Endpoint Management Deployment

Management R77.30.03

Jumbo Hotfix 292

Endpoint E80.81

V1.5

Content

Endpoint Management Deployment....0
1. Needed files....2
2. Deployment of GAIA OS....3
3. First Time Configuration Wizard....6
4. Copy files to the Management....9
5. Update the CPUSE agent....10
5.1 Online update....10
5.2 Offline update....11
6. SmartConsole R77.30.03 / E80.81 Installation....12
7. Licenses creation (just needed during a POC)....13
8. Licenses installation....15
9. Contracts installation....16
10. Activación de Endpoint Policy Management....17
11. Enable SmartLog....18
12. Jumbo Hotfix Installation for Endpoint Server....19
13. Jumbo Hotfix R77.30.03 Installation for GAIA....19
14. Update to the latest JumboHotfix....20
15. Import the Endpoint packages....21
16. Endpoint client deployment....22
Appendix I: Help Resources....24
Appendix II: ESX/ESXi doesn't detect the hard drive (sk7440)....25
Appendix III: SmartEndpoint console crashes when uploading Endpoint packages (sk121722)....26

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

1. NEEDED FILES

Here you are the needed files to download:

A

1. R77.30 ISO for Open Server > Download
2. E80.81 Endpoint Security Clients for Windows OS > Download
3. SmartConsole for Endpoint Security Server R77.30.03 / E80.81 > Download

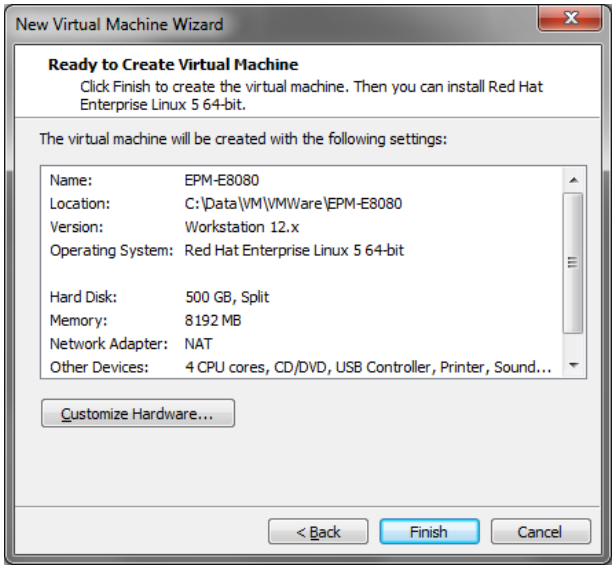
B

4. R77.30 Jumbo Hotfix for Endpoint Security Server > Download
5. R77.30.03 Endpoint Security Server Package for Gaia OS > Download
6. CPUSE Agent latest version (Optional) > Download

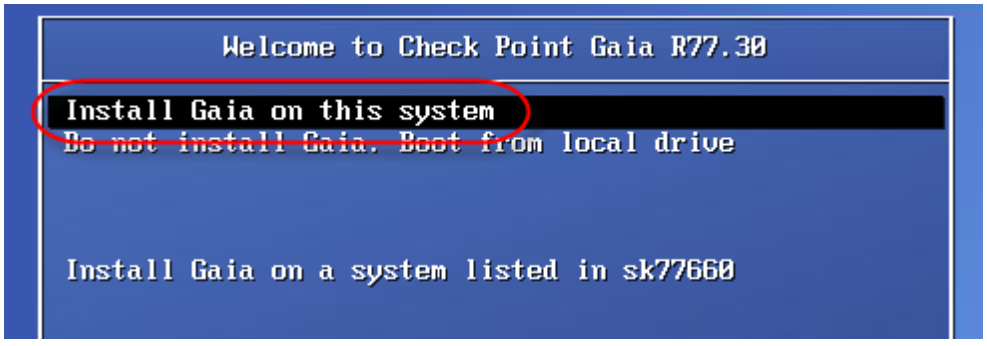
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

2. DEPLOYMENT OF GAIA OS

- Requirements to create the Virtual Machine:
  - Cores: 4
  - RAM: 8GB
  - Disco: 500GB

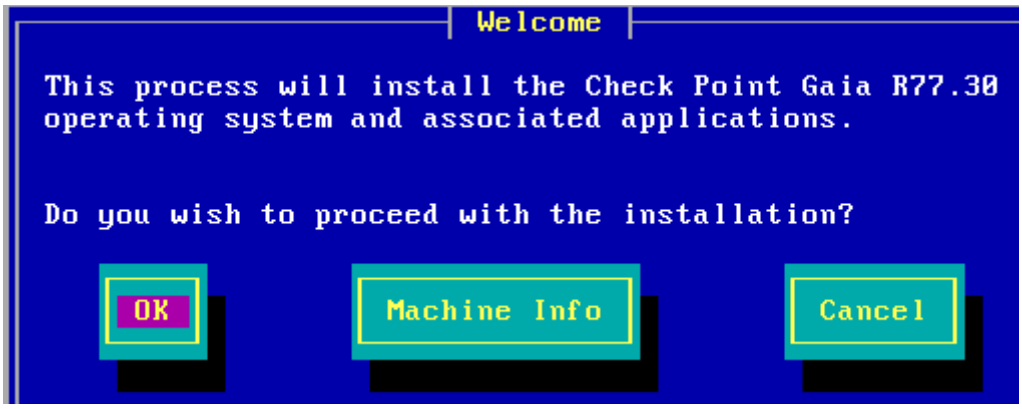


- Mount the ISO file (File 1 from list A from the needed files) on the VM and boot the VM from the ISO.
- Select **"Install Gaia on this system"** at the boot menu



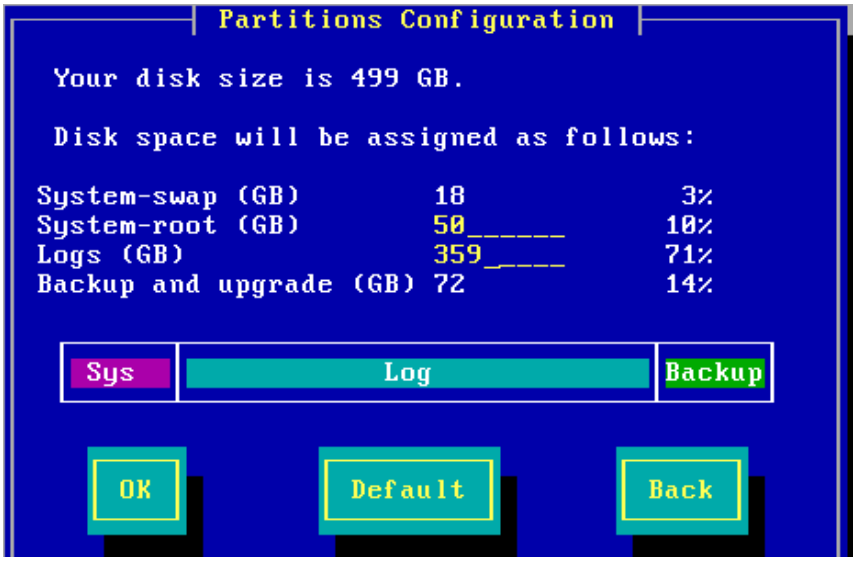
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

- Select **"OK"**



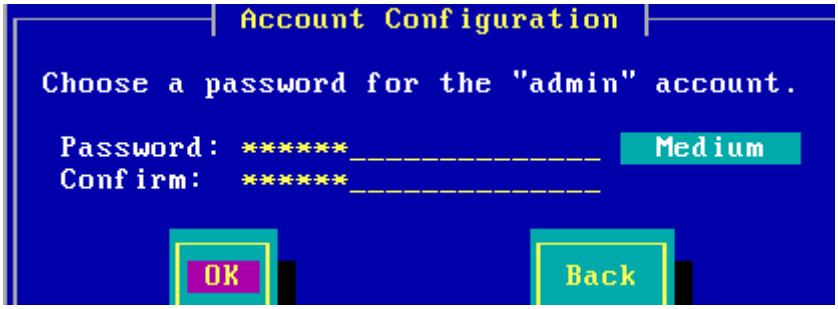
- Select **"Spanish" (**or your keyboard language layout)

