Management Upgrade Workbook

Do you have critical infrastructure you cannot consistently patch, upgrade, and change? Do you have gateways that must be up-to-date, on the latest firmware, with the newest features? Do you use Check Point's centralized management infrastructure to manage these gateways along with other gateways that are constantly changing? If you answered "yes" to all three of these questions, this document will describe the steps you should use to safely and reliably bring up, configure, and upgrade a new manager and swing the constantly changing gateways over to it for management.

This procedure allows you to have an up-to-date management appliance and enables gateway firmware upgrades, while mitigating any risks to your critical infrastructure. You will have two managers by the end of this document, one on newer code, managing gateways on newer firmware, and another management appliance on older code, managing the gateways you cannot upgrade.

These steps have been tested, and successfully used in customer environments to upgrade a management server from R77.30 to R80.10. Please keep in mind, the new manager will be completely separate and have different IPs from the older one and will you must add the object to any firewalls rules containing the current manager.

These steps will allow either manager to push policy, and will allow for logging to either manager. This configuration is used in the interim to provide a roll back plan in the event of an issue and should be cleaned up after a period.

Introduction

The process of upgrading a management server from 77.30 to 80.10 will be detailed in this whitepaper in two phases. The first phase will describe how to prepare the old management for the migration, and the second phase will describe how to successfully complete the migration on the new management.

PHASE ONE:

- First, download the appropriate R80.10 migration tools found in sk111841.

Management Server Migration Tool	Gaia R80.10 to R80.10 Tool (TGZ) Gaia R7X.X to R80.10 Tool (TGZ) SecurePlatform and Linux Tool (TGZ) Windows Tool (TGZ)

- Then, use the Pre-Upgrade Verifier to detect and resolve any errors that could prevent a successful migration.

Using the Pre-Upgrade Verifier

The Pre-Upgrade Verifier runs automatically during the upgrade process. You can also run it manually with this command.

Syntax:

```
pre_upgrade_verifier.exe -p <ServerPath> -c <CurrentVersion> (-t
<TargetVersion> | -i) [-f <FileName>]
```

Parameters:

Parameter	Description
`-p`	Path of the installed Security Management Server (FWDIR)
`-c`	Currently installed version
`-t` `-i`	Target version If `-i` is used, only the INSPECT files are analyzed, to see if they were customized.
`-f`	Output report to this file

- Next, create a dummy object that will allow communication between the existing gateways and the new management server.
  An example of a dummy object and its creation could look like this:
  1) Create the object as Check Point Host and enable Network Management Blade (Secondary Server)
  2) Use any name e.g. <SC Name>-dummy
  3) Specify a new IP address for R80.10 server
  4) Add the temp/dummy object to below sections on all Gateways
     a. Fetch Policy

b. Logs
c. Rules containing the original manager

5) Save Policy
6) Install Database on all servers
7) Install policy to all gateways

- Disconnect all GUI clients
- Export configuration using migrate export command
- Perform MD5 check on the .tgz file
- Transfer file to local machine or new SC if is already built (FTP (binary mode) /WinSCP), verify MD5

PHASE TWO:

- First, install R80.10 using the new IP Address
- When going through the First Time Configuration Wizard, the settings and definitions should be consistent with the original management server
- Confirm that the appropriate interfaces are connected and link is up
- Transfer the database backup (FTP/SCP) using binary mode
- Check MD5 after transfer
- Import earlier configuration using the migrate import command
- Use SmartConsole to connect to the new management server
- Confirm that the SmartCenter object has the new IP Address
- Remove the original manager object from all gateways you need to be managed via the new R80.10 object
- Install Database
- Backup old licenses using “Getting Last License”
- Re-issue a license with the new IP
- Re-license devices with the new IP in the UC
- Attach the new license with the new IP address to each of the gateways being moved
- Migrate the specified gateways (minimum version R75.20)
  a. Push Policy to GW
  b. Test Traffic
  c. If testing is successful, delete firewall objects from the R77 Management server.

After you have upgraded your management server, you may want to upgrade some (if not all) of your gateways. The steps for that process will be below.

PREREQUISITES FOR THE UPGRADE:

Required Disk Space:

- The hard disk on the target machine must be at least 5 times the size of the exported database.
- The size of the /var/log folder on the target must be at least 25% of the size of the /var/ log directory on the source machine.

Required Network Access:

- The source and target servers must be connected to a network.
- The connected network interface must have an IP address.

IPv4:

The target must use the same IP address configuration as the source. If the source uses IPv6, you must change it to IPv4 before you can migrate.

