



Preventing Access by Desktop Search Engines to iGate Protected Resources

This document describes how to set iGate policies that will prevent access by Desktop Search Engines to iGate SSL VPN protected resources.

The Vulnerability Created by Desktop Search Engines

New PC indexing tools, such as Google Desktop Search, pose security risks to businesses that use SSL remote access. These search tools copy material accessed during SSL sessions and make it available to unauthorized people who later use the same PC.

Caches created by PC search tools combat the security controls many SSL vendors have put in place to purge cached data from remote machines as secure sessions shut down. These so-called cache-cleaning agents erase temporary files created during SSL sessions, but they don't erase the copies made by the search tools.

iGate Policies—A Resolution to the Issue

To solve this problem for our customers, the SafeNet iGate uses policies to detect whether Google Desktop Search is running on a remote PC. If so, access to the corporate network is denied or restricted.


With the iGate and its end-point security features, you can set a client product policy to check if one of these desktop search engines is running on the client machine. Based on the results of this check, you can prevent access to some or all applications.

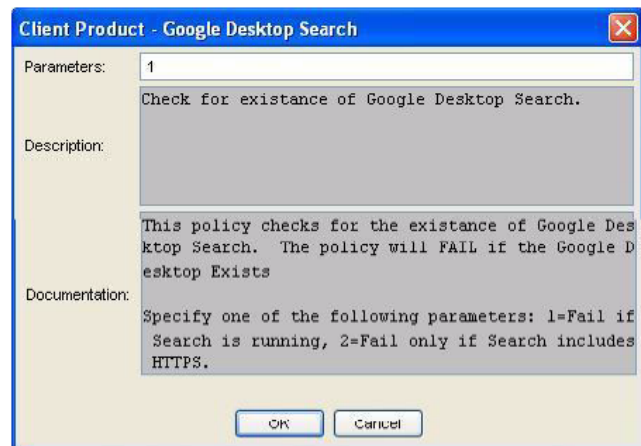
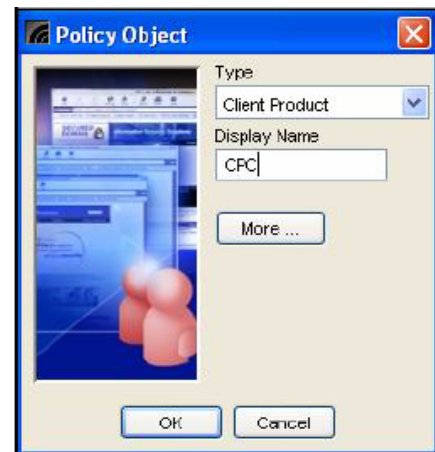
The SafeEnterprise™ SSL iGate Client Policy Feature (ICPF) is a system whereby policies can be assigned to users, groups, roles, and site/application resources. Policies are represented in iGate by Policy Objects. Each Policy Object represents a test that will be evaluated when a user accesses an iGate and its resources. The administrator can assign Policy Objects to individual users, groups, roles, sites, applications, or other iGate resources.

Setting Up Policy Checks for the Google Desktop Search Engine

iGate's Client Product Policy enables you to check if the Google Desktop Search engine is running on the client machine. The policy checks can be defined using either Access Control Manager (ACM) or Simple Web Administration.

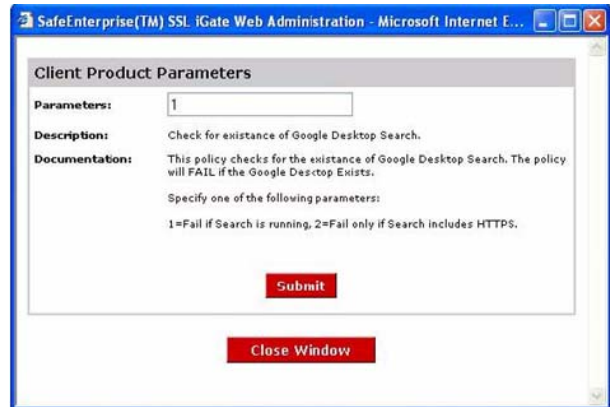
Setting Up Policy Checks with ACM

1. Start the Access Control Manager.
2. Download the existing ACL from the iGate. For detailed instructions, see the ACM online Help.
3. In the navigation pane, click **Policy Objects**. The **Policy Object** working pane appears.
4. Click **Add**. The **Policy Object** dialog box appears.
5. From the **Type** drop-down list, select **Client Product**.
6. In the **Display Name** field, enter the display name you want for the policy.
7. Click **More**. The **Client Software Installation** dialog box appears.
8. Select the **Google Desktop Search** check box.
9. Click **Specify parameters** to specify the parameter name for the selected Client Software Product and to view its description. Enter your checks in the **Parameters** field. (See "Specifying Parameters for the Google Desktop Search Client product" on page 4.)
10. Click **OK** to close each dialog box. You will be returned to the **Policy Object** working pane.
11. Click **Apply**.
12. Click the **Upload** button  to upload the ACL to the iGate so that your changes will take effect on the appliance.



Setting Up Policy Checks with Simple Web Administration

1. Log in to Simple Web Administration from any computer on your network. Simply type the IP address of the iGate's admin interface into your web browser's address field.
2. On the left-hand side of the page, click **Define Policy Restrictions**.
3. In the **Policy Name** field, enter a name for the policy.
4. Scroll down to select the **Check Client Product** check box.
5. In the **Client** product list on the right, select **Google Desktop Search**.
6. Click **Specify parameters** to specify the parameter name for the Google Desktop Search Tool and to view its description. Enter your checks in the **Parameters** field. (See “Specifying Parameters for the Google Desktop Search Client product” on page 4.)
7. Click **Submit**.
8. Click **Close Window**.
9. Click **Add Policy** to add the policy to the iGate.



Specifying Parameters for the Google Desktop Search Client

The following table illustrates the parameters that can be set for the **Google Desktop Search** client:

Software Product	Description	Parameter Format
<ul style="list-style-type: none"> □ Google Desktop Search 	Checks for the existence of Google Desktop Search .	<ul style="list-style-type: none"> □ 1 - When specified in the Parameters field, it checks if the Google Desktop Search is running on the client machine. The policy fails if it detects the Google Desktop Search Tool running on the client machine and access to the protected resource is denied. □ 2 -When specified in the Parameters field, it checks for <i>HTTPS Indexing</i> being OFF (deselected) in the Google Desktop Search Tool Preferences. If <i>HTTPS Indexing</i> is ON (selected) in the Google Desktop Search Tool Preferences, then the policy fails and access to the protected resource is denied.

© Copyright 2004, SafeNet, Inc. (Baltimore) All rights reserved.

All attempts have been made to make the information in this document complete and accurate. SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SafeEnterprise[™] SSL iGate is a trademark of SafeNet, Inc. All other product names referenced herein are trademarks or registered trademarks of their respective manufacturers.

Software versions 4.0.1 and later.

Revision	Action/Change	Date
A	Initial Release	November 2004