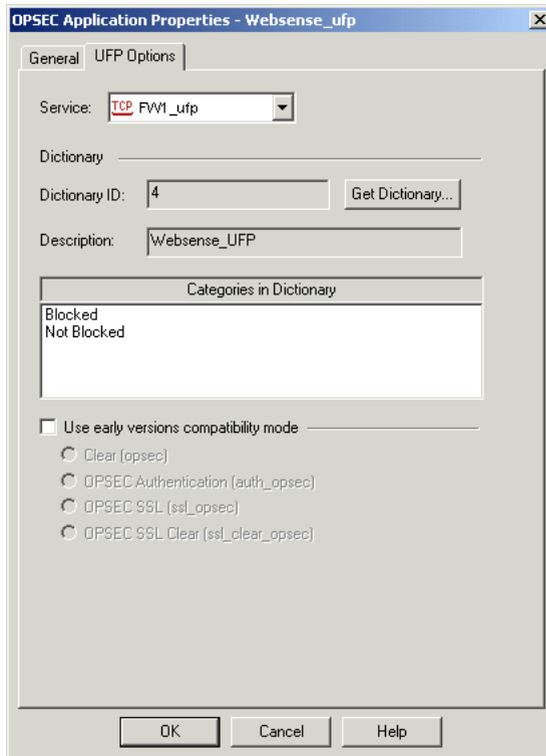
After Websense software has been configured to use SIC, update the OPSEC Application object created for the Websense UFP Server.

1. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
2. Double-click on the OPSEC Application object you created for the Websense UFP Server in [Creating an OPSEC application object](#), page 13.  
The OPSEC Application Properties dialog box for this object appears.
3. Click **Communication**.
4. Verify that the **Trust state** field shows **Trust established**.



5. Click **Close** to return to the OPSEC Application Properties dialog box.
6. Click **OK**.
7. Close the Servers and OPSEC Applications dialog box.
8. Select **Policy > Install** to install the policy on the firewall. See Check Point product documentation for more information.

9. Open the OPSEC Application object created for the Websense UFP Server again.
10. Go to the **UFP Options** tab of the OPSEC Application Properties dialog box for this object.



11. Make sure the **Use early versions compatibility mode** check box is *not* selected. (This field was called **Use backwards compatibility mode** in earlier versions.)
12. Click **Get Dictionary**.

Websense software provides the Check Point product with a dictionary of 2 categories: Blocked and Not Blocked. The full set of Websense categories is configured through TRITON - Web Security.

See TRITON - Web Security Help for more information.



### Important

Before continuing, make sure the **Use early versions compatibility mode** check box is *not* selected.

13. Click **OK**.
14. Close the Servers and OPSEC Applications dialog box.
15. Select **Policy > Install** to install the policy on the firewall. See Check Point product documentation for additional information.

The SIC trust is established now between Websense software and the Check Point product. Continue with the configuration in [Creating Resource Objects](#), page 16.

## Restoring Clear Communication

To restore clear communication (*early versions compatibility* mode) on a system configured for Secure Internal Communication (SIC):

1. On the Websense Filtering Service machine, navigate to the directory where the Check Point integration files are installed (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).

2. Open the **ufp.conf** file in any text editor.

When the Check Point product is configured for SIC, this file contains the following syntax:

```
#ufp_server port 18182
ufp_server auth_port 18182
opsec_sic_policy_file ufp_sic.conf
opsec_sic_name "place_holder_for_opsec_SIC_name"
opsec_sslca_file opsec.p12
```

When SIC is fully configured, the contents of the quotation marks in line 4 are replaced with an actual `opsec_SIC_name`, such as  
CN=Websense\_UFP,0=fw1\_server..dwz26v

3. To restore clear communication, remove the comment symbol (#) from the first line, and comment out the remaining lines:

```
ufp_server port 18182
#ufp_server auth_port 18182
#opsec_sic_policy_file ufp_sic.conf
#opsec_sic_name "place_holder_for_opsec_SIC_name"
#opsec_sslca_file opsec.p12
```

