

## Install Checkpoint Firewall on VMware Workstation:

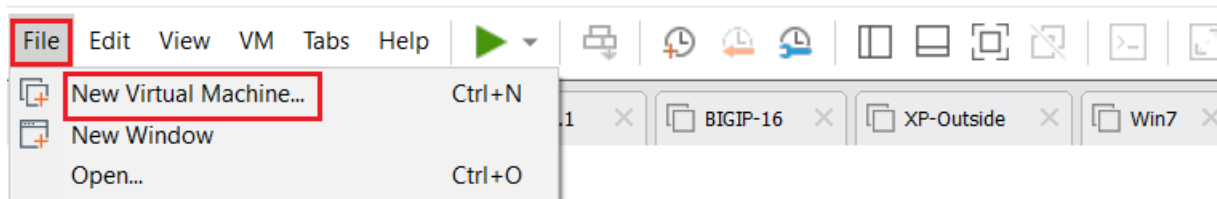
First download Gaia on the link below:

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk160736](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk160736)

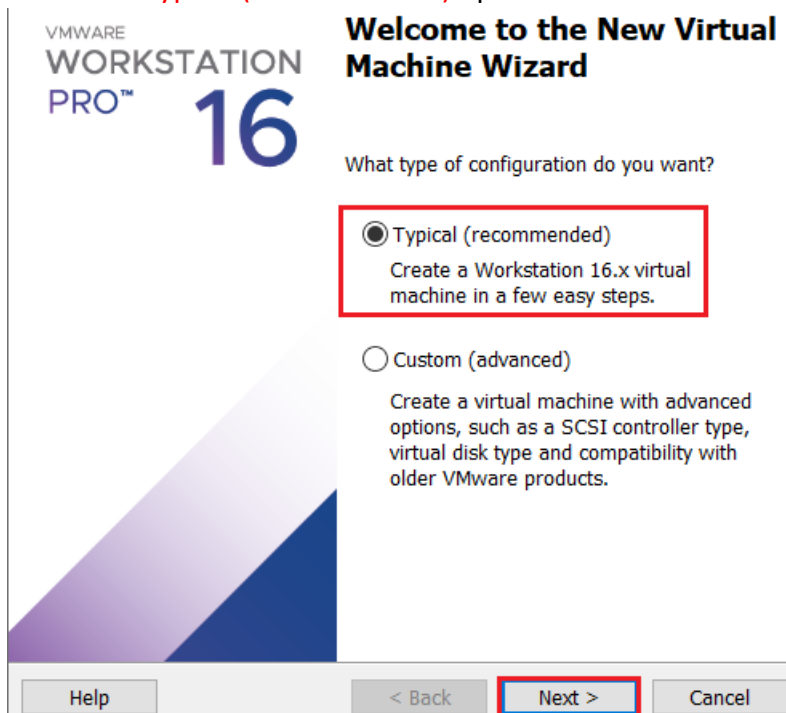
Choose the option: **Security Gateway>Standalone>Security Management>Clean Install.**



Now open VMware Workstation, click on the " **New Virtual Machine...**"



Select the **Typical (recommended)** option and click the **Next**.



Then provide the Gaia Image iso file location

Install from:

☐ Installer disc:

No drives available

☒ Installer disc image file (iso):

C:\Users\USER\Downloads\Check\_Point\_R80.40\_T29

Browse...

⚠ Could not detect which operating system is in this disc image.  
You will need to specify which operating system will be installed.

☐ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back **Next >** Cancel

Guest Operating System select the "Linux" and in version Select "Other Linux 2.6x kernel 64-bit" option.

New Virtual Machine Wizard

**Select a Guest Operating System**

Which operating system will be installed on this virtual machine?

Guest operating system

☐ Microsoft Windows

☒ Linux

☐ VMware ESX

☐ Other

Version

Red Hat Enterprise Linux 5 64-bit

Help < Back **Next >** Cancel

Now Give the Name of your virtual Machine such as **Checkpoint** and location where to save in your system then Click on **Next**.

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:

Location:

The default location can be changed at Edit > Preferences.

< Back **Next >** Cancel

Assign disk size and choose store virtual disk as a single file and then Click on **Next**.

**Specify Disk Capacity**  
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

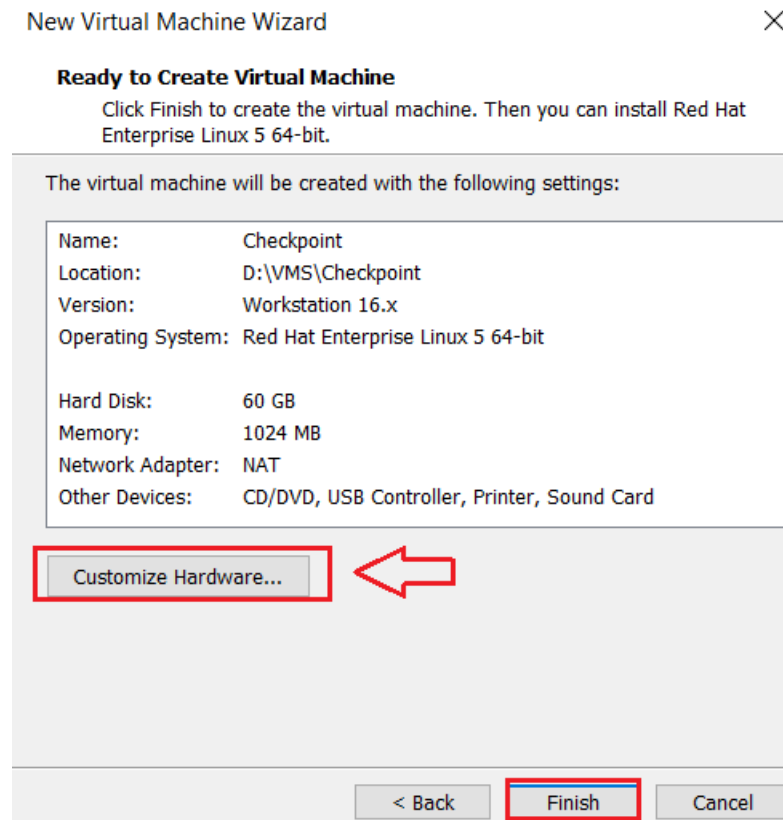
Recommended size for Red Hat Enterprise Linux 5 64-bit: 20 GB

☒ Store virtual disk as a single file  
☐ Split virtual disk into multiple files

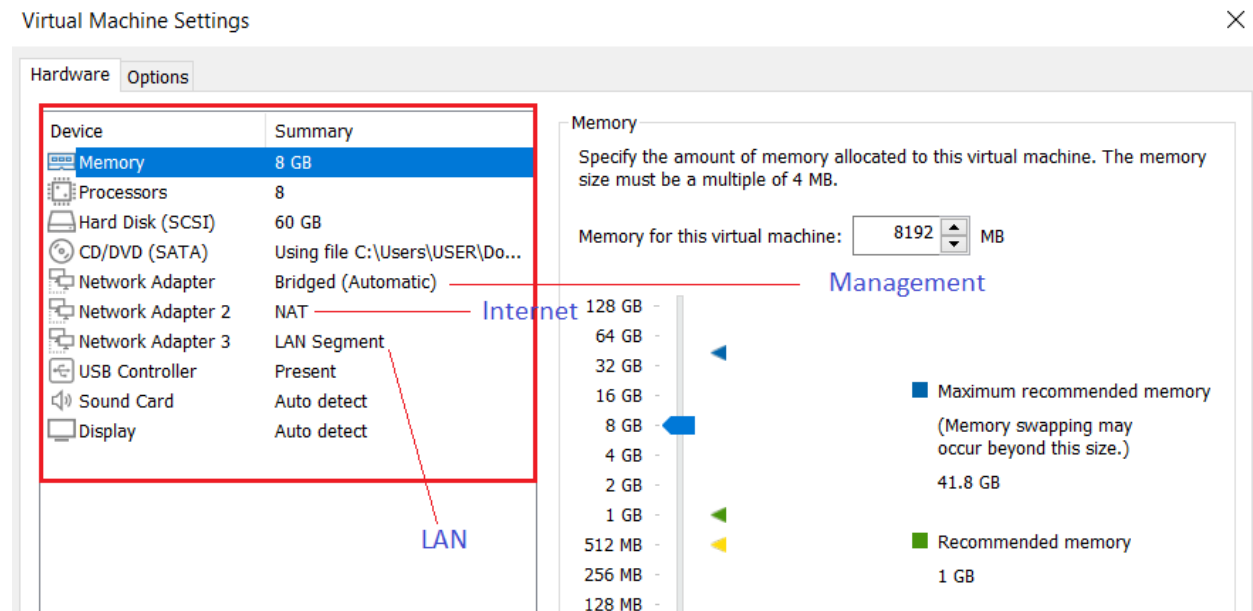
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help < Back **Next >** Cancel