- Configure the different partitions and select **"OK"**

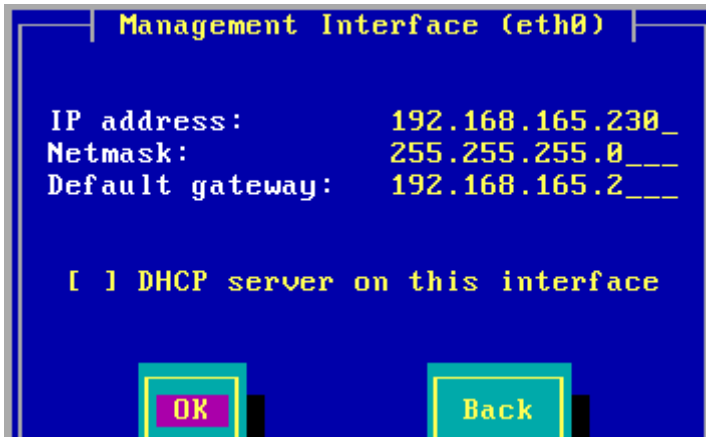


©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

- Choose a password for the **admin** user and select "**OK**"



- Configure the network details, they will depend on your own environment, you don't need to configure exactly the same IP range.

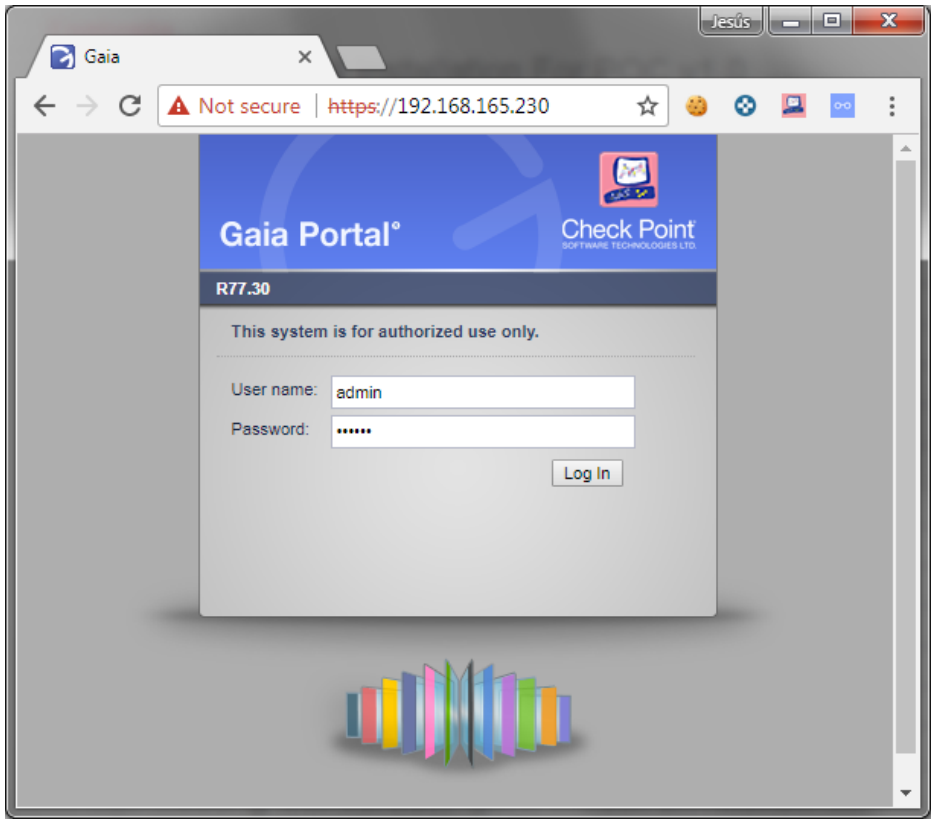


- End the process and wait until VM finish rebooting.

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

3. First Time Configuration Wizard

- Go to your management IP address configured in the previous step. You should go through a web browser and use the HTTPS protocol.



- Log in with the admin user and the password chosen in the step 2.

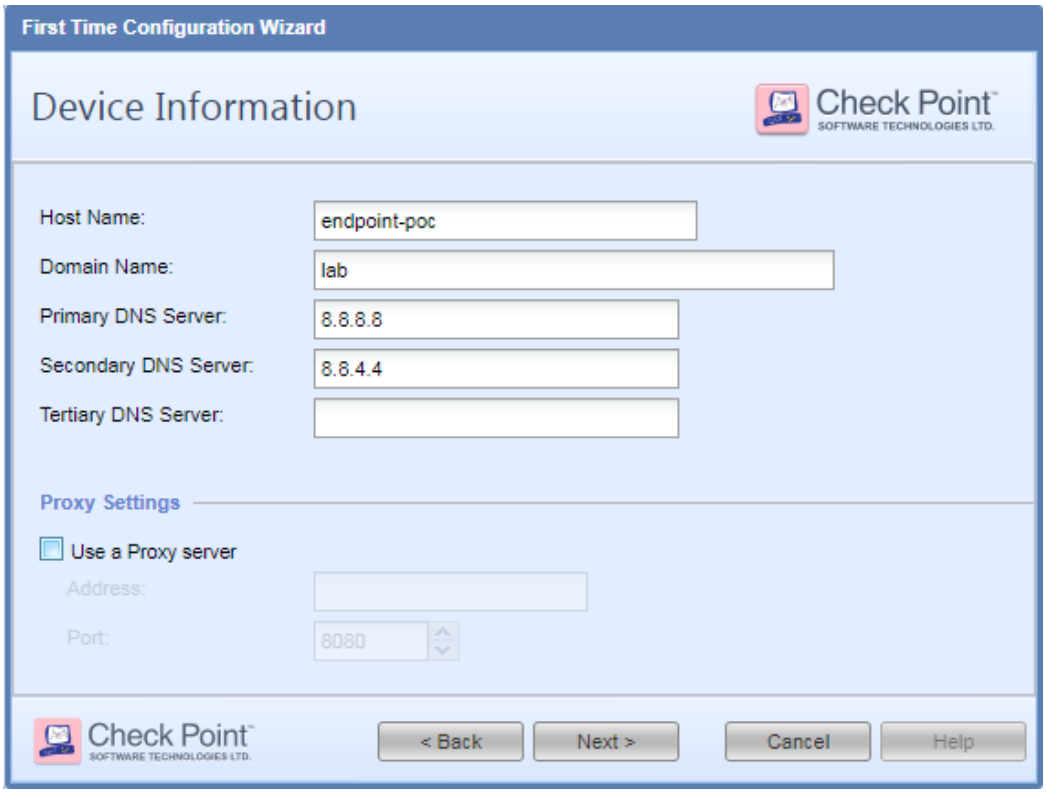
- Select **"Next"** in the first menu.

- Select **"Next"** in the second menu.

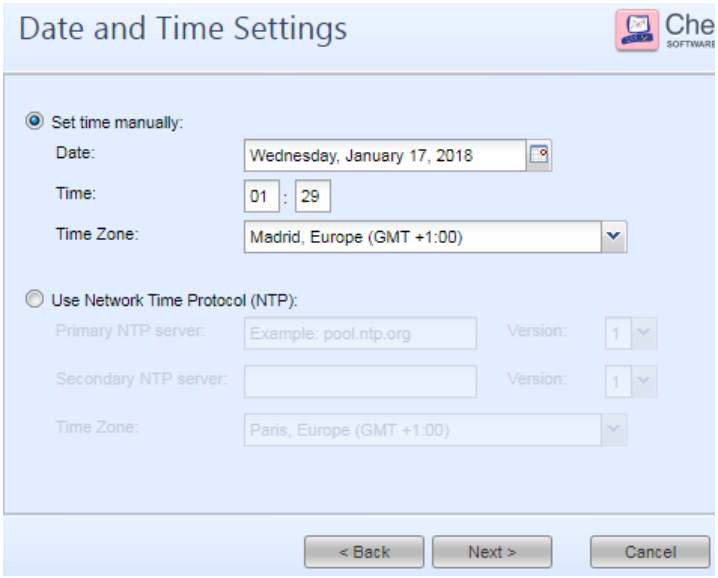
- Select **"Next"** in the third menu.

