



Check Point Check Point Web Visualization Tool

December 2003

<http://www.checkpoint.com>

In This Document

“Need for Web Visualization” on page 1
“The Web Visualization Solution” on page 1
“Configuration” on page 1
“Acknowledgement” on page 4

Need for Web Visualization

Many players in an organization have the need to view a Security Policy. They do not necessarily want, nor are they necessarily permitted to organize or manage the Security Policy via SmartDashboard and the SmartCenter Server. For instance, an ISP can provide Read Only access to its customers who would like to view their security profile. In this scenario, the customer’s security profile is administrated by the ISP; therefore, the customers are only granted visuals.

The Web Visualization Solution

The Web Visualization solution allows the Security Policy as well as objects in the objects database to be exported into a readable format. This exported information represents a snapshot of the database. This Security Policy can be viewed by anyone who is not connected to the SmartCenter in real time. Professionals such as Security auditors and IT support engineers who are mobile, need this capability on a daily basis.

The Security Policy can be exported in any of the following formats:

HTML — HTML will most likely be the common format of choice for the majority of users because:

- it is extremely simple to use
- it concentrates the information into a single HTML file
- it can be viewed by all major web browsers thereby making it accessible to the widest range of users

The information is sorted according to type and in alphabetical order. For example, all Gateways will be displayed one beneath the other in alphabetical order.

XML — XML will most likely be the choice of users who meet one of the following requirements:

- users who would like to view the Security Policy in a more sophisticated manner. The data is divided into logical segments which can be viewed separately. It includes icons which are similar to the icons used in SmartDashboard. These icons are familiar to Check Point users and are helpful in the categorization of objects.
- users who would like to customize the way that the Security Policy is viewed, using XSL
- users who would like to utilize some or all of the data in the XML files for other means and purposes, such as using the data in other applications that can read XML.

The Security Policy is gathered into several XML files. Each XML file represents an object table or a Rule Base.



Note – If your browser is not able to view XML data with XSL, please install a patch provided by Microsoft at: <http://msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/MSDN-FILES/027/001/772/msdncompositedoc.xml&frame=true>

Configuration

The HTML utility and the XML utility are two separate standalone Command Line utilities which can both be used in order to implement Web Visualization. The HTML utility is likely to be the utility of choice because of its simplicity.

The HTML Utility

During the running of the HTML utility an HTML file is generated. By default the HTML file is named 1.html. In order to generate a single HTML file, run the following command from the SmartCenter Server.

```
cpdb2html <cpdb2html_path> <output_directory> <SmartCenter_Server>
<admin_name> <password> [-o output_file_name] [-m host_name] [-gr] [-go]
```

where,

cpdb2html_path is the Web Visualization Tool's root directory.

output_directory is the path to where the html file will be written.

SmartCenter_Server is the name or IP address of the Management server. In Provider-1 this should be the virtual IP address associated with the CMA.

admin_name is the user name of the Smart Server administrator.

password is the administrator's password.

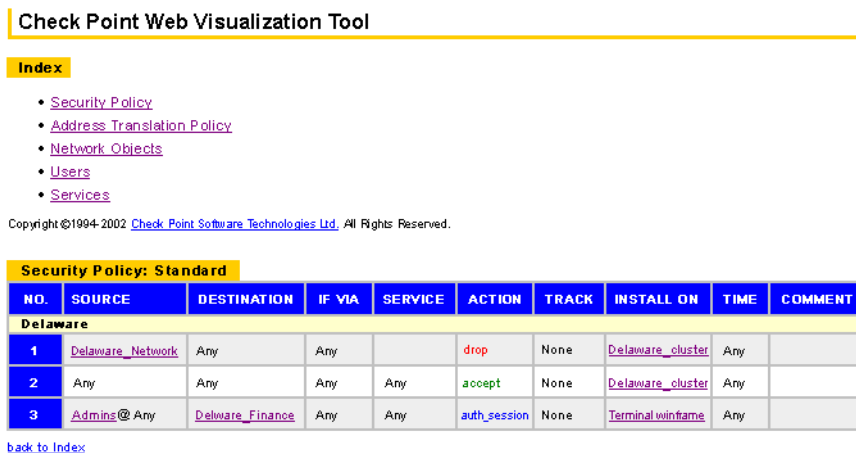
-o output_file_name is the name of the HTML file that will be generated, (where the default file name is 1.html).

-m host_name is the name of the module whose database you would like to see.

-gr is for Check Point Provider-1 users only. When this option is set the output includes customer rules only, (no global rules).

-go is for Check Point Provider-1 users only. When this option is set the output will include customer objects only (no global objects).