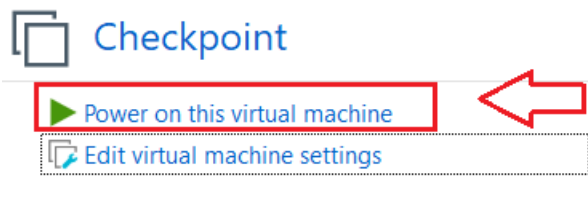
Click on **Customize Hardware....** Or just click finish to customize the Hardware.



Customize the memory, processors and add interfaces.



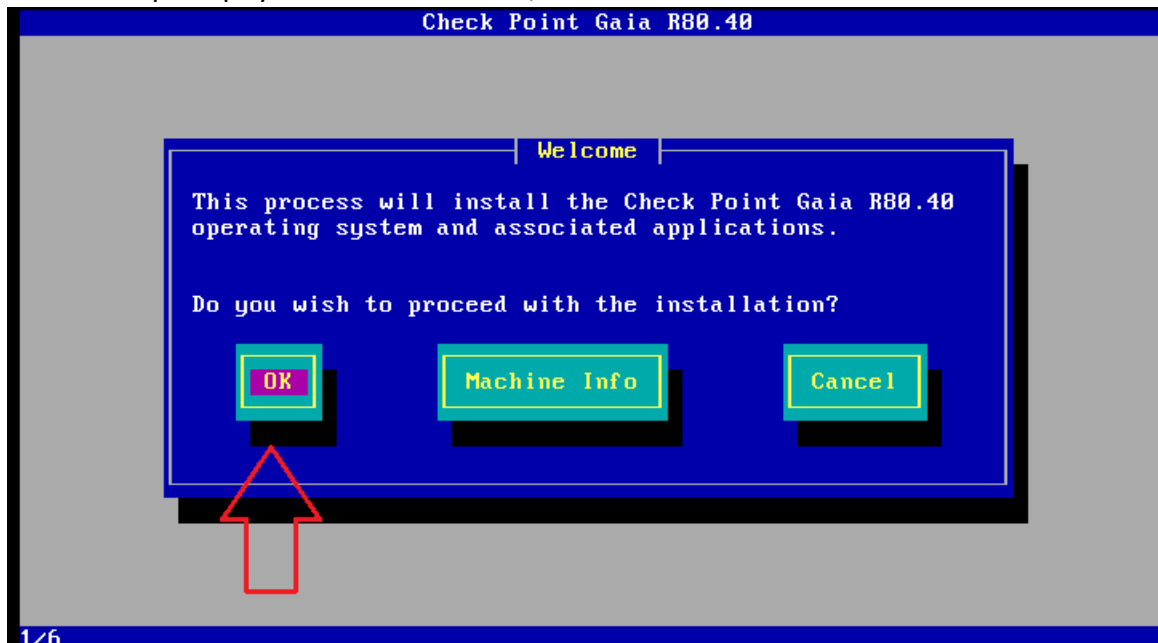
Click on **Power on this virtual machine** to start the checkpoint firewall installation.



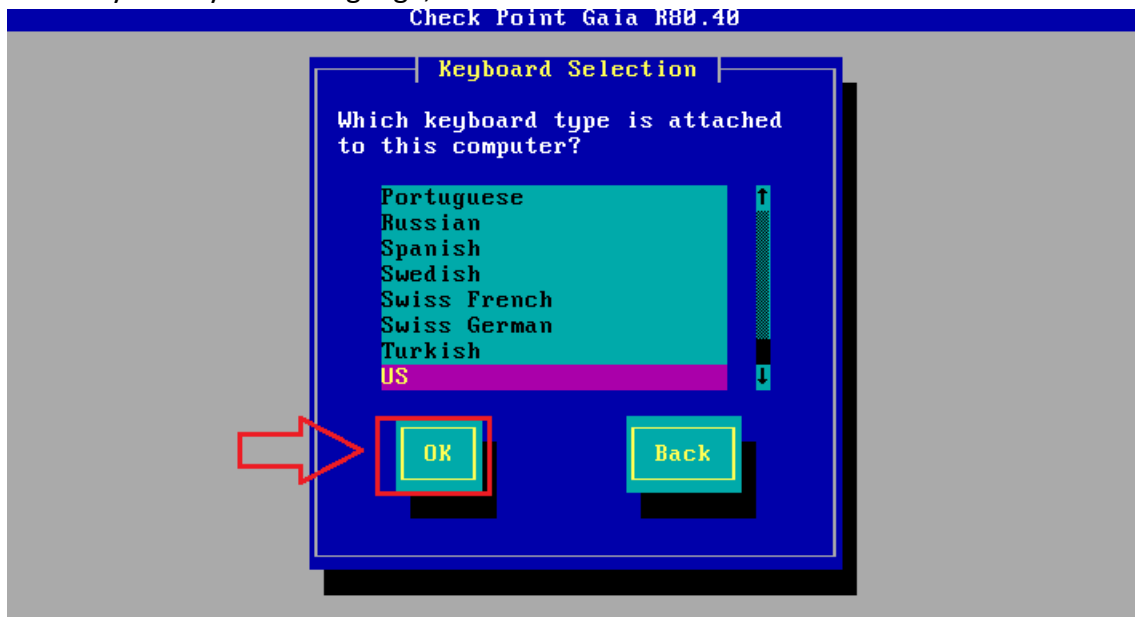
It will prompt you Gaia installation wizard, Stop the boot process by typing any key and select **Install Gaia on this system**.