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

- Configure your device details and select **"Next"**



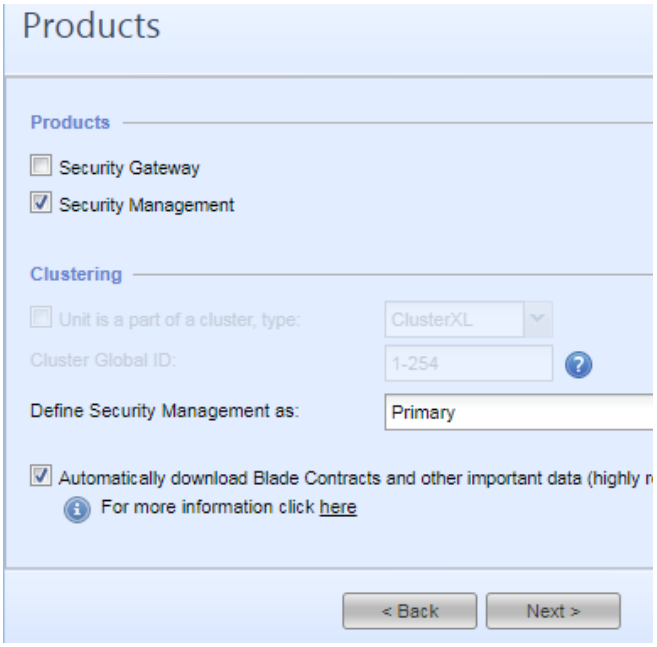
- Configure your right Time Zone and your NTP server in case you're using one.



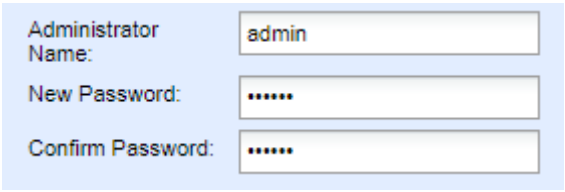
- Select **"Next"** in the next menu.

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

- Check only **"Security Management"** and select **"Next"**



- Configure your first admin user and select **"Next"**



- Select **"Next"** in the next menu.

- Select **"Finish"** and **"Yes"** in the last menu.

- Wait until the initial First Time Configuration Wizard finishes and the VM reboot.

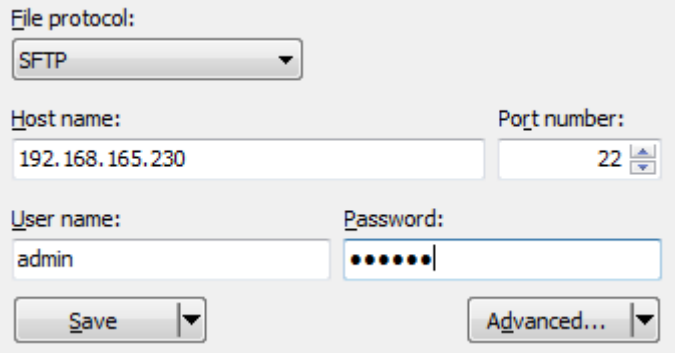
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

4. COPY FILES TO THE MANAGEMENT

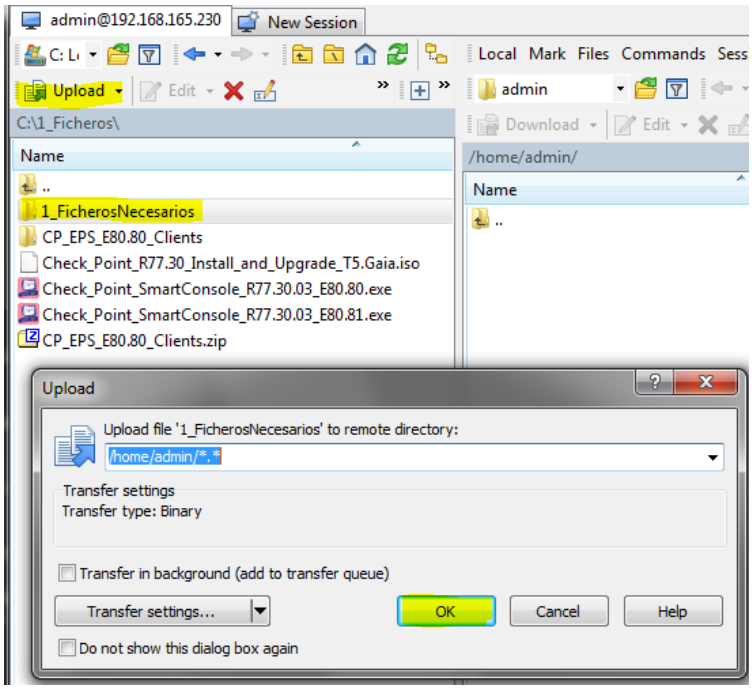
- Execute the next commands through SSH/Console session:

```
endpoint-poc> set expert-password
Enter new expert password:
Enter new expert password (again):
endpoint-poc> set user admin shell /bin/bash
endpoint-poc> save config
```

- Use WinSCP to copy the "**Needed Files**" from step 1 to the management.



- Select the folder "**1_FicherosNecesarios**" that contains the files from the step **1.B**
- Select "**Upload**" and "**OK**".
- The folder with the needed files will be copied to the path **/home/admin**

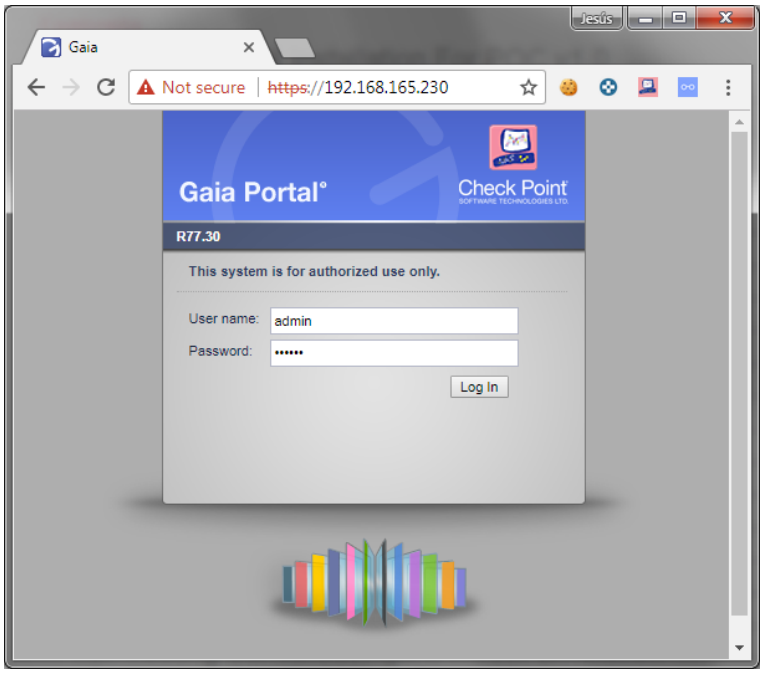


©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

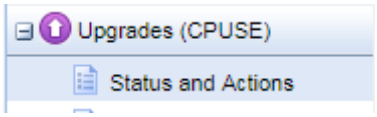
5. UPDATE THE CPUSE AGENT

5.1 ONLINE UPDATE

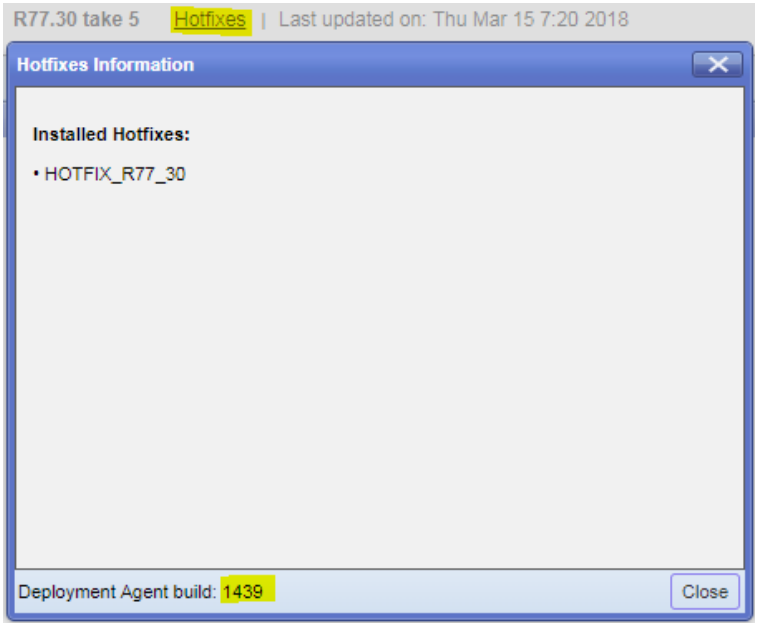
- CPUSE Agent will be updated automatically in case the management has access to the Internet.
- Go to the management web portal.



