How To Backup a SmartCenter
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=11973
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/6/2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Backup a SmartCenter ).
How To Backup a SmartCenter

Objective

This guide assists in the recording and storage of current configurations on the SmartCenter to another location. In case of hard drive failure, failed upgraded, database corruption or other system failures the data can easily be restored.

It is important to always have a copy of the most recent information in the Security Management server and Security Gateway databases.

There are two methods of taking a Snapshot and creating a Backup with SecurePlatform, through the WebUI and CLI. You can use the Upgrade Tools for Linux and Windows.

Supported Versions

- All current Check Point versions

Supported OS

- SecurePlatform
- Windows
- Linux
- Solaris
- IPSO

Supported Appliances

- All current Check Point Appliances

Related Documentation and Assumed Knowledge

Experience with command line interfaces (CLI) and WebUI tools.

Terminology

Standalone - Security Gateway and Security Management on the same machine
Distributed - Security Gateway and Security Management on separate machines

Related Documentation

Refer to:

- R75 Installation and Upgrade Guide
  (http://supportcontent.checkpoint.com/documentation_download?ID=11648)
Impact on Environment and Warnings

The Snapshot and Backup process is recommended to be run during a maintenance window.

Take a Snapshot

A Snapshot, including drivers, will be created and is only available for SecurePlatform.

The Snapshot can be used to backup up both Security Gateways and Security Management servers. The Snapshot will generate a large file.

Note - The Snapshot can only be restored to the same machine that is in the same state (same OS, same CP version, same patch level).

For UTM-1 and Power-1 appliances, you can only take a Snapshot with the WebUI. The snapshot must stay on the appliance.

Snapshot using the CLI Command

To take a Snapshot with the CLI:

- Run: `snapshot`

  The Snapshot uses default backup settings and place the file in the directory `/var/CPsnapshot/snapshots` when no flags are set. Additional flags for file name or tftp server can be used. Use the command `snapshot -h` for help and a listing of available flags.

To restore the system from the Snapshot file:

- Run: `revert`

  The system is restored to the configuration as set in the Snapshot. Use the `revert -h` for help.

Snapshot using the WebUI

To take a Snapshot with the WebUI:

1. Login to https://mgmt:4434.
2. Click Appliance -> Image management -> Create.

To restore:

1. Login to https://<ip_address>/mgmt:4434.
2. Select the snapshot.
3. Select revert.
Backup Procedure

A Backup of the Check Point configuration and networking/OS system, such as routing data, is restored. It is only available on SecurePlatform. The Backup can be used to restore both Security Gateways and Security Management servers. The file will be slightly smaller than the file generated by Snapshot. The restoration must be done to the same machine, same OS, same Check Point version and patch levels.

Backup using the CLI

To Backup the system with the CLI:

- Run: `backup`

If no flags are used the default Backup settings will place the file in the directory: `/var/CPbackup/backups`. On the UTM-1 and Power-1 appliances, the file will be stored in `/var/log/CPbackup/backups`. Additional flags for file name or tftp server can be used. Use the command `backup -h` for help and a listing of available flags.

To restore the system from the Backup file:

- Run: `restore`

The system is restored to the configuration as set in the Backup file. Use the `restore -h` for help.

Backup using the WebUI

To create a Backup from the WebUI:

1. Login to https://<ip_address>/mgmt:443.
2. Click Device -> Backup

You can choose to either perform the Backup now or schedule a Backup.

Note - The Backup can only be restored from the command line interface.

Upgrade tools

Upgrade tools will perform a Backup for all Check Point configurations, but not OS configuration data. You can backup Check Point configuration on the Security Management server independent of hardware, OS or Check Point version. You can also restore to a higher Check Point version only.

Depending on the size of your policy, the created file is smaller than a Snapshot or Backup file. If the system is not running on high CPU you can do a backup on live system without interruption of the services. The Upgrade tools are also available for Solaris and IPSO. This utility is used through the command line.
Upgrade tools using Linux

To export on Linux:
1. Enter: cd $FWDIR/bin/upgrade_tools
2. Enter: ./upgrade_export filename

To import on Linux:
1. Enter: cd $FWDIR/bin/upgrade_tools
2. Then enter: ./upgrade_import filename
   • The command upgrade_import will stop all active Check Point services.

Upgrade tools using Windows

To export on Windows:
1. Enter: cd c:/windows/fw1/bin
2. then enter: upgrade_export <filename>

To import on Windows:
• Enter: upgrade_import <filename>
Additional Backup options

Database Revision Control

This utility creates a version of your current policies, object database, IPS updates. It is useful for minor changes or edits performed in the dashboard.

Note - It cannot be used to restore the system in cases of failure.

To perform database revision control, in the dashboard go to: File > Database revision control > Create
You can create a database revision when you install a policy.

Saving Routing and Interface Information

You can save the routing and interface information from your machines with these commands:

- netstat -rn > routes.txt
- ipconfig -a > ipconfig.txt
- ifconfig > ifconfig.txt
- copy /etc/sysconfig/netconf.C <location>
Recommended Backup Schedule

We recommend that you schedule backups for:

- **Snapshot** – Backup at least once before any major changes (for example an upgrade)
- **Backup** – Backup approximately every two months, depending on frequency of network/ policy changes, as well as before every major change
- **upgrade_export** – Backup approximately every month, depending on frequency of network/ policy changes, and before every upgrade or migration
Verifying the Procedure

It is highly recommended to test your Backup procedures and confirm that all data has been restored correctly.

The *backup* and *upgrade_export* options are used for this.