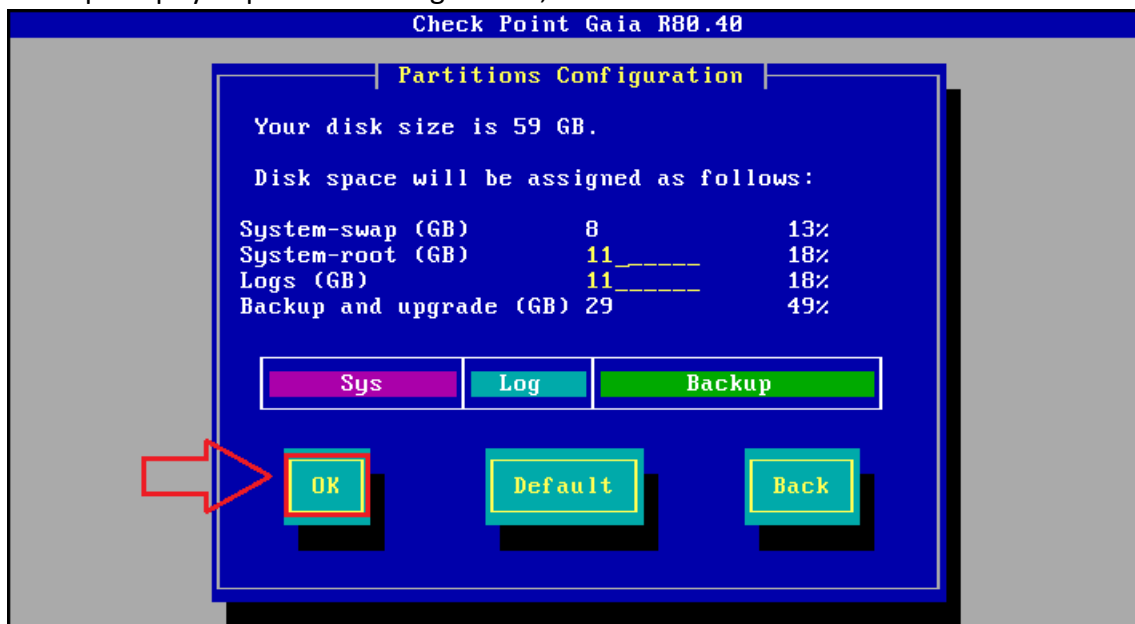
Now it will prompt you Welcome screen, click on the **OK** to start the installation.



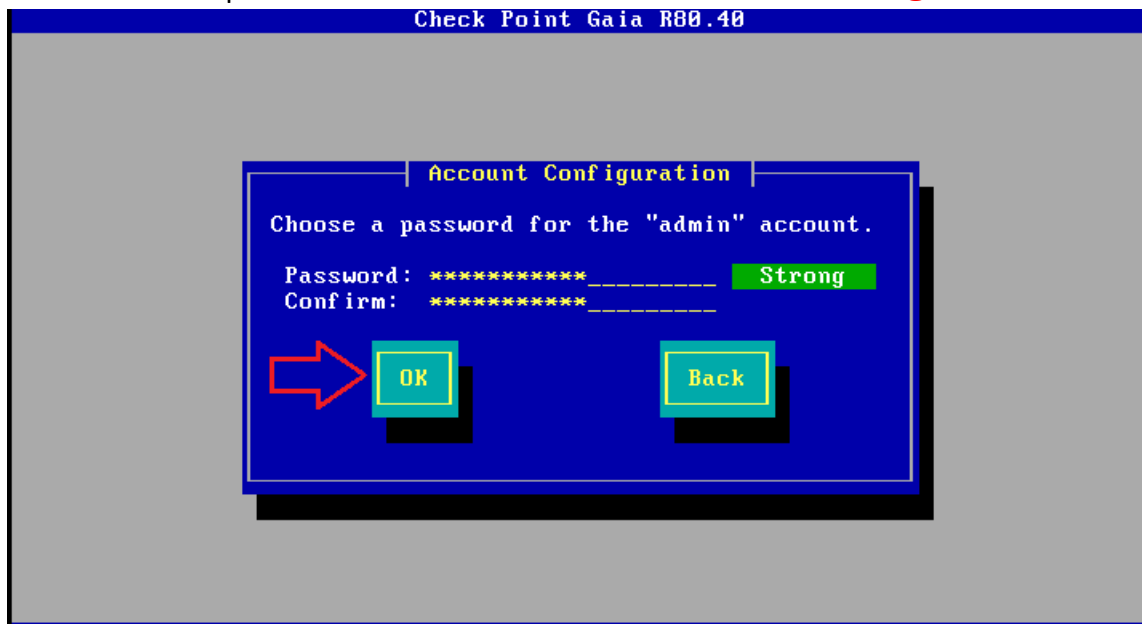
Choose your keyboard language, in this case **US** and click **OK**.



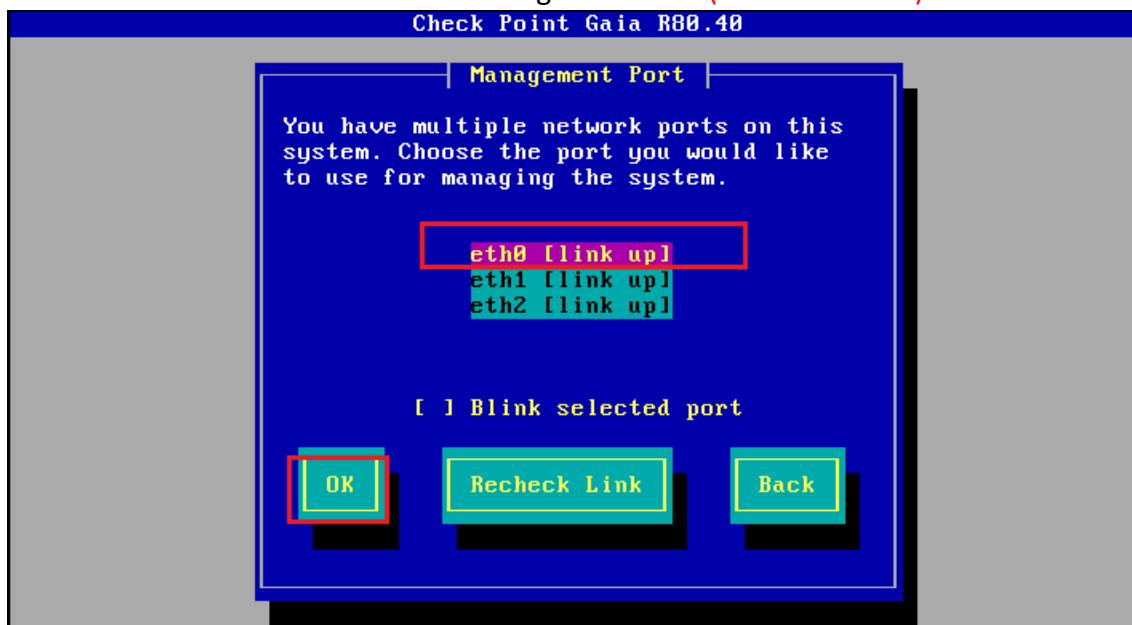
It will prompt you partition configuration, leave it all default and enter on **OK**.



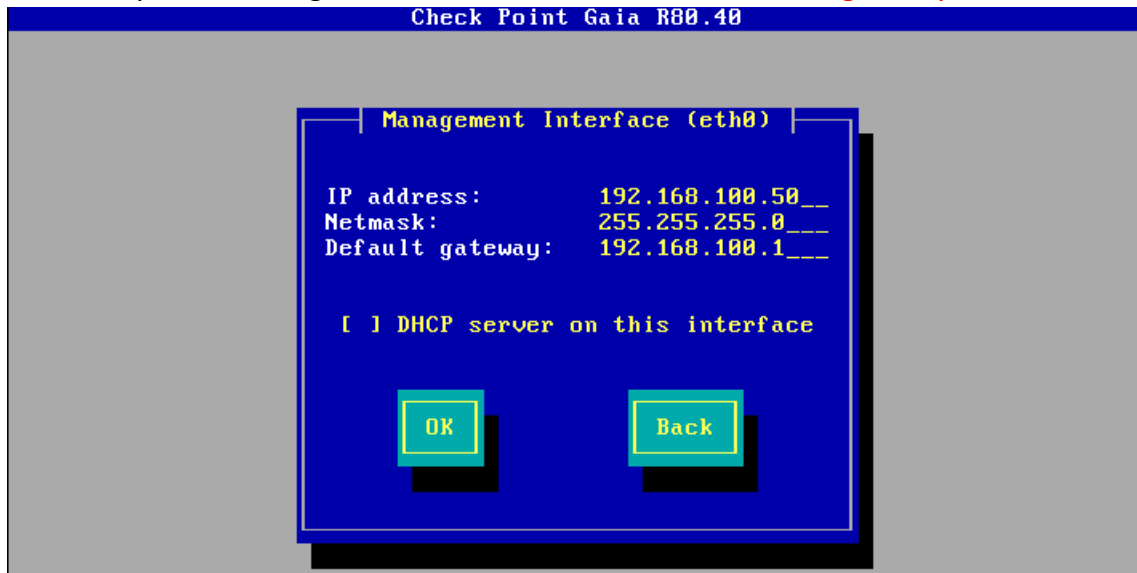
Now choose the password for admin account in this case I set **Admin@12345** click **OK**.



