How To Migrate SmartCenter and Change the IP Address and Hostname

7 January 2014
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=15421)
To learn more, 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>07 January 2014</td>
<td>Updated for Gaia and R77</td>
</tr>
<tr>
<td>10 April 2012</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 Migrate SmartCenter and Change the IP Address and Hostname  ).
How To Migrate a Security Management Server and Change the IP Address and Hostname

Objective

This document explains how to migrate a Security Management Server and change its IP address and Hostname. These are the situations in which there is a need to change the Hostname and IP address of a Security Management Server:

- When you need to upgrade to a new hardware, and leave the old Security Management Server online.
- When you need to adhere to a Naming convention to reflect your company policy.
- When you need to upgrade Check Point on a new production server, and leave the old server online.
- When you move Datacenters and run two Security Management Servers to lead up to the changeover.

Supported Versions

R65 and higher.

Supported Operating Systems

All operating systems that support the Security Management Server.

Before You Start

Related Documents and Assumed Knowledge

- *Firewall Administration Guide* for your version
- *SecurePlatform Administration Guide* for your version
- *Security Management Server Administration Guide* for your version
- *Installation and Upgrade Guide* for your version
- How to intensively reset SIC and delete all certificates from Security Management Server - sk34373
  (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk34373)
- fwm sic _reset command fails on the Smart Center/Security Management server - sk14532
- Troubleshooting SIC - sk30579
- How to back up your Security Management Server - sk54100
  (http://supportcontent.checkpoint.com/solutions?id=sk54100)
Impact on Environment and Warnings

- A new License must be generated from the Check Point User Center (https://usercenter.checkpoint.com/usercenter/index.jsp) with the new Security Management Server IP address.
- SIC must be reset to all gateways.
- All VPN and Client certificates must be revoked.
- Third Party certificates must be regenerated to reflect the new Security Management Server Hostname and IP address.
- Any rule with a gateway selected in INSTALL ON needs to be changed from that gateway to Any. Otherwise you must forcibly reset SIC according to sk34373 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk34373).
- All VPN and Remote access communities must not contain any firewalls. If any site to site, or remote access communities do, you must remove their firewalls.
- You must clear the VPN blade option from all gateways. Otherwise you must forcibly reset SIC according to sk34373 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk34373).

Migrating Security Management Server and Changing IP Address and Hostname

To migrate, or upgrade Security Management Server, you must export the old one and then import the new one.

**To Export the Old Security Management Server:**


   **Note** - upgrade_export backs up all Check Point configurations, independent of hardware, Operating System or Check Point version, but does not include Operating System information. You can only upgrade the Check Point version, not downgrade.

2. To export on SecurePlatform, IPSO, or Redhat, run: cd $FWDIR/bin/upgrade_tools and .//upgrade_export filename
# cd $FmDIR/bin/upgrade_tools
# ls
Upgrade_export upgrade_import
# ./upgrade_export test.export

You are required to close all Check Point clients before the Export operation begins. If the export fails stop Check Point services and run the upgrade_export command again. Press ENTER when ready.

Checking the existence of necessary files...
Copying files to temp dir...
Building configuration file...
Compressing the files...

The export operation finished successfully.
# ls
est .export .tgz upgrade_export upgrade_import

To export on Windows, run: cd %FWDIR%\bin\upgrade_tools and upgrade_export filename

3. Note the MD5 of the created export file and write it down. It appears as:
   md5sum <filename> in Gaia, SecurePlatform, and Linux
   md5 <filename> in IPSO
   A md5 program is needed in Windows

4. To transfer the file to a secure location, use SFTP or FTP.

To Import a New Security Management Server
1. Create a new Security Management Server with the image of your choice (R70 image or above). Do not apply any HFA at this time.
2. Configure the new Security Management Server with the old IP and Hostname.
3. Log into the New Security Management Server with the old IP address for the first time to make sure that everything works. You may have to connect with a local network or crossover cable for the first time.
4. Transfer the export file from the old Security Management Server to the new Security Management Server with SFTP or FTP. You might have to transfer the export file to the new Security Management Server from a locally connected laptop.
5. Verify the MD5 of the export file matches the md5 value written before:
   md5sum <filename> in Gaia, SecurePlatform or Linux
   md5 <filename> in IPSO
   An md5 program is needed in Windows

6. To import the exported file into the system:
   On Gaia, SecurePlatform or Linux, these commands in the Expert mode:
   cd $FWDIR/bin/upgrade_tools
   ./upgrade_import filename
   On Windows, run:
   upgrade_import <filename>

   For more information, see sk54100 (http://supportcontent.checkpoint.com/solutions?id=sk54100)

7. To reboot the system, run: reboot
8. Make sure you can log into your Management station with the old IP and login details.

To Change the IP Address and Hostname:
1. Open SmartDashboard. Do not close SmartDashboard until this procedure is completed.
2. Open SmartUpdate.
3. In the **Network Objects Licenses & Contracts** tab, right click the Security Management Server object, and select **Detach all Licenses**.

4. In SmartDashboard, double click the Security Management Server object. The **Check Point Host-General Properties** window opens.

5. In the **Name** field, change the host name of the Management station object to the new name.

6. In the **IP Address** field, enter the new IP address and click **OK**.

7. In SmartUpdate, right click the Security Management Server object, and select **Attach Licenses**. You can obtain the license from the Check Point User Center account.

8. Open an SSH connection to the Security Management Server and run:
   - `cpstop`
   - `sysconf_wizard`

9. Change the host name and IP address to reflect the changes made in SmartDashboard.

10. Close the wizard.

  **Note** - In Windows you must open the system properties, and change the Hostname, Network, IP Address, and reboot.

11. Run:

    ```bash
    cpstart
    ```

12. Log into SmartUpdate with the new IP address. It may be necessary to reconnect to the Security Management Server to reach the new network.

13. Log into SmartDashboard and save the database.

14. Close SmartDashboard and SmartUpdate.

**To Reset the Certificate Authority (to match the new Name and IP):**

1. Connect to the Security Management Server console with SSH or CMD, and run: `fwm sic_reset`
2. To regenerate the Security Management Server Certificate authority, run `cpconfig` and then enter 7 to select **Certificate Authority**.

3. Restart Check Point, run: `cprestart`
4. Confirm you can log back into SmartDashboard. The system prompts you for a new Fingerprint.

**To Reset SIC:**

To reset SIC for the entire gateway, use the details in skI1896 (http://supportcontent.checkpoint.com/solutions?id=skI1896). Use the new certificate.