Target Version and Products:

You can only upgrade or migrate the version of the server or set of products. The target must have the same or higher version and the same set of installed products.

For information regarding R80 Desk (the Upgrade Verification and Environment Simulation service), see sk110267

Note that we will provide SFTP credentials when the CPinfo files are ready to be transferred. At that time, we will take the following steps:

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]_**

Example:

1907139894_1o1_onetera127_21_3_2016_14_36.info.gz

OR

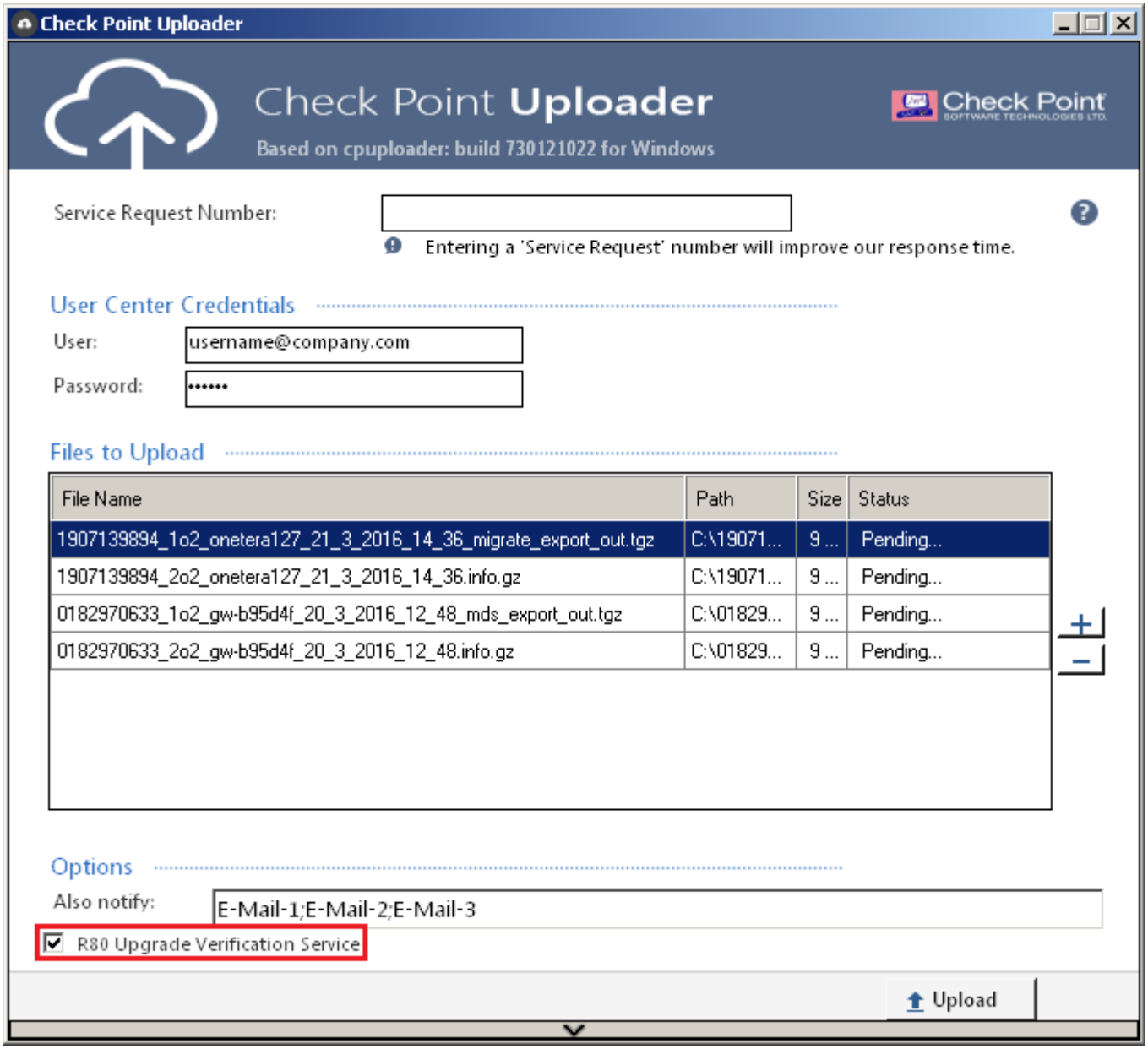
0182970633_1o2_gw-b95d4f_20_3_2016_12_48_mds_export_out.tgz
0182970633_2o2_gw-b95d4f_20_3_2016_12_48.info.gz

- 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.