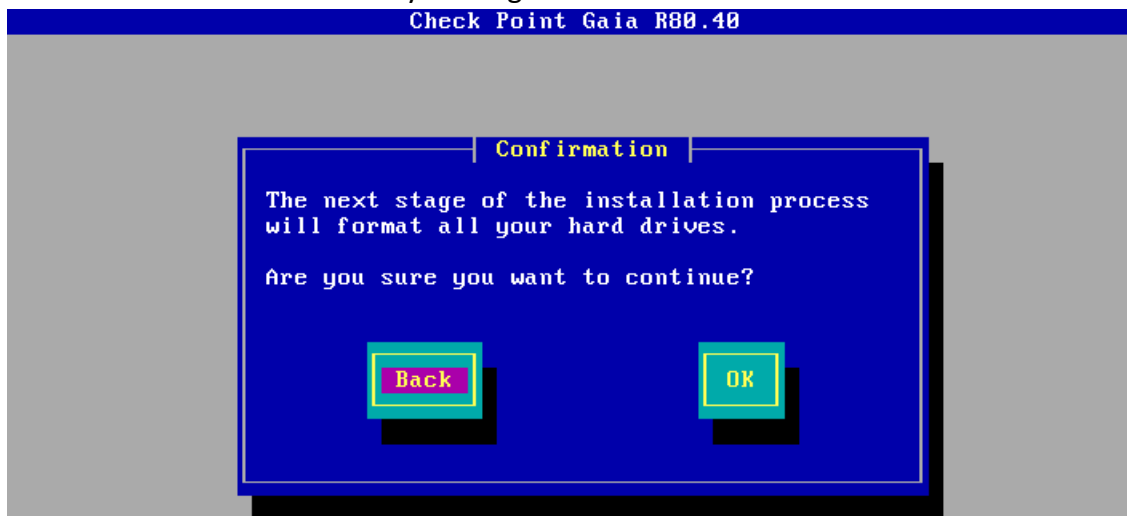
Choose which interface will be the Management Port (I'll choose **eth0**)



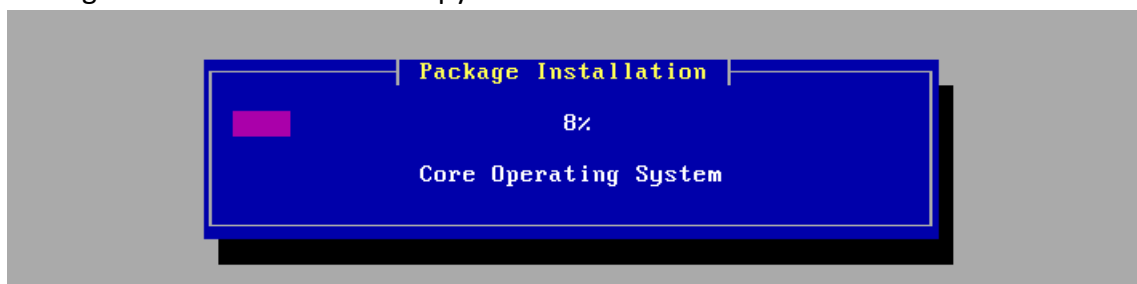
It will ask you for management interface IP-address and default gateway.



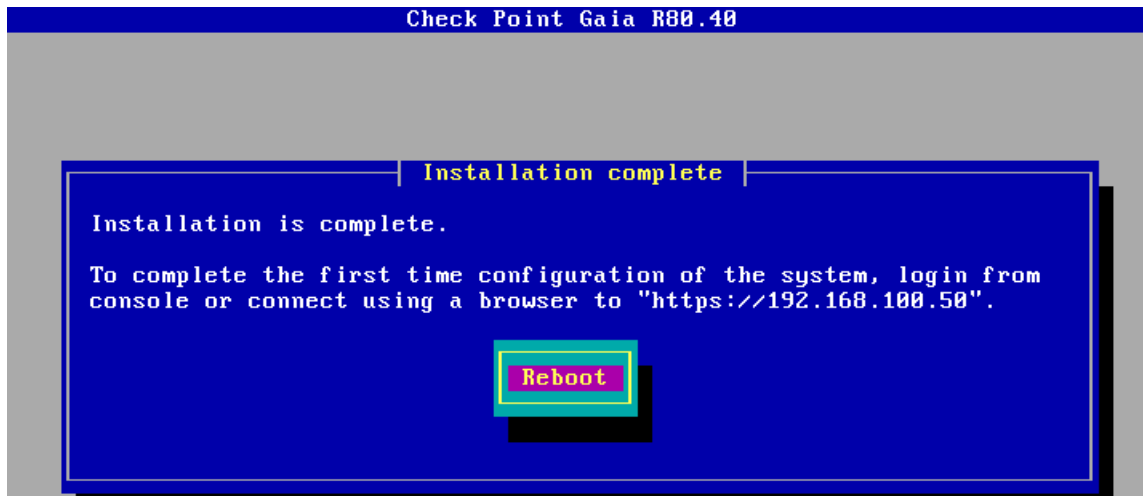
Proceed with the installation by clicking the OK button.



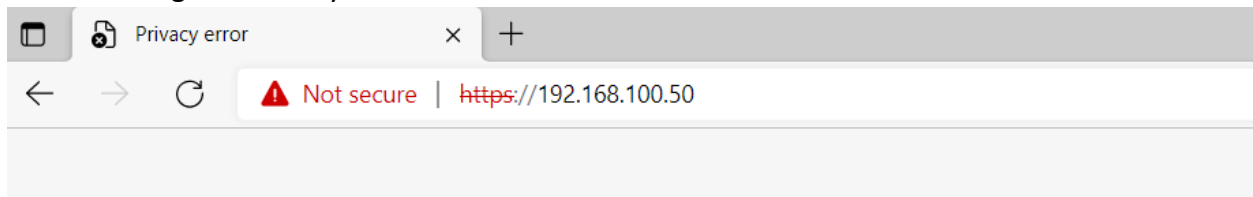
Package Installation started to copy files.



Once it finishes we'll **reboot** the machine. After completion of installation, it will give URL path for the first-time installation.



Now open your browser and navigate to **https://your\_gaia\_ipaddress** and accept the certificate error warning and enter your credentials here.



## Your connection isn't private

Attackers might be trying to steal your information from **192.168.100.50** (for example, passwords, messages, or credit cards).