- Select Upgrades (CPUSE) > "**Status and Actions**"



- Check if the build is higer or equal to 1439 (Date: 15/03/18)



©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

5.2 OFFLINE UPDATE

- Download the last version of the CPUSE Agent: sk92449
- Copy the download file to the management through WinSCP.
- Unzip the download file: **tar -zxvf DeploymentAgent_<build>.tgz**
- Install the RPM package through: **rpm -Uhv --force CPda-00-00.i386.rpm**
- Stop all clish processes: **killall -v clish clishd**
- Restart the Confd Daemon: **tellpm process:confd => tellpm process:confd t**
- Start manually the CPUSE Agent daemon: **$DADIR/bin/dastart**

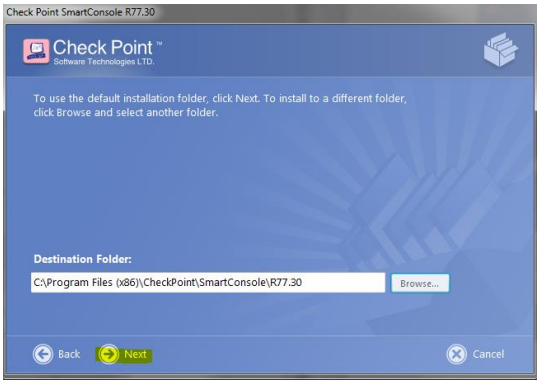
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

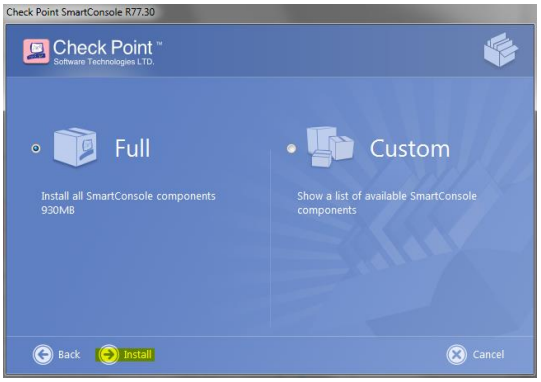
6. SmartConsole R77.30.03 / E80.81 Installation

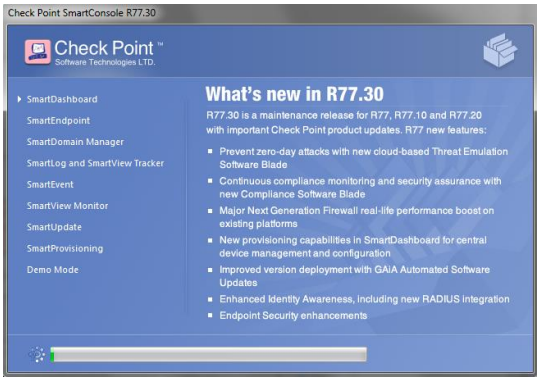
- Execute the download file from: step 1 > List A > File 3:

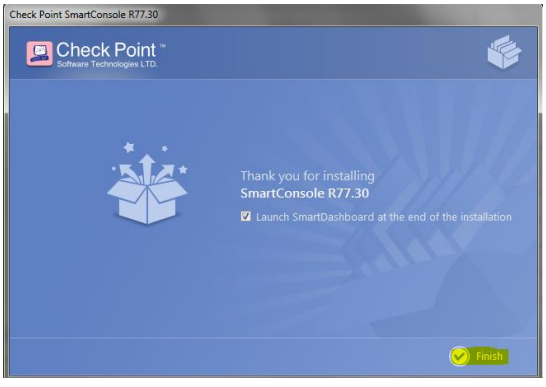
  SmartConsole for Endpoint Security Server R77.30.03 / E80.81 > Download

- Install the exe file following next steps with the default options:







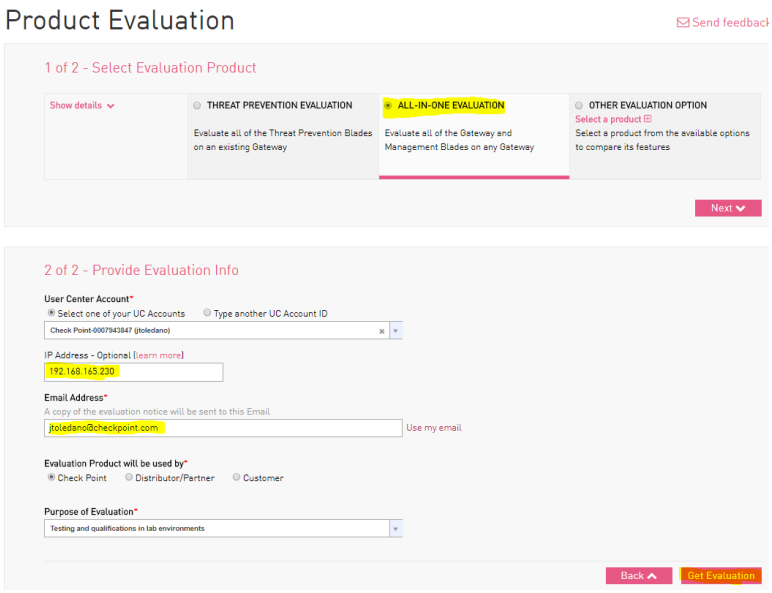


©2018 Check Point Software Technologies Ltd. All rights reserved

7. LICENSES CREATION (JUST NEEDED DURING A POC)

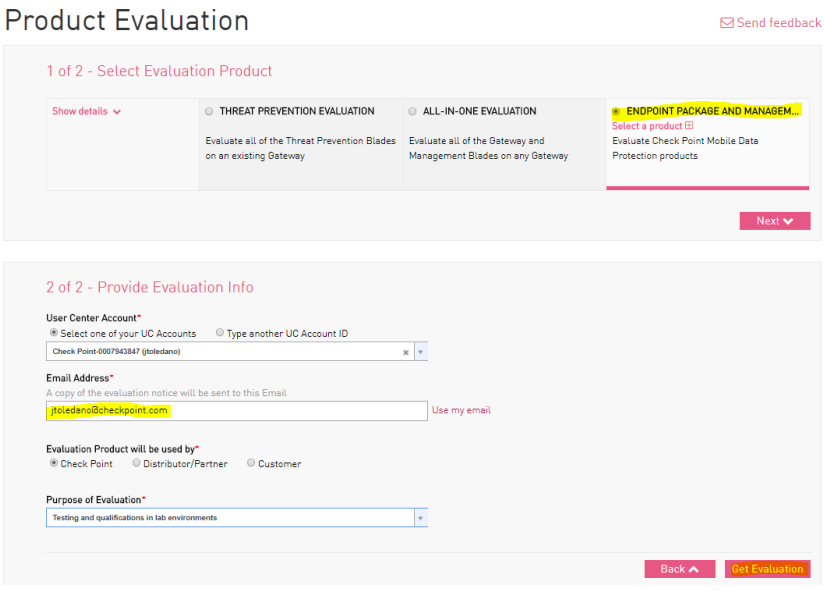
Create the needed licenses through the UserCenter:

- Endpoint Management License: All-In-One



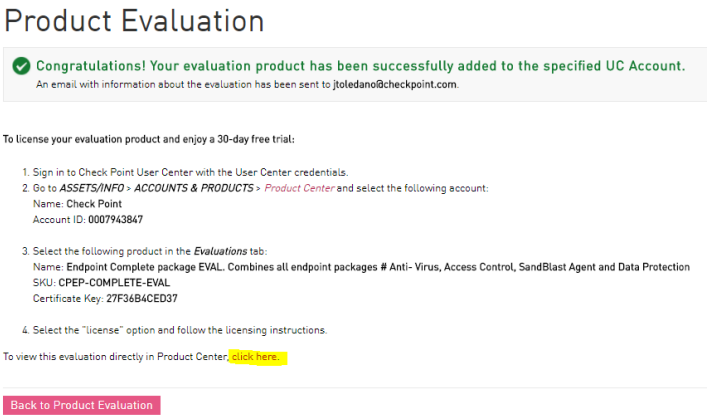
The license file (**CPLicenseFile.lic**) will be sent to the email address chosen through the form.

- Licenses to be able to use the Endpoint agent software and his blades (máximum 100 seats):

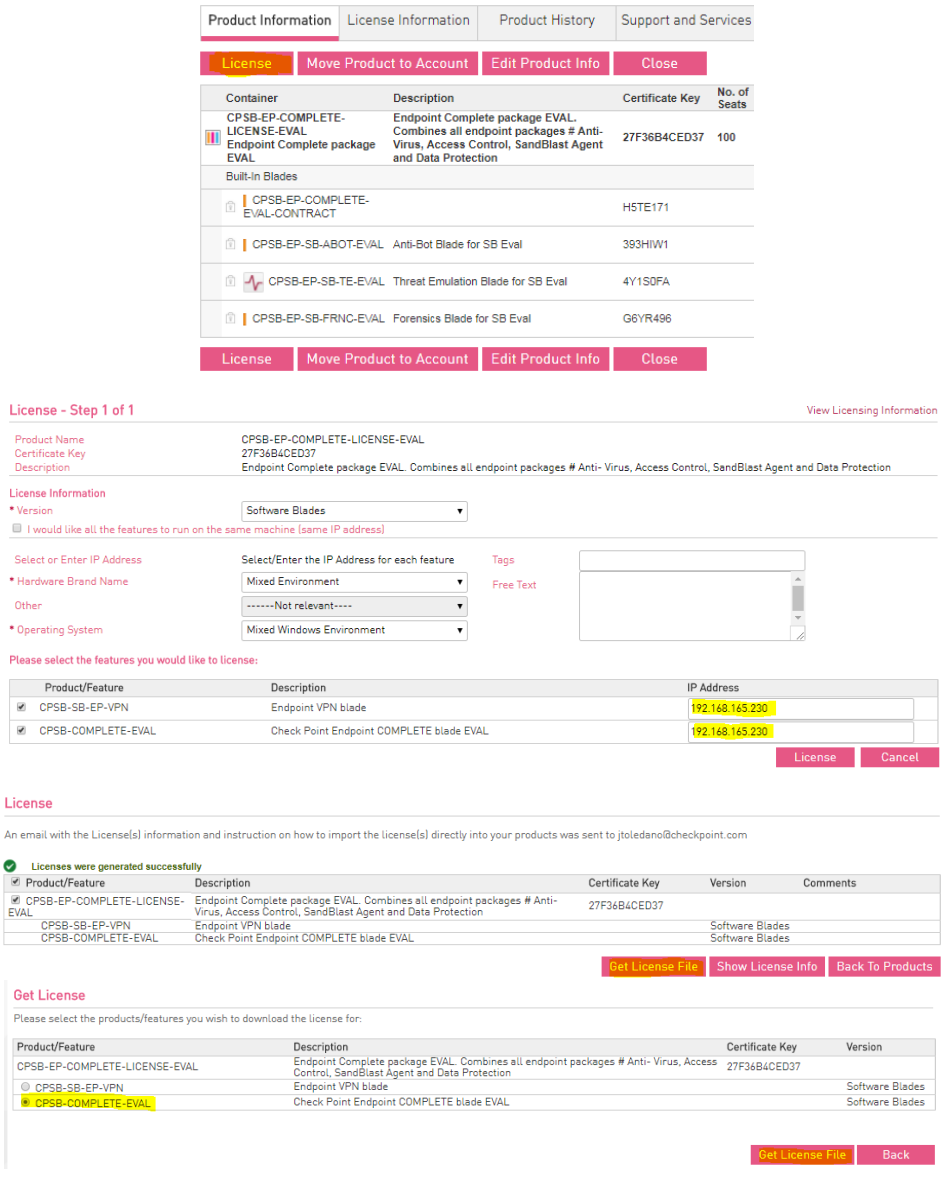


©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

8. Select “**Click here**”:



9. Select “**License**” to link the license to your Management IP Addresses.



You’ll be able to download a licenses file like:

CPLicenseFile_27F36B4CED37_CPSB-COMPLETE-EVAL.lic

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

8. LICENSES INSTALLATION

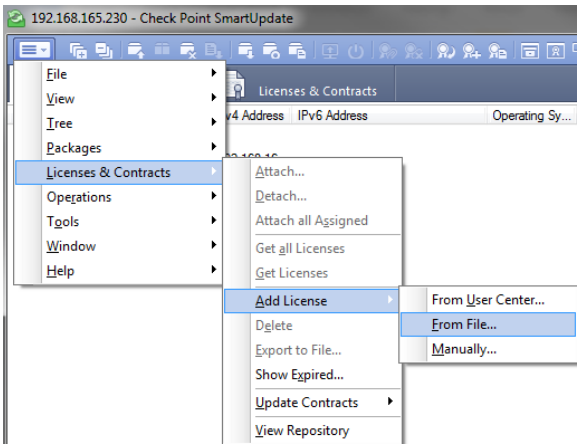
During the previous step (7) we got the next license files:

CPLicenseFile.lic

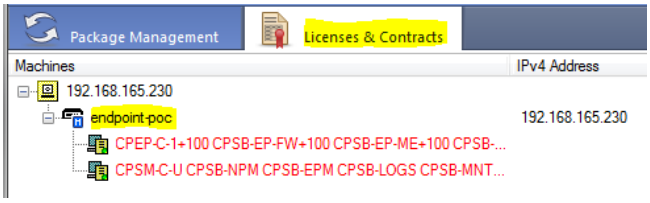
CPLicenseFile_27F36B4CED37_CPSB-COMPLETE-EVAL.lic

1. Open SmartUpdate:

2. Import your license files:



3. The files will do automatically the "**Attachment**" process:

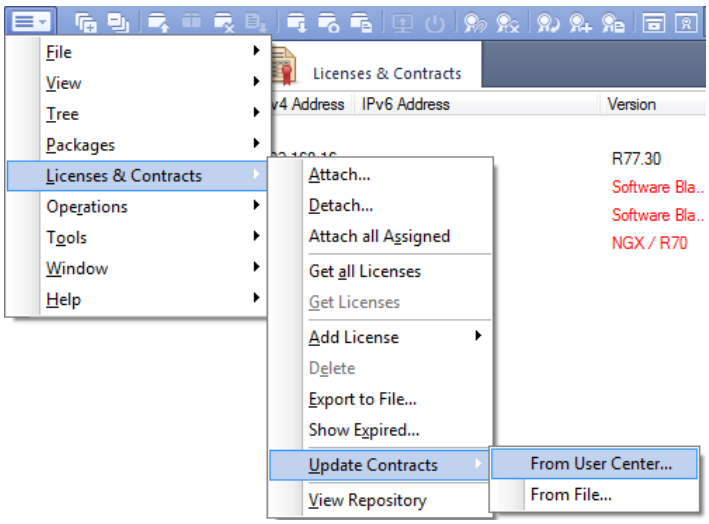


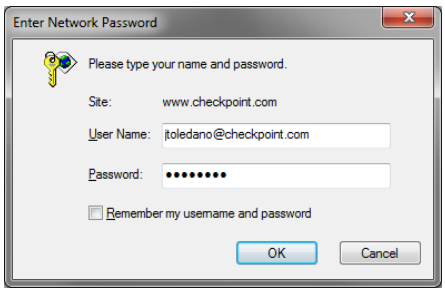
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