  Note: In Offline Mode, enter your e-mails 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.

  Example:



UPGRADE PROCESS

1. Get the R80 migration tools package from the Support Center

   a. Extract the downloaded package, to the source and the target servers.

   Important - Extract all the files to the same directory and run the tools from that directory.

   b. Make sure the files have executable permissions: chmod 777 *

When you open the **upgrade_tools** package, you see these files:

Package	Description
migrate.conf	Holds configuration settings for Advanced Upgrade / Database Migration.
migrate	Runs Advanced Upgrade or migration. On Windows, this is **migrate.exe**.
pre_upgrade_verifier	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. On Windows this is **pre_upgrade_verifier.exe** `pre_upgrade_verifier -p $FWDIR -c` *<Current Version>* `-t` *<Target Version>*
migrate export	Backs up all Check Point configurations, without operating system information. On Windows, this is **migrate.exe export**
migrate import	Restores backed up configuration.

The migrate command exports a source Security Management Server database to a file, or imports the database file to a target Security Management Server. Use absolute paths in the command, or relative paths from the current directory.

Before you run this command for export, close all SmartConsole clients or run cpstop on the Security Management Server.

Before you run this command for import, run cpstop on the Security Management Server.

Syntax:

```
migrate {export | import} [-l] [-n] <filename> [--exclude-uepm-postgres-db] [--include-uepm-msi-files]
```

Parameters	Description
`export` `import`	One of these actions must be used. Make sure services are stopped.
`-l`	Optional. Export or import SmartView Tracker logs and SmartLog data. Only closed logs are exported. Use the `fw logswitch` command to close the logs before you do the export.
`-n`	Optional. Run silently (non-interactive) using the default options for each setting. **Important**: If you export a management database in this mode, to a directory with a file with the same name, it is overwritten without prompting. If you import using this option, the command runs `cpstop` automatically.
`--exclude-uepm-postgres-db`	Skip over backup/restore of PostgreSQL database of the Endpoint product.
`--include-uepm-msi-files`	Export/import the uepm msi files.
`filename`	Required. Enter the name of the archive file with the server database. The path to the archive must exist.

2. Create a new temporary host object in SmartConsole or SmartDashboard with the IP address of the target.

3. Define a Firewall rule that lets the new R80 server connect to Security Gateways:

   Source: *new server*

   Destination: target Security Gateways

   Service:

   FW1 (TCP 256)

   CPD (TCP 18191)

   FW1_CPRID (TCP 18208)

   CPM (TCP 19009)

4. Install the new security policy on all gateways.

5. If the source has IPv6 addresses, on the source operating system, disable IPv6.

6. In SmartConsole or SmartDashboard, delete the temporary host objects from the primary Security Management Server.

7. Close all Check Point GUI client connections to the Security Management Server.
8. If this server is not in production, run: cpstop
9. Export the database with the R80 export tools:

   - Log in to **expert** mode.
   - Run the Pre-Upgrade Verifier tool: pre_upgrade_verifier
     - If there are errors, correct them before you continue.
   - Run: *<upgrade_tools_path>*/migrate export *<filename>*.tgz
     - The migrate export command exports the content of one Security Management Server database to a TGZ file.
   - Follow the instructions.
     - The management database is exported to the file that you named in the command. Make sure you define it as a TGZ.
   - If SmartEvent is installed on the source server, export the Events database.

10. Clean install the new R80 Security Management Server

    For an Open Server:

    Install the Gaia Operating System before installing R80:

    - When you start the Gaia installation, you must select Gaia and press **Enter** in 60 seconds, or the server tries to start from the hard drive. The timer countdown stops when you press **Enter**. There is no time limit for the next steps.
    - Start the server using the installation media.
    - When the first screen shows, select **Install Gaia on the system** and press **Enter.**
    - Press **OK** to continue with the installation.
    - Select a keyboard language. **English US** is the default.
    - Configure the hard disk partitions.
    - Enter and confirm the password for the **admin** account.
    - Select the management interface (default = eth0).
    - Configure the management IP address, net mask and default gateway. You can define the DHCP server on this interface.

- Select **OK** to format the hard drive and installation the Gaia operating system.
- **Reboot** to complete the installation.