NET::ERR\_CERT\_AUTHORITY\_INVALID

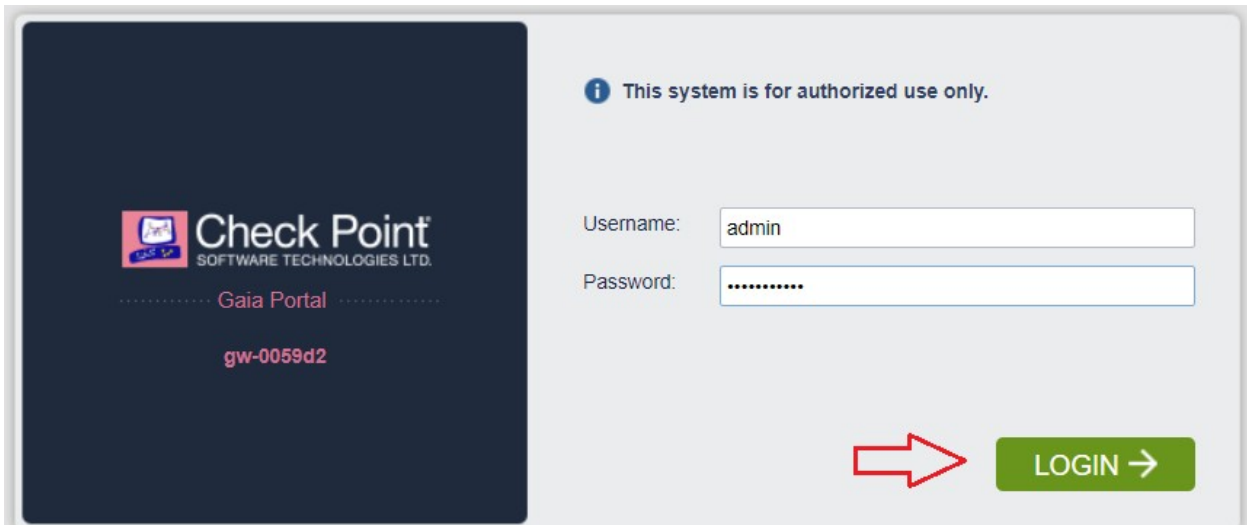
Hide advanced

Go back

This server couldn't prove that it's **192.168.100.50**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

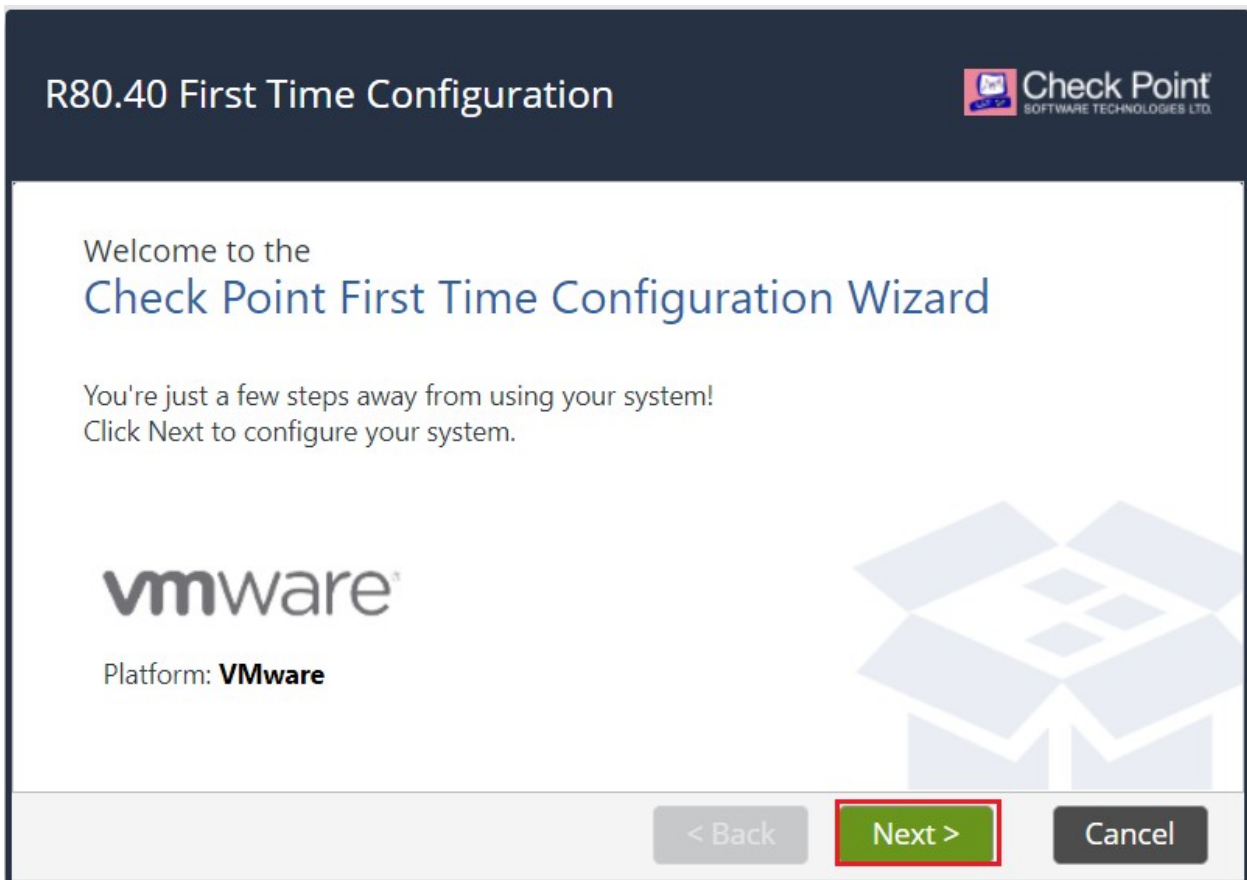
[Continue to 192.168.100.50 \(unsafe\)](#)

Then you will get Login Screen of Checkpoint Firewall. Now you can Login with your **User Name** and **Password** which you have assign to your firewall.



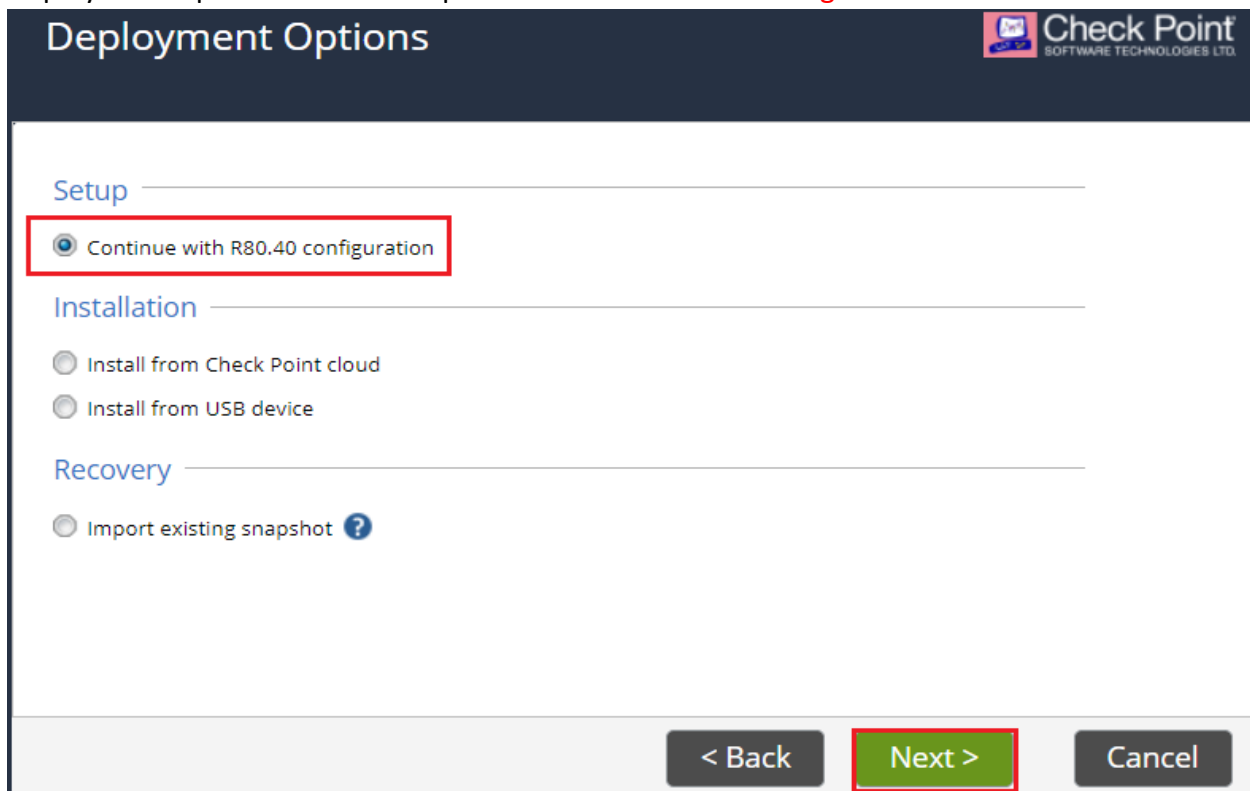
The login screen for the Checkpoint Firewall. On the left, a dark blue panel displays the Check Point logo, 'Gaia Portal', and the device ID 'gw-0059d2'. On the right, a light gray panel contains a message: 'This system is for authorized use only.' Below this, there are input fields for 'Username:' (containing 'admin') and 'Password:' (masked with dots). A red arrow points to a green 'LOGIN →' button.