FIGURE 1 HTML Index Page



The XML Utility

During the running of the XML utility, several XML files are generated. Run the SmartCenter Server in order to export your Policy information to XML files:

```
cpdb2web [-s SmartCenter Server] [-u admin name | -a certificate file]
[-p password] [-o output file path] [-t tables names] [-c | -m host mane
| -l packages names] [-gr] [-go]
```

Where,

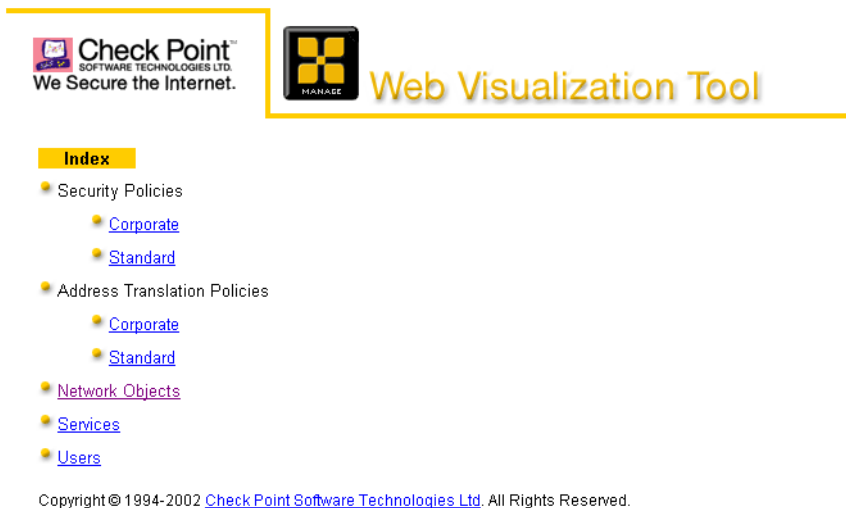
-s SmartCenter Server is the name or IP Address of the SmartCenter Server. In Provider-1 the host should be the virtual IP Address of the CMA.

-u admin name is the name of the Check Point administrator who has permissions for reading the Check Point objects.

-a certificate file is the path of a Check Point certificate for the administrator who has permissions for reading the Check Point objects.

- p password is the password of the Check Point administrator who has permissions for reading the Check Point objects.
- o output file path is the full path for the output files. The XML files should be placed in the XML subdirectory of the XSL directory which comes with the package, since all related files should be stored in the XSL directory.
- t tables names is an optional parameter that allows you to specify a specific table (where all available scheme tables can be used). In order to export a list of tables, the tables names should be printed using a comma as a separator. Spaces cannot be used as a separator. If this parameter isn't specified, all the default tables (including Policies, Network Objects, Services, Users and Communities) will be exported. However; the initial export operation of the Communities scheme table will not include the GUI.
- c this is an optional parameter that triggers the exporting of the active Policy Package only, instead of exporting all existing Policy Packages by default. The active Policy Package is the Policy Package that is currently open in SmartDashboard.
- m the same as the -c option, it triggers the exporting of the active Policy Package only, but only on the given host.
- l packages names this is an optional parameter that allows you to export a specific Policy Package, instead of exporting all existing Policy Packages by default. In order to export a list of packages, the packages names should be printed using a comma as a separator. Spaces cannot be used as separators..
- gr is an optional parameter relevant to Provider-1 users only. When this is switched on, the output does not include Global Rules, but rather it contains Customer Rules only.
- go is an optional parameter relevant to Provider-1 users only. When this is switched on, the output does not include Global Objects, but rather it contains Customer objects only.

FIGURE 2 XML Index Page

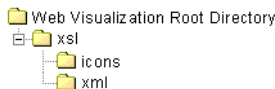


The XML Files Structure

The XML Files structure is a fixed structure which needs to be maintained in order to view the Security Policy in XML using XSL. This structure is as follows:

In the root directory where all the Check Point executables are located, there is a sub directory called XSL. This sub directory includes all XSL files as well as a file called index.xml which is the file to be opened in order to view the Security Policy. Beneath the XSL directory there are two sub directories Icons and XML, where the former includes the familiar Check Point icons used in SmartDashboard and the latter should include all XML files generated by the XML Generation utility. The XML directory is the only directory that can be edited by the user.

FIGURE 3 Web Visualization Root Directory.







In order to view the XML static files as a Security Policy, the structure of the directories from XSL up to and including XML, need to be maintained.

FIGURE 4 XML Network Objects table with Icons

Network Objects

[back to Index](#)

	Name	Type	IP	Netmask	Products Installed	Nat Address	Members	Version	Comments
	dsshield	Dynamic Object	-	-	-	-	-	-	-
	California_GW	Check Point Gateway	192.7.100.2	-	SVN Foundation FireWall-1	-	-	-	-
	DAG_range	Address Range	-	-	-	-	-	-	-
	California_controller	Check Point Host	172.16.2.16	-	SVN Foundation	-	-	-	-

[back to Index](#)

Acknowledgement

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