

NP-View Documentation for Check Point R80

Last Updated July 17, 2023

The team at Network Perception has added support for Check Point R80 through an API connector. This document presents a step-by-step testing procedure to ensure that the connector works as expected.

Overview:

The configuration exporter is read-only and connects to port TCP/443 (HTTPS) of the Check Point management server. The following API calls are made:

- run-script netstat -rn
- show-{gateways-and-servers, global-assignments, packages, access-rulebase, groups, networks, hosts, address-ranges, multicast-address-ranges, groups-with-exclusion, simple-gateways, security-zones, dynamic-objects, dns-domains, access-roles, service-groups, services-tcp, services-udp, services-icmp, services-icmp6, services-sctp, services-other, services-dce-rpc, services-rpc, application-site-groups, application-site-categories, application-sites, vpn-communities-meshed, vpn-communities-star, show-mdss}

To learn more about the Check Point API, please visit:

<https://sc1.checkpoint.com/documents/latest/APIs/>

To see a demo of the connector, check out the video:

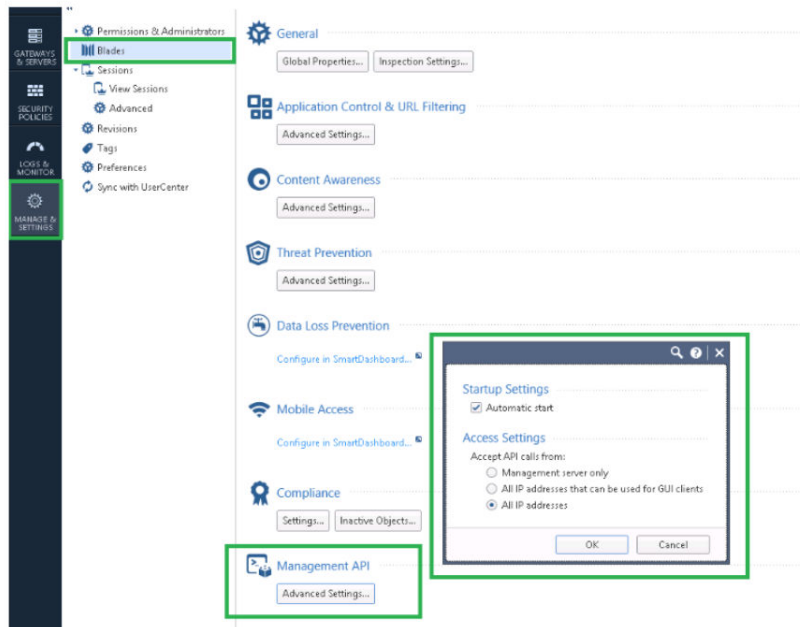
<https://www.youtube.com/watch?v=wziBm0prAHE>

Prerequisites:

- Download the checkpoint R80 config exporter:
https://download.network-perception.com/R80_for_KB/checkpoint_r80_exporter.zip
shasum: cc3131da37362da1291fa4a77cd8496fcb010596

Instructions to retrieve the R80 configuration file:

- **Step 1:** ensure that the Check Point R80 API is enabled and your workstation can connect to it:



Note: Access Settings can be set to "All IP addresses" or "All IP addresses that can be used for GUI clients". This can also be configured through the CLI with the commands:

- `mgmt_cli -r true --domain MDS set api-settings accepted-api-calls-from "all ip addresses" api restart`

or

- `mgmt_cli -r true --domain MDS set api-settings accepted-api-calls-from "all ip addresses that can be used for gui clients" api restart`