Now it will prompt you, First-time configuration wizard. Click on the **next** to start your configuration.



The 'R80.40 First Time Configuration' wizard. The title bar shows 'R80.40 First Time Configuration' and the Check Point logo. The main content area says 'Welcome to the Check Point First Time Configuration Wizard' and 'You're just a few steps away from using your system! Click Next to configure your system.' The VMware logo and 'Platform: VMware' are shown. At the bottom, there are three buttons: '< Back' (disabled), 'Next >' (highlighted with a red box), and 'Cancel'.

Deployment Options choose Setup **Continue with R80.40 configurations** and click **Next**.



The screenshot shows the 'Deployment Options' window with the Check Point logo in the top right. The 'Setup' section is active, and the option 'Continue with R80.40 configuration' is selected and highlighted with a red box. Below it, the 'Installation' section has two unselected options: 'Install from Check Point cloud' and 'Install from USB device'. The 'Recovery' section has one unselected option: 'Import existing snapshot' with a help icon. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

## Deployment Options

Setup

- ☒ Continue with R80.40 configuration

Installation

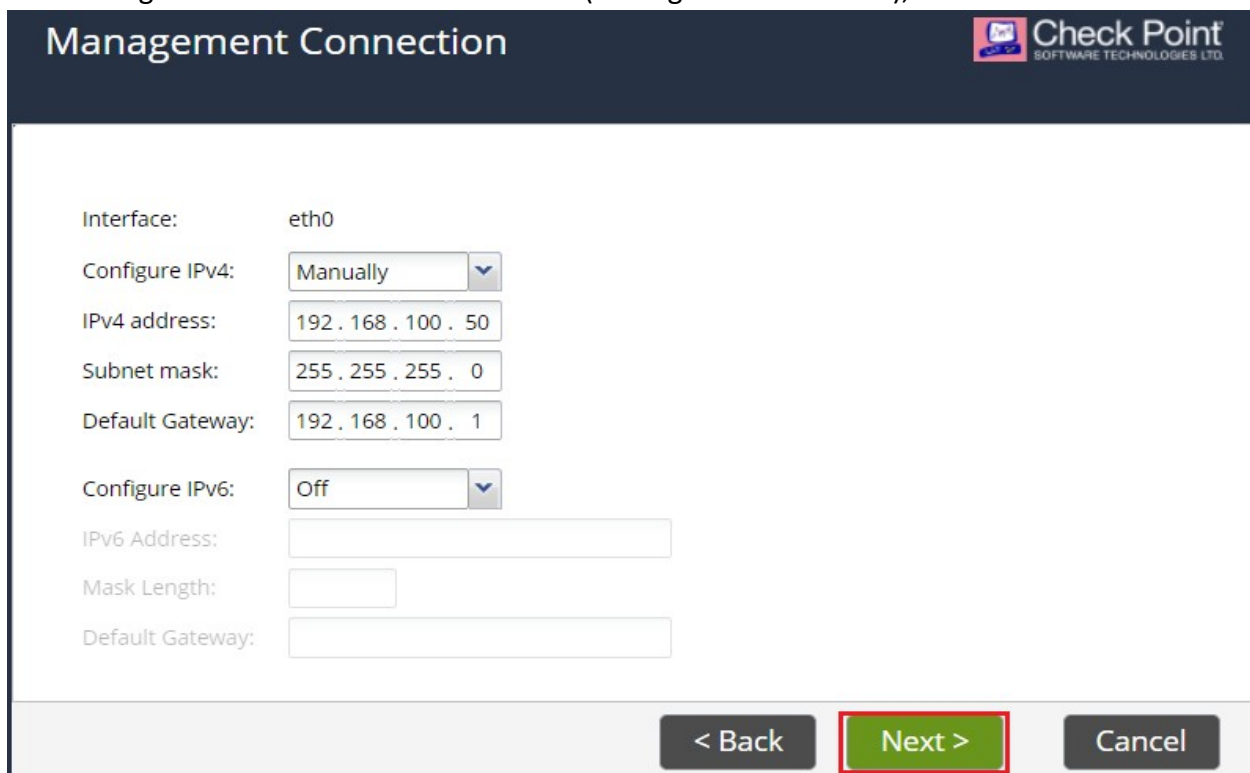
- ☐ Install from Check Point cloud
- ☐ Install from USB device

Recovery

- ☐ Import existing snapshot ?

< Back   Next >   Cancel

Now configure Network Connection of **eth0** (Management Interface), and then Click on **Next**.



The screenshot shows the 'Management Connection' window with the Check Point logo in the top right. The 'Interface' is set to 'eth0'. Under 'Configure IPv4', the 'Manually' option is selected in a dropdown. The IPv4 address is '192 . 168 . 100 . 50', the subnet mask is '255 . 255 . 255 . 0', and the default gateway is '192 . 168 . 100 . 1'. Under 'Configure IPv6', the 'Off' option is selected in a dropdown. The IPv6 address, mask length, and default gateway fields are empty. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

## Management Connection

Interface: eth0

Configure IPv4: Manually

IPv4 address: 192 . 168 . 100 . 50

Subnet mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 100 . 1

Configure IPv6: Off

IPv6 Address:

Mask Length:

Default Gateway:

< Back   Next >   Cancel

## Internet Connection



Configure the interface to connect to the Internet (optional) ?

Interface: eth1

Configure IPv4: Off

IPv4 address:

Subnet mask:

Configure IPv6: Off

IPv6 Address:

Subnet:

< Back

Next >

Cancel

Now provide the **Host name**, **Domain name** and Primary **DNS** address here.

## Device Information



Host Name: GW-FW

Domain Name: Optional

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

Tertiary DNS Server:

### Proxy Settings

☐ Use a Proxy server

Address:

Port: 8080

< Back

Next >

Cancel

Now on the Next Screen Select your Time and set Time and date then Click on **Next**.

## Date and Time Settings



☒ Set time manually:

Date:

Time:  :

Time Zone:

☐ Use Network Time Protocol (NTP):

Primary NTP server:  Version:

Secondary NTP server:  Version:

Time Zone:

[< Back](#) [Next >](#) [Cancel](#)

Now here you have to choose the installation type, Select the **Security gateway or Security management** option here.