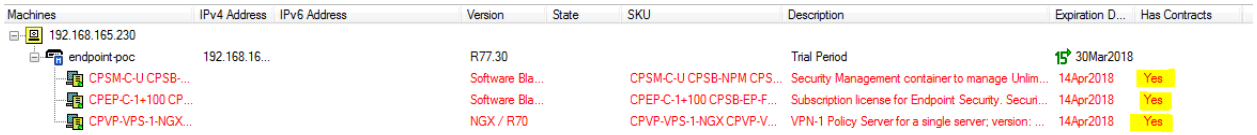
9. CONTRACTS INSTALLATION

1. Open SmartUpdate:

2. Update the contracts from the UserCenter:





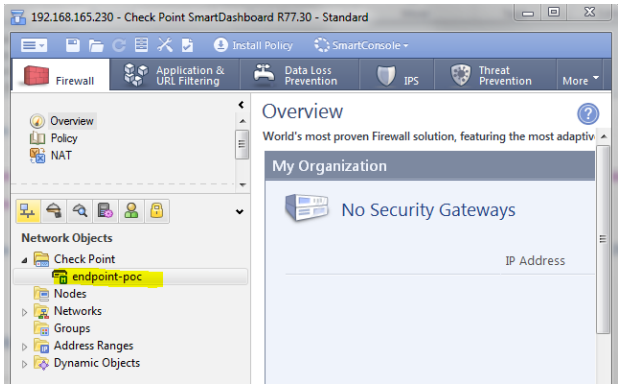


©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

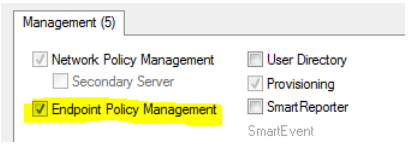
10. ACTIVACIÓN DE ENDPOINT POLICY MANAGEMENT

- Open SmartDashboard:

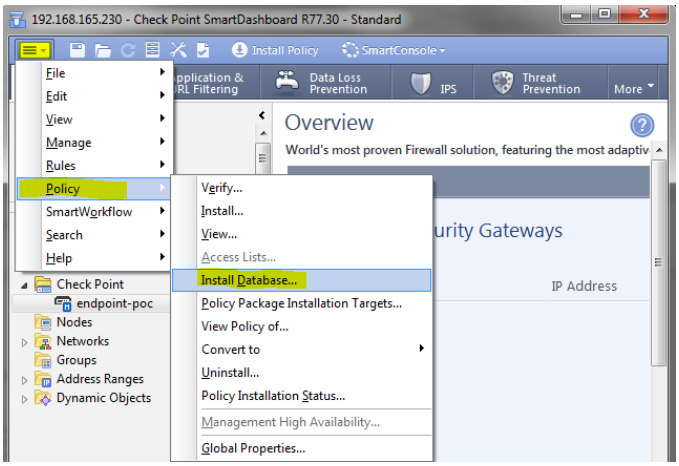
- Edit the Management object.



- Check "**Endpoint Policy Management**" and click "**OK**"



- Do "**Install Database…**"

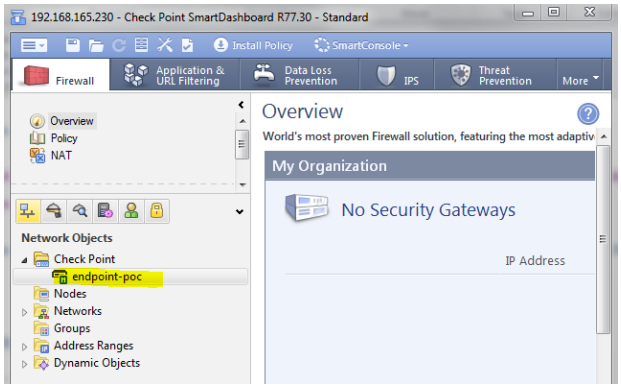


©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

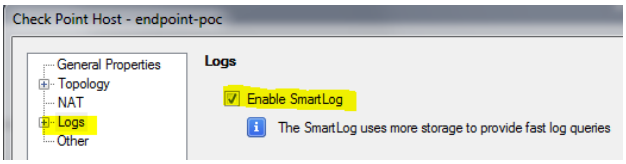
11. ENABLE SMARTLOG

- Open SmartDashboard:

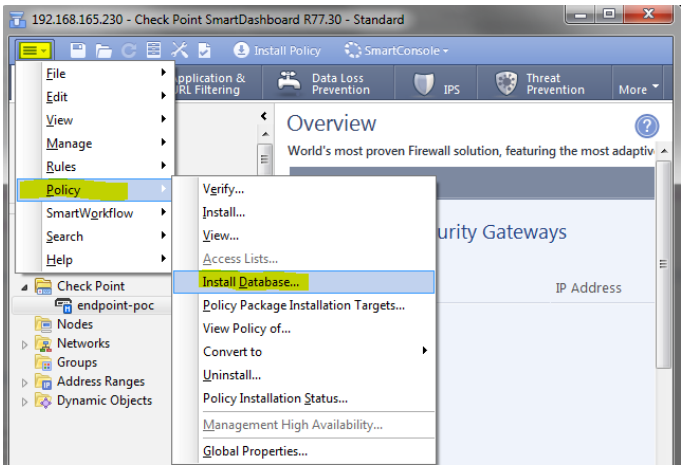
- Edit the Management object.



- Check "**SmartLog**" and click "**OK**"



- Do "**Install Database…**"



©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

12. JUMBO HOTFIX INSTALLATION FOR ENDPOINT SERVER

Execute the next commands through SSH/Console session:

[Expert@endpoint-poc:0]# **cd /home/admin/1_FicherosNecesarios/**

[Expert@endpoint-poc:0]# **mkdir R77.30_jhf_T143_EP**

[Expert@endpoint-poc:0]# **tar -xvzf R77.30_jhf_T143_EP.tgz -C R77.30_jhf_T143_EP/**

[Expert@endpoint-poc:0]# **cd R77.30_jhf_T143_EP**

[Expert@endpoint-poc:0]# **./UnixInstallScript**

[……..]

Do you want to continue (y/n) ? ***y***

[……..]

Installation program completed successfully.

Do you wish to reboot your machine (y/n) ? **y**

13. JUMBO HOTFIX R77.30.03 INSTALLATION FOR GAIA

Execute the next commands through SSH/Console session:

[Expert@endpoint-poc:0]# **cd /home/admin/1_FicherosNecesarios/**

[Expert@endpoint-poc:0]# **mkdir R77.30.03_Gaia**

[Expert@endpoint-poc:0]# **tar -xvzf R77.30.03_Gaia.tgz -C R77.30.03_Gaia/**

[Expert@endpoint-poc:0]# **cd R77.30.03_Gaia**

[Expert@endpoint-poc:0]# **./UnixInstallScript**

[……..]

Do you want to continue (y/n) ? ***y***

[……..]

Installation program completed successfully.

Do you wish to reboot your machine (y/n) ? **y**

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

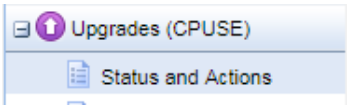
14. UPDATE TO THE LATEST JUMBOHOTFIX

- Go to the Management Web Portal. After the Endpoint Policy Management activation, you should get access through 4434

  https://[Dirección_IP]:4434

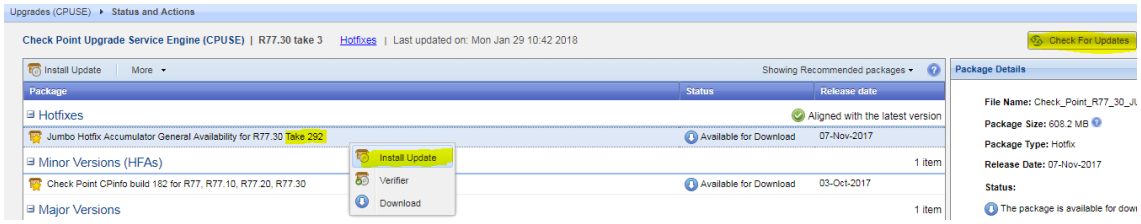
  NOTE: In case you don't get Access, go again through the step 10.