- **Step 2:** extract the archive `checkpoint_r80_exporter.zip`
- **Step 3:** open a Windows CMD terminal and run the executable `checkpoint_r80_exporter.exe` extracted from the archive
- **Step 4:** answer the command line prompt:
 - Management server ip or name
 - Apache GAIA port (default is 443)
 - Expert user name
 - Expert user password
 - (optional if using MDS) MDS server name
 - (optional if using MDS) name of domain to export
 - (optional if using RSA authentication) other password to log into domains

```

Command Prompt - checkpoint_r80_exporter.exe
10:28:56 - INFO CheckPoint R80 Exporter 2.1
(type ctrl-C at any time to abort execution)

R80 Management server address? checkpoint-r80-cma
Web API port (type Enter to use default 443)?
Expert user? admin
Expert password?
10:29:13 - INFO Logging as user admin
10:29:16 - INFO Connection to CheckPoint server checkpoint-r80-cma successful with session gzHG7mivQs1fg_c_zbr3mn1Tpmv4WzYc9Wh
DzhQv-Uk and uid 77a0492f-c711-488b-bb7c-88d99c7f9cf6
10:29:16 - INFO show-mdss (('details-level': 'standard')) successful
10:29:16 - INFO Identified 1 MDS(s) checkpoint-r80-cma
10:29:16 - INFO Connecting to multi-domain server checkpoint-r80-cma to get list of domains
10:29:17 - INFO show-mds (('name': 'checkpoint-r80-cma', 'details-level': 'standard')) successful
10:29:17 - INFO Identified 1 domain(s) east
10:29:17 - INFO Invoking show-global-assignments with params {'limit': 50, 'offset': 0, 'details-level': 'full'}
10:29:18 - INFO show-global-assignments - DB has a total of 1 object(s) - got 1
10:29:18 - INFO show-global-assignments (('limit': 50, 'offset': 0, 'details-level': 'full')) successful
A second login is needed to access domain-specific information.
Are you using RSA tokens or need to provide different credentials to log into domain east? Type y/N
  
```

- Alternatively, you can provide the option directly on the command line:

```
export_checkpoint_r80_config.exe -s 10.1.1.1 -u
admin -p <password> -mds MDS-1-R80.20 -d USA
```

```

Command Prompt - checkpoint_r80_exporter.exe -h
# checkpoint_r80_exporter.exe -h
usage: checkpoint_r80_exporter.exe [-h] [-o output_dir] [-s R80 server]
                                  [-u username] [-p password] [-port port]
                                  [-proxy_host proxy_host]
                                  [-proxy_port proxy_port] [-mds mds]
                                  [-domain domain] [--test function_name]
                                  [-xp] [--version]

Connect to Checkpoint R80 management server and export configuration to .json
file

optional arguments:
  -h, --help            show this help message and exit
  -o output_dir         where to store configuration file (.json)
  -s R80 server         management server hostname or ip
  -u username           expert username
  -p password           expert password
  -port port            web api port (default 443)
  -proxy_host proxy_host
                        HTTP proxy server address (without "http://")
  -proxy_port proxy_port
                        HTTP proxy server port (default 8080)
  -mds mds              name of domain server
  -domain domain       name of domain
  --test function_name test an internal function ['_get_gateways_and_routes',
'_get_network_objects', '_get_rulebases',
'_get_service_objects', '_get_vpn_communities'] - no
json config produced
  -xp, --extra_pwds    Need additional and separate passwords to connect to
domains in MDM environment. Default is True and
separate passwords will be prompted for unless this
flag is set.
  --version            show version number

Done.
Press Enter to exit...
  
```

- **Step 5:** if the connection to the Check Point R80 is successful, the configuration file will be generated (it can take up to 10 minutes) and stored in the file

```
checkpoint_config_<server_address>_<domain_server_name>_<domain_name>.json
```

in the directory where checkpoint_r80_exporter.exe was launched. An output log file r80_config_exporter_log.txt is also saved next to the .json file.

Instructions to import the R80 configuration file into NP-View:

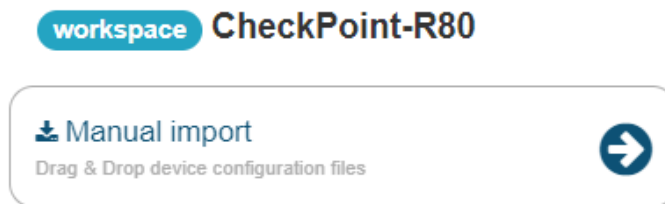
- **Step 1:** launch NP-View and import the configuration file by selecting Import Data from the main menu.



+ Import Data



then select manual import



then click the import box and select the files for importing.

Alternatively, the user can drag and drop the downloaded checkpoint file into a new workspace and select the upload button.

- **Step 2:** when prompted by NP-View, choose the devices to import and select the Import button.

Import Configurations

[Supported devices and how to get configurations](#)

Notice: Importing new devices requires available licenses. Devices are activated in the order they are imported. If the total license count is exceeded, importing of additional unlicensed devices will be prohibited. See License and Terms to determine the available number of licenses.

2 device configurations are available in the selected file. Please choose which configurations to import.

Select/Deselect All
 checkpoint-r80-gw2
 checkpoint-r80-mds-gw1

0 devices selected

Import



20 N Wacker Dr #1200
Chicago, IL 60606
(872) 245-4100

The files will then be uploaded into the active workspace

For feedback on the usability and performance of NP-View, please contact support@network-perception.com.