## Installation Type

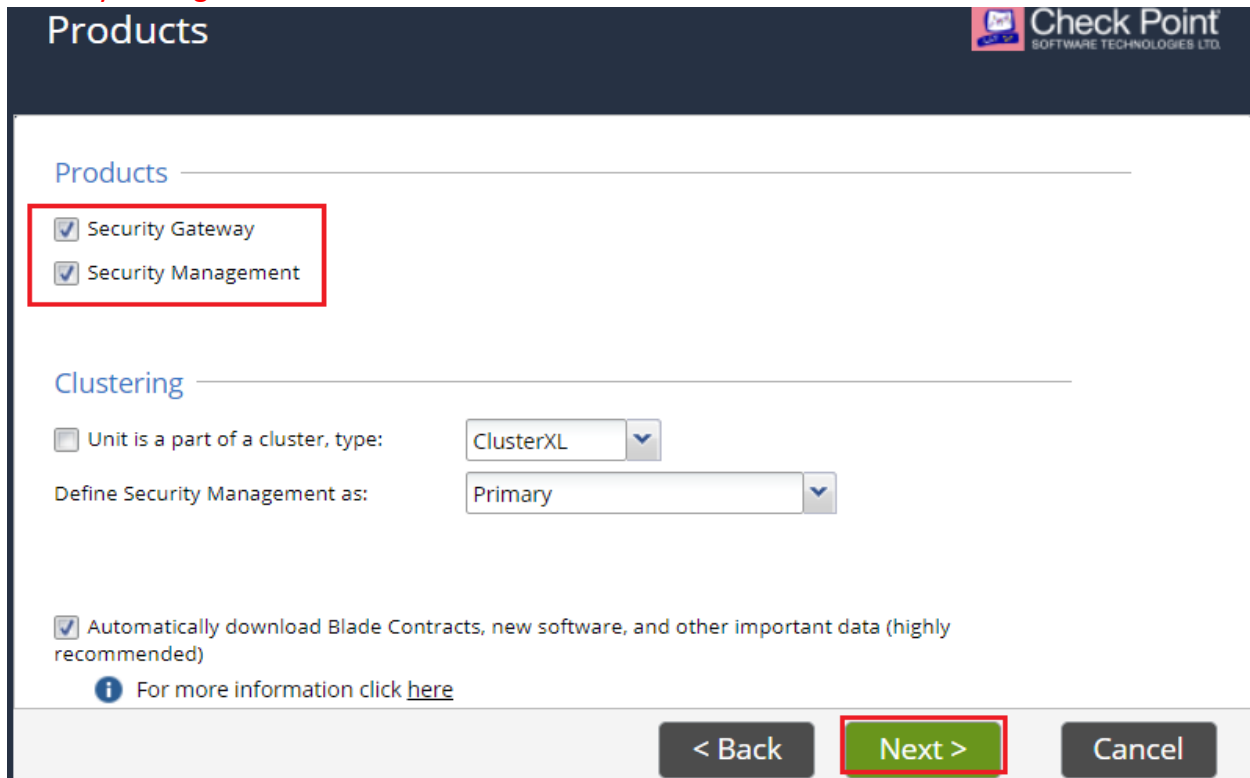


☒ Security Gateway and/or Security Management

☐ Multi-Domain Server

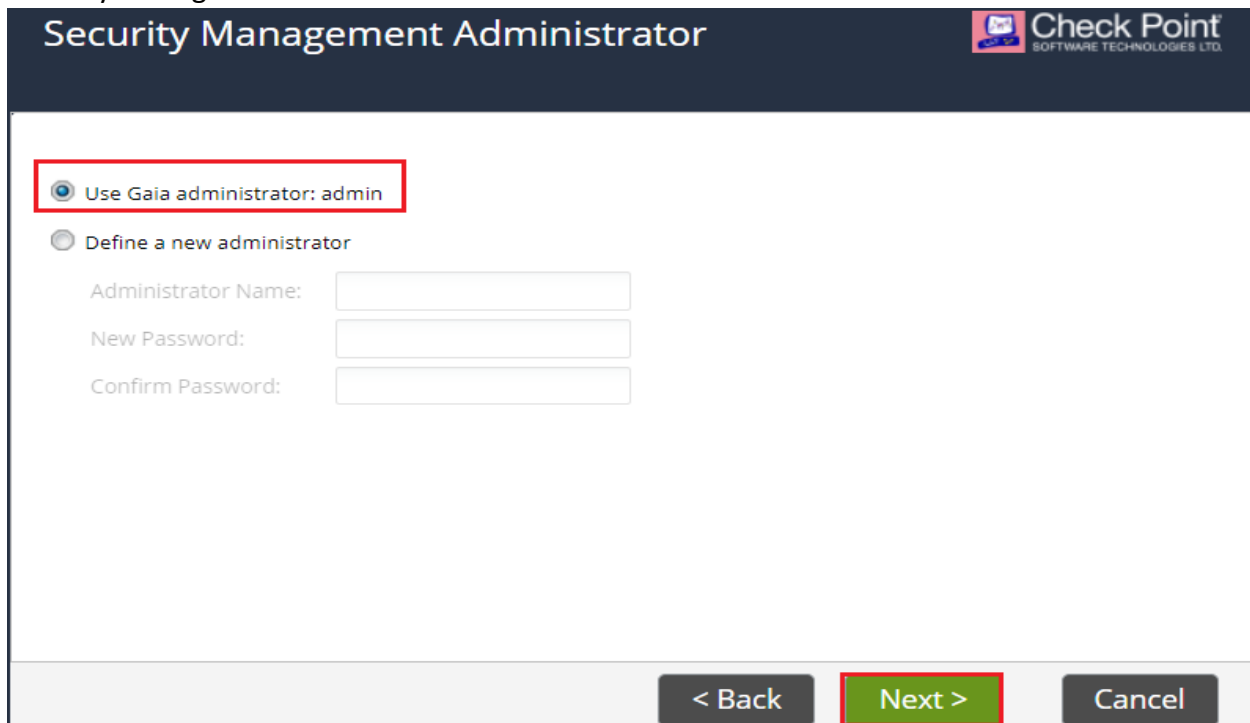
[< Back](#) [Next >](#) [Cancel](#)

As we doing Standalone deployment. Now on Product Wizard Select **Security Gateway** and **Security Management** check box to install both in same machine. Then click on **Next**.



The screenshot shows the 'Products' step of the Check Point Product Wizard. The 'Products' section has two checked checkboxes: 'Security Gateway' and 'Security Management', which are highlighted by a red rectangle. The 'Clustering' section has an unchecked checkbox for 'Unit is a part of a cluster, type:' with a dropdown menu set to 'ClusterXL'. Below it, 'Define Security Management as:' has a dropdown menu set to 'Primary'. At the bottom, there is a checked checkbox for 'Automatically download Blade Contracts, new software, and other important data (highly recommended)' and a link 'For more information click here'. The bottom navigation bar contains three buttons: '< Back', 'Next >' (highlighted with a red rectangle), and 'Cancel'.

Now on the Security Management Administrator Wizard, Put User name and password for your Security management. Then click on **Next**.



The screenshot shows the 'Security Management Administrator' step of the Check Point wizard. It has two radio button options: 'Use Gaia administrator: admin' (selected and highlighted with a red rectangle) and 'Define a new administrator'. Below the second option are three input fields: 'Administrator Name:', 'New Password:', and 'Confirm Password:'. The bottom navigation bar contains three buttons: '< Back', 'Next >' (highlighted with a red rectangle), and 'Cancel'.

