

# OS Advanced Migration Quick Guide

Colter Ets Hokin  
Security Engineer - Rockies  
August 31, 2018

**This guide will provide step by step instructions on the process for OS advanced migration to the R80.10 platform.**

## Step 1:

### Backup server configuration:

There are three different procedures for backing up and restoring the operating system and networking parameters on your appliances, Snapshot, Backup, and Upgrade\_export. Each procedure can be executed either from command line interface (CLI) or from the SecurePlatform web interface (WebUI).

- **-Snapshot-** a snapshot of the entire system and configuration settings, it backups everything including drivers, system data, network settings and check point configurations.
- From the command line (CLI), run - # snapshot
- Use – ‘snapshot –h’ for help or to list all available flags.
- **Reminder:** Performing snapshot can take a long time and can interrupt your services as the cpstop command is run.
- In order to revert to a snapshot file:
  - From the CLI, run - # revert
  - This command will open the default menu
- In order to use a local snapshot file, you need to locate this file under */var/CPsnapshot/snapshots/* otherwise it's not possible to choose this file when using a local snapshot image option

- **-Backup-** The backup utility can be used to backup both firewall gateways and management servers.
- To generate a backup file in command line, use the following command:  

```
# backup
```

Running backup without any flags will use default backup settings and put the file under /var/CPbackup/backups
- Using the WebUI, you can also choose to configure a scheduled backup, or you can choose to perform an instantaneous backup operation.
- **Reminder:** Performing backup can take a long time and can interrupt your services as the cpstop command is run.
- The 'restore' command restores the system configuration (in open servers from /var/CPbackup/backups/, in Check Point appliances from /var/log/CPbackup/backups/).
- Syntax:  

```
# restore [-h] [-d] [--tftp <ServerIP> <Filename>] | [--scp <ServerIP> <Username> <Password> <Filename>] | [--file <Filename>]]
```
- When the restore command is executed without additional flags, a menu of options is displayed. The options in the menu provide the same functionality, as the command line flags
- **-Upgrade\_export-** Upgrade\_export tool backs up all Check Point configurations, independent of hardware, OS or Check Point version, but does not include OS information (i.e NIC interfaces).
- The upgrade tool folder is located under \$FWDIR/bin/upgrade\_tool/ and it contains both the upgrade\_export (and also the upgrade\_import) and the migrate tool.
- For generating an upgrade\_export file of the system, from the CLI run:  

```
# ./upgrade_export <export_file_name>
```
- For generating a Migrate Export file of the system, from the CLI run:  

```
# ./migrate export <export_file_name>
```
- Both tools are very similar, the only difference is that the Migrate tool can be used in a Provider-1 environment and it's the same tool both for the export and the import operations with a separate flag assigned for each operation. Check Point recommendation is to use the Migrate Tool to backup Management servers from R71 and above.
- In order to import a database file, you should use one of the following commands:  

```
# upgrade_import <path to export file>
# migrate import <path to export file>
```

In case the import operation failed, a notification will be sent about it and you can check the migrate log file if the migrate tool was used, located at \$CPDIR/log/. There is a separate migrate log file for each try of import operation.

## Step 2:

### Contract Verification:

Before upgrading a valid support contract is needed that includes software upgrade and major releases registered to your Check Point User Center account. The contract file is stored on Security Management Server and downloaded to Check Point Security Gateways during the upgrade process. By verifying your status with the User Center, the contract file enables you to easily remain compliant with current Check Point licensing standards.

## Step 3:

### Acquire Migration tools:

Make sure you have the latest version of the upgrade tools! Download the appropriate package from the **Tools** section in the Check Point R80.10 Support site

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk111841&partition=General&product=All%22#Documentation](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111841&partition=General&product=All%22#Documentation)

There is a different package for each operating system.

When you open the **upgrade\_tools** package, you see these files: Package

migrate.conf -----

migrate -----

pre\_upgrade\_verifier -----

migrate export -----

migrate import -----

puv\_report\_generator -----

Description

Holds configuration settings for Advanced Upgrade / Database Migration.

Runs Advanced Upgrade or migration.

Analyzes compatibility of the currently installed configuration with the upgrade version. It gives a report on the actions to take before and after the upgrade. `pre_upgrade_verifier -p $FWDIR -c <Current Version> -t <Target Version>`

Backs up all Check Point configurations, without operating system information.

Restores backed up configuration.

Runs in the end of `pre_upgrade_verifier` and converts the text file to HTML.

## Step 4:

### Pre-upgrade verifier:

For full detailed instructions on this step see [sk110267](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk110267)

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk110267](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk110267)

- Run: *CPinfo* and notify users about upload status:

```
cpinfo -iR <e-mail address>
```

Example:

```
cpinfo -iR e-mail1 @domain.com;e-mail2 @domain.com;e-mail3 @domain.com
```

Upload the CPinfo files. This can be done in two different ways.

### First option: Upload the CPinfo files using [Check Point Uploader](#):

- Copy the CPinfo output files to an online Windows-based machine.

**Note:** Names of files should be in the following naming convention: *[10 Digits]\_[1Digit]o[1Digit]\_\**

- Verify that the '*R80 Upgrade Verification Service*' checkbox at the bottom is selected. If this checkbox is not selected, the offline process will upload the files, but they will not be automatically simulated. Files will be uploaded to our secure FTP server, but remain untouched.

In Offline Mode, enter your e-mail again in the Check Point Uploader GUI as these are separate tools.

**Important:** When uploading files from R80 environment via Check Point Uploader, do not enter the Service Request Number.

### Second option: Upload the files using CPInfo.

To upload files to R80.10 Upgrade Verification service from an online machine (which has no Check Point products installed on it), use the following syntax:

```
# cpinfo -n -r R80_desk -u user@exampledomain.com -s <SR number> -e  
" user1 @exampledomain.com;user2 @exampledomain.com" -f <MGMT machine  
migrate export file>.out.tgz <MGMT machine file>.info.gz
```

## Step 5:

### Run export of current database:

- Run migrate export command :  
`./migrate export /var/log/customerDB_export_for_R80_10`

This command will create the file from which customer specific configurations and settings will be imported later.

## Step 6:

### Save current configuration settings

- Run:  
`save config`

Run in CLI or web UI to copy networking properties in addition to security configuration.

## Step 7:

Download newest take of R80.10 ISO

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk111841&partition=General&product=All%22#Documentation](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111841&partition=General&product=All%22#Documentation)

- Reimage hardware with this ISO
- Run First time wizard from the web UI  
Reminder: use the same IP address from old configuration when configuring first time wizard.

## Step 8:

### Transfer stored database file:

- Copy exported database file from source management server to newly configured server using for example: FTP server access

## Step 9:

### Import stored database to new OS:

- Run command:  
`unset TMOUT`

This will ensure you are not logged out during the next part of this step

- Run migrate import command:  
`./migrate import /home/admin/customerDB_export_for_R80_10.tgz`

This command will import the stored database settings and configurations to the new OS management server

## Step 10:

### Check new server readiness status:

- Run command:  
`watch -n1 $FWDIR/scripts/cpm status.sh`

## Step 11:

### Connect to new server:

- Install Smartconsole  
[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk111841&partition=General&product=All%22#Documentation](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111841&partition=General&product=All%22#Documentation)
- Log into new management server