- Select Upgrades (CPUSE) > "**Status and Actions**"

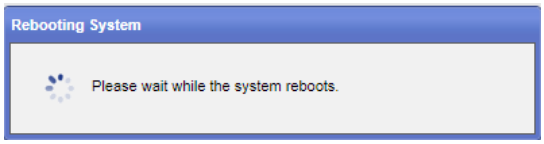


- "**Check for Updates**"

- Install the latest **Jumbo Hotfix Accumulator Take…**



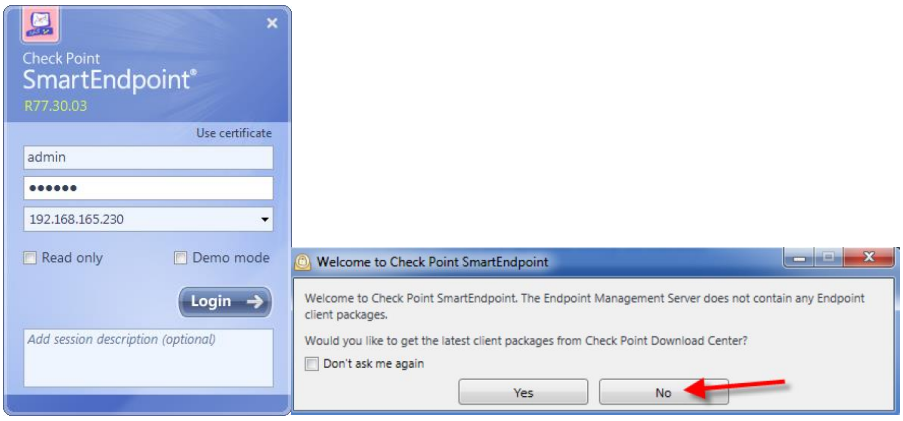
- The VM will automatically reboot.



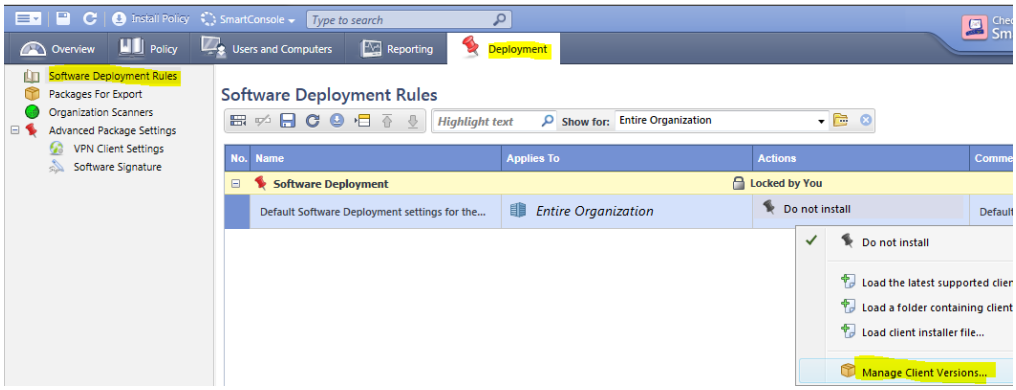
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

15. IMPORT THE ENDPOINT PACKAGES

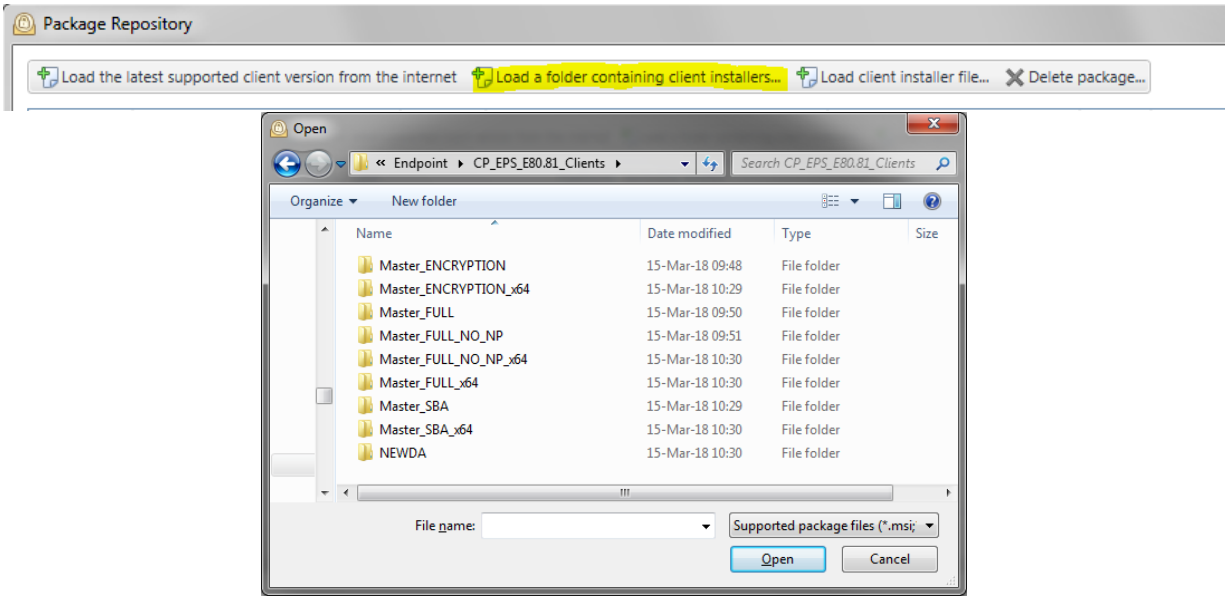
- Open SmartEndpoint and select No:



- Open the package repository:



- Import the container folder with all of the Endpoint packages previously downloaded from (Step 1 > List A > File 2):

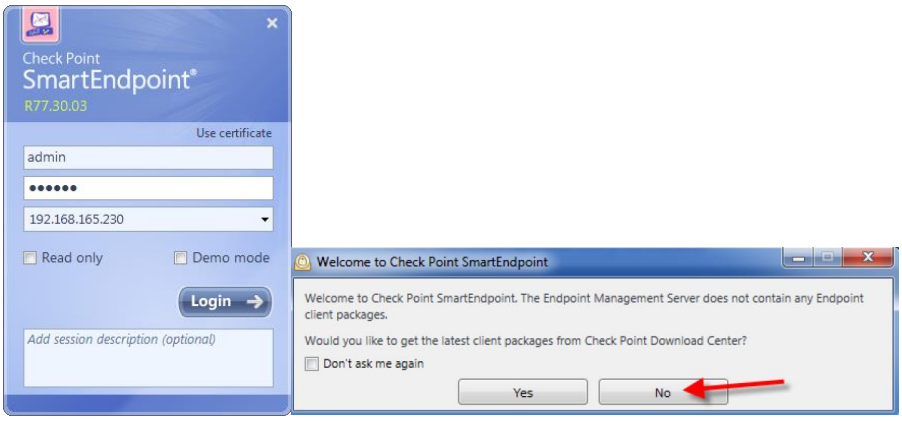


NOTE: In case the SmartConsole gets frozen and doesn't end uploading the packages, go through **Appendix III**