THEN

Configure Management Server on Gaia

- Open a browser to the WebUI: https://*<Gaia management IP address>*
- In the **Gaia Portal** window, log in with the administrator name and password that you defined during Gaia installation.
- The WebUI shows the **First Time Configuration Wizard**. Click **Next**.
- Select **Continue with configuration of Gaia R80**. Click **Next**.
- If you did not change the default administrator password, do it now. Click **Next**.
- Set an IPv4 address for the management interface.
- If you change the management IP address, the new IP address is assigned to the interface. The old IP address is added as an alias and is used to maintain connectivity. **This will need to be removed in the future.**
- Enter the **host name** of the server.
- **Optional:**
- Enter the **domain name**, and IPv4 addresses for the **DNS servers**.
- Set the IP Address and Port for a Proxy Server.
- Click **Next**.
- Set the date and time manually, or enter the hostname and IPv4 address of the NTP server. Click **Next**.
- Select **Security Management**. Click **Next**.
- Enter the username and password for the Security Management Server administrator account. Click **Next**.
- Define IPv4 addresses from which SmartConsole clients can log in to the Security Management Server **if you will be filtering access outside of the Security Policy.** Click **Next**.
- Get a license automatically from the UserCenter and activate it, or use the trial license.

- If there is a proxy server between the server and the Internet, enter its IP address and port.
- Click **Next**.
- Review the summary and then click **Finish**.
- Click **Yes** when prompted to start the configuration process.
- A progress bar tracks the configuration of each task.
- Click **OK**.
- If the **Help Check Point Improve Upgrades (CPUSE)** window shows, click **Yes** or **No**. Check Point recommends that you click Yes. Your data is never shared with third parties **(if you subscribe to PRO level support this needs to be enabled!).**

THIS COMPLETES THE TASKS FOR OPEN SERVER INSTALL

In order to install on an appliance from the ISO file:

- Create the removable installation media:
- USB drive - To prepare a USB drive, see: sk65205
- Connect the USB drive with the R80 ISO to the appliance.
- Open the terminal emulation program.
- Restart the appliance.
- Redirect the boot sequence to the installation media:
- USB drive - In the boot screen, at the boot prompt, enter serial and press **Enter**.
- The R80 is file is installed on the appliance.
- Reboot the appliance, press **CTRL + C**.
- Configure the Management IP Address.
- Run the First Time Configuration Wizard.

****THIS COMPLETES THE TASKS FOR APPLIANCE INSTALL**

11. Import the database

Important: When you transfer the exported database from the source to the target, use **binary mode** during the transfer.

- Log in to **Expert** mode.
- Transfer (with FTP, SCP, or similar) the exported configuration file collected from the source () to the new server.
- Calculate the MD5 for the transferred file and compare to the MD5 that was calculated on original server:
  - # md5sum /*<directory>*/*<name>*.*DDMMYYY-HHMMSS*.tgz
- Import the configuration: *<migration_tools_path>*/migrate import *<path_exported_database>*/*<filename>*.tgz
- Test the target installation.
- Disconnect the source server from the network.
- Connect the target server to the network.

Now your upgrade is complete!

Things to keep in mind post upgrade:

- When you migrate the Security Management Server to R80, the SmartEvent databases are not included. For more about how to migrate the events database to R80, see sk110173.

LICENSING

Migrating a License to a New IP Address (Security Management Server):

Licenses are related to the management IP addresses. You must update the license and configure the environment to recognize the new server.

1. Update the licenses with the new IP address. If you use central licenses, they must also be updated with the new IP Address.
2. Run cpstop and cpstart on Security Management Server.
3. Connect to the new IP address with SmartConsole.
4. Remove the host object and the rule that you created before migration.
5. Update the primary Security Management Server object to make the IP Address and topology match the new configuration.

6. Run evstop and evstart on SmartEvent servers.

7. On the DNS, map the target Security Management Server host name to the new IP address.

Configuring the new IP address for Log Servers and SmartEvent:

1. When you log in to SmartConsole for the first time, open the Domain Log Server or SmartEvent object.

2. Change the IP address to the new IP address.

3. Publish and install the database.

4. Open the distributed Domain Log Server or SmartEvent object again.

5. In the **Platform** section, click **Get**.

   This updates the server to the correct version.

6. Click **OK**.

7. Publish and install the database.

RESTORING ON FAILURE

If there are issues with the upgrade, you can restore the original database. Make sure you have the OS settings that you noted when you backed up.

1. Clean install the original version.

   Use the *Installation and Upgrade Guide* for major versions, or the *Release Notes* for minor versions or hotfixes.

2. Configure Gaia OS settings in the Gaia WebUI or CLI.

3. Import the exported database.

   - Security Management Server