4. Save the file.

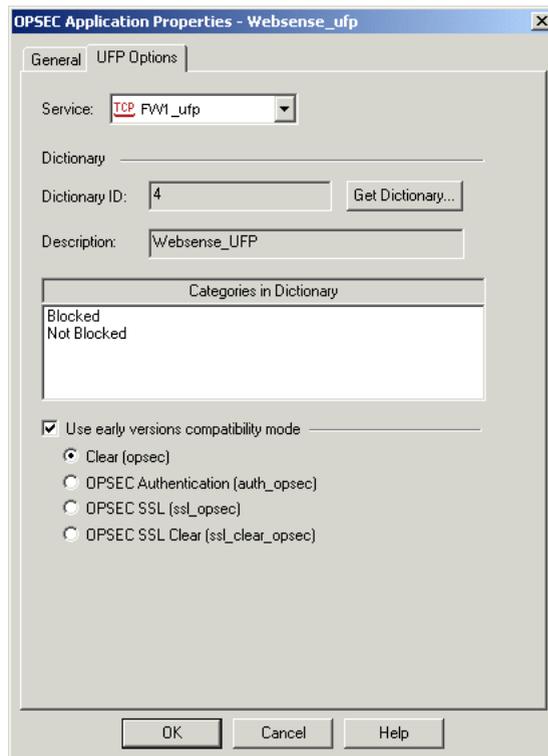
5. Stop and start the Websense UFP Server:

- **Windows:** Use the Windows Services dialog box.
- **Linux:** Use the `./WebsenseAdmin restart` command.

See the *Installation Guide* for instructions on stopping and restarting Websense services. See also [Stopping and restarting the UFP Server](#), page 35.

6. Open the SmartDashboard, and select **Manage > Servers and OPSEC Applications**.
7. Double-click on the OPSEC Application object for the Websense UFP Server. The OPSEC Application Properties dialog box for this object appears.
8. Click **Communication**.  
The Communication dialog box appears.
9. Click **Reset** to revoke the SIC certificate and stop SIC.  
A confirmation dialog box is displayed.
10. Click **Yes** to continue.
11. Click **Close** to return to the OPSEC Application Properties dialog box.

12. Go to the **UFP Options** tab.



13. Check the **Use early versions compatibility mode** option (**Backwards Compatibility** in earlier versions of FireWall-1 NG).
14. Select **Clear (opsec)**.
15. Click **Get Dictionary**.  
Websense software provides the Check Point product with a dictionary of 2 categories: Blocked and Not Blocked. The full set of Websense categories is configured via TRITON - Web Security.
16. Click **OK**.
17. Close the OPSEC Applications dialog box.
18. Select **Policy > Install** to install the policy on the firewall. See Check Point product documentation for more information.

# Index

## A

activation key, 33

## C

clear communication, 37–38  
client computers, 7  
communicating with Websense software, 7  
creating OPSEC Application objects, 13–15

## D

dictionary  
    fails to load, 25–28  
    in FireWall-1 NG, NG with AI, and NGX, 15, 38  
    policy properties in Check Point, 27  
Distributed environments, 7

## E

Enhanced UFP performance  
    configuring, 21  
error messages  
    location of, 25

## F

Filtering Service  
    defined, 5  
FireWall-1 NG  
    clear communication, 37–38  
    configuration tasks, 11  
    creating resource objects, 16–18  
    defining rules for, 18–20  
    Secure Internal Communication (SIC) with, 29–36  
FireWall-1 NG with AI  
    clear communication, 37–38  
    configuration tasks, 11  
    configuring Enhanced UFP Performance, 21–24  
    creating resource objects, 16–18  
    defining rules for, 18–20  
    Secure Internal Communication (SIC) with, 29–36  
FireWall-1 NGX  
    clear communication, 37–38  
    configuration tasks, 11  
    configuring Enhanced UFP Performance, 21–24  
    creating resource objects, 16–18

defining rules for, 18–20  
Secure Internal Communication (SIC) with, 29–36

## I

integrating with Check Point products, 5–6

## M

Master Database download  
    error message location, 25

## N

Network Agent  
    defined, 5

## O

OPSEC application objects  
    creating, 13–15  
opsec\_pull\_cert command, 33

## P

port numbers  
    Check Point messages, 6  
    errors caused by mismatch, 25

## R

Resource Objects  
    creating  
        NG, NG with AI, NGX, 16–18  
rules, defining  
    NG, NG with AI, NGX, 18–20

## S

Secure Internal Communication (SIC)  
    OPSEC application object  
        creating, 30–33  
        updating, 35–36  
    prerequisites, 30  
    troubleshooting the SIC trust, 27–28  
    Websense configuration for, 33–35

## U

UFP Server  
    stopping, 35  
ufp.conf file, 34

---

upgrading  
migrating to a newer Check Point version, 10

## W

Websense.log, 25