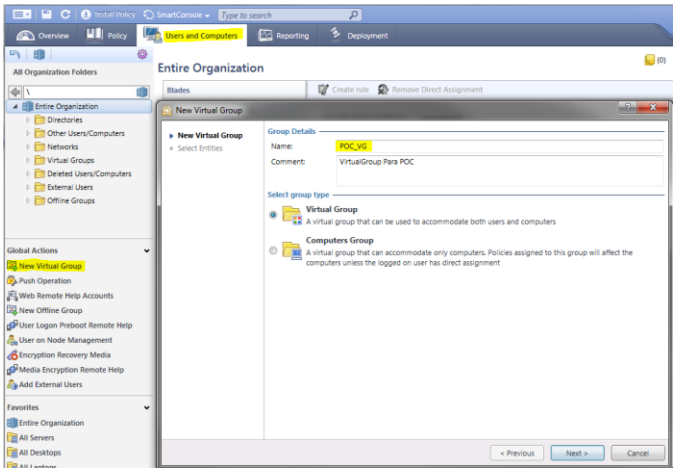
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

16. ENDPOINT CLIENT DEPLOYMENT

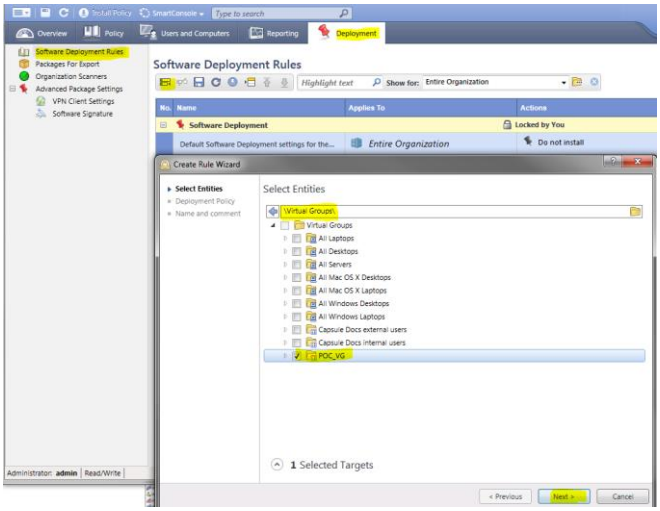
- Open SmartEndpoint:



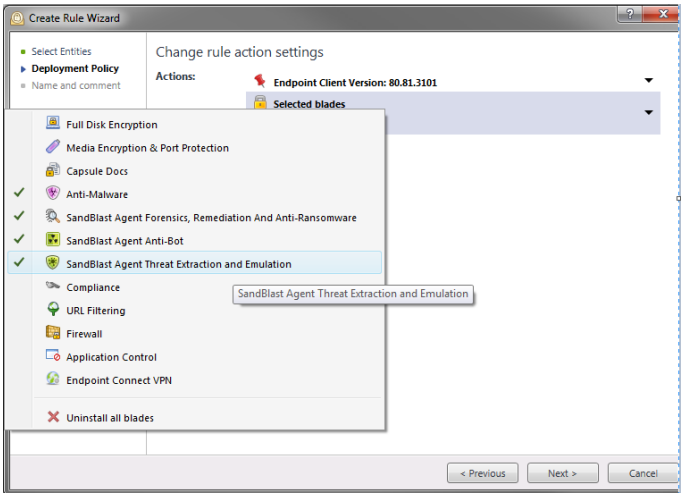
- Create a Virtual Group for the Deployment, select "**Next**" and "**Finish**":



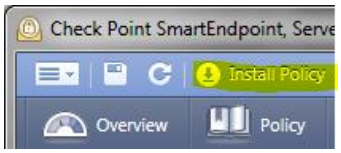
- Create a Deployment Rule for the Virtual Group created.



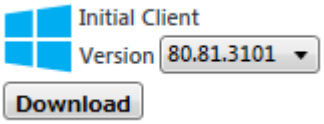
©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

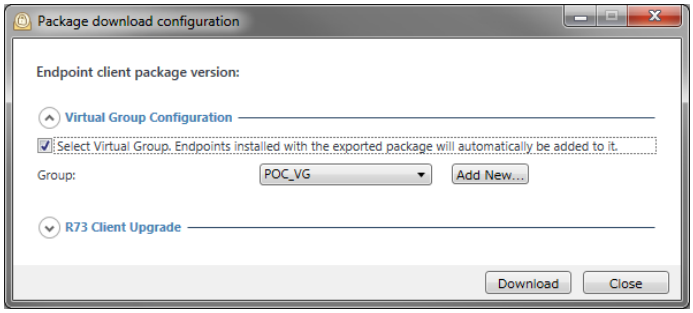


- Install Policy.



- Download “**Initial Client**”





The machines with Initial Client installed will be under your Virtual Group **POC_VG** created previously and will get the blades you chose above.

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

APPENDIX I: HELP RESOURCES

Endpoint Security Server:

- R77.30.03 Management Endpoint Security Release Notes > Download
- R77.30.03 Endpoint Security Management Administration Guide > Download

Endpoint Security Clients:

- E80.81 Endpoint Security Client for Windows User Guide > Download
- E80.81 Endpoint Security Client for Windows Release Notes > Download

Tools:

- SandBlast Agent Remediation Manager for Administrators > Download

  This admin tool have the end user features and add the next ones:

  - Quarantine – Send files to quarantine.
  - Delete – Use the SandBlast Agent Remediation Service to delete a file.
  - Import – Import a quarantine file from a different Endpoint.

- E80.81 Full Disk Encryption Offline Management Tool > Download

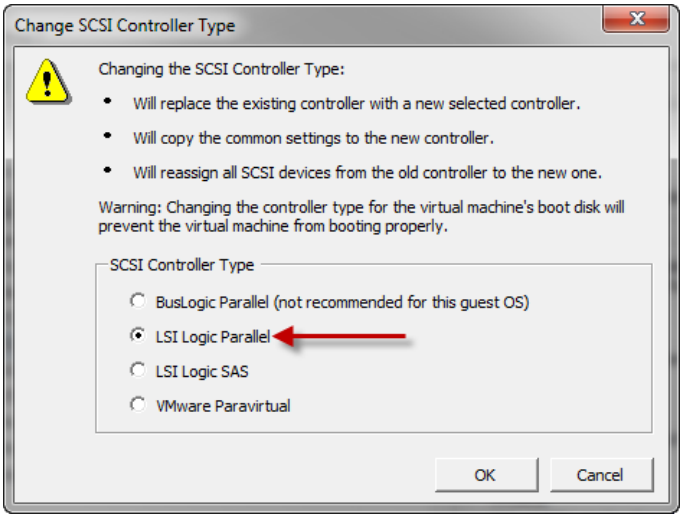
  This tool lets offline manage the users and give them a password to recovery their password and hard drives.

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

APPENDIX II: ESX/ESXI DOESN'T DETECT THE HARD DRIVE (SK7440)

If your ESX/EXi doesn't detect the hard drive added, it's due to the hard drive cpntroller:

Select one of this SCSI Controllers: "LSI Logic Parallel" or "LSI Logic SAS"



©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees

APPENDIX III: SMARTENDPOINT CONSOLE CRASHES WHEN UPLOADING ENDPOINT PACKAGES (SK121722)

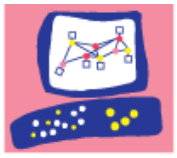
If your SmartEndpoint crashes when uploading Endpoint packages can be due to:

- Third-party Anti-Malware software prevents Endpoint packages from being uploaded to the server.
- User who installs and runs SmartConsole does not have administrator privileges.
- There is a missing folder on the server or missing files inside the /opt/CPsuite-R77/fw1/conf/SMC_Files/uepm/recimg folder.

To solve the last cause issue, follow next steps:

- Run: **# cpstop**
- Run: **# cd /opt/CPsuite-R77/fw1/conf/SMC_Files/uepm**
- Run: **# mkdir recimg**
- Run: **# chmod 2760 recimg**
- Copy "last.dll" amd "last.txt" from another running environment to the "recimg". If you don't have a previous environment, open a ticket with the support.
- Run: **# cd recimg**
- Run: **# chmod 660 ***
- Run: **# cpstart**

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees



Check Point
SOFTWARE TECHNOLOGIES LTD

©2018 Check Point Software Technologies Ltd. All rights reserved
[Internal Use] for Check Point employees