Now on the Security Management GUI Clients wizard, now give GUI access control to Client from smart Dashboard, Give any, Specific Machine, Network or Range of IP address. In my case Select any IP Address radio button. Then Click on **Next**.

## Security Management GUI Clients



GUI clients can log into the Security Management from:

☒ Any IP Address

☐ This machine

IP address:

☐ Network

IP Address:

Subnet:

☐ Range of IPv4 addresses:

-

< Back **Next >** Cancel

## First Time Configuration Wizard Summary



Your device will be configured with the following products:

- Security Gateway
- Security Management: Primary Security Management

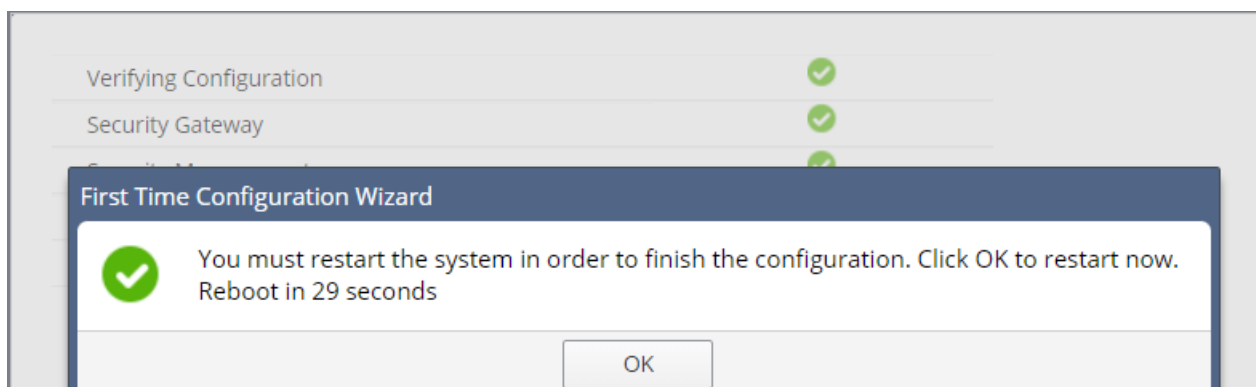
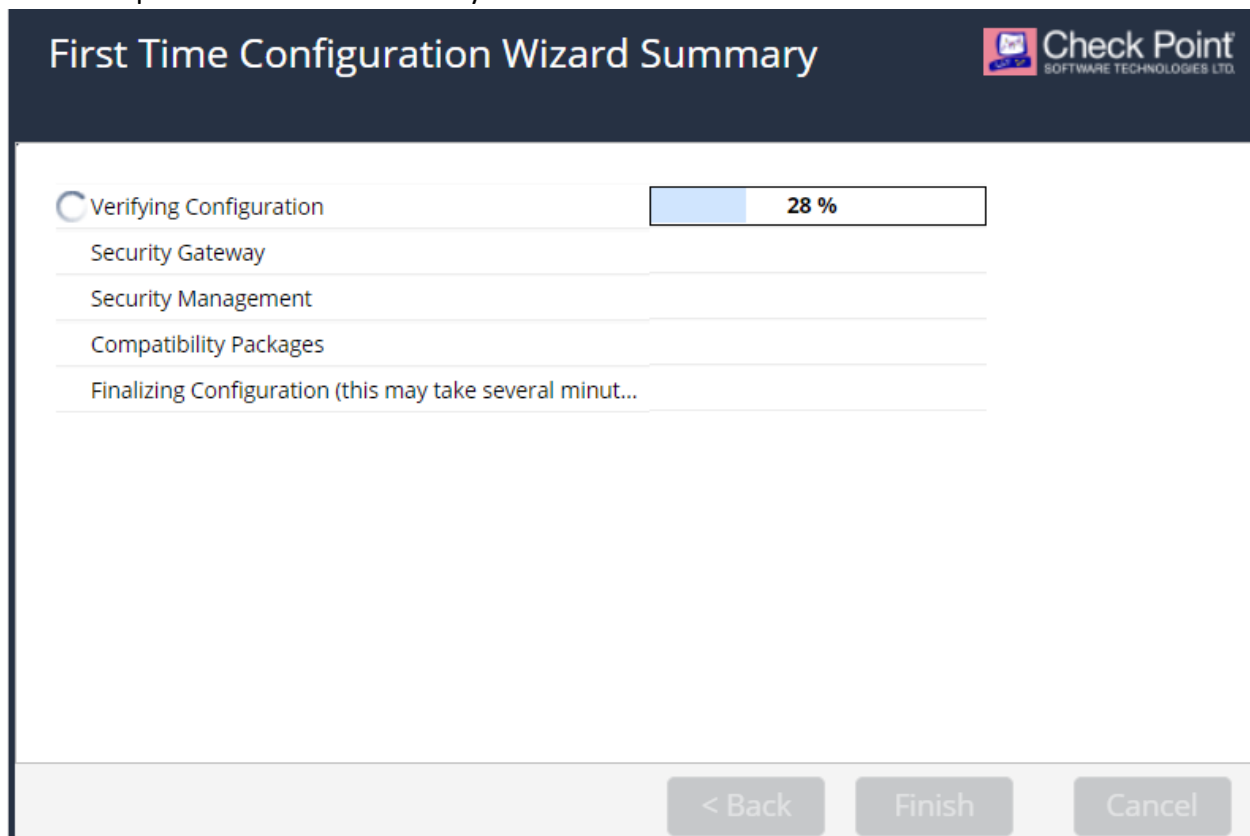
Improve product experience:

☒ Send data to Check Point | [more >](#)

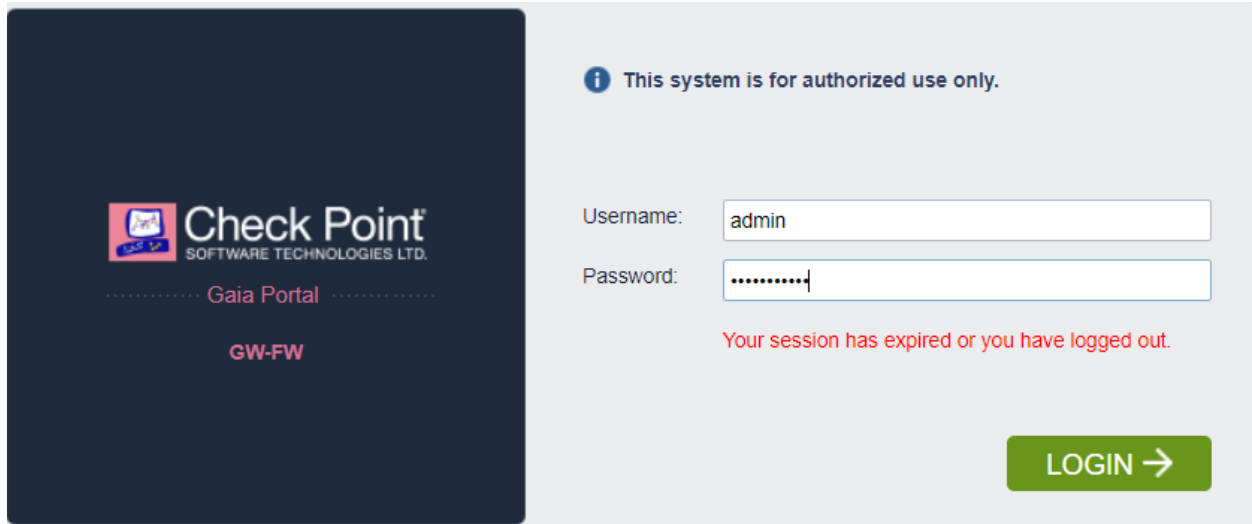
☐ Send crash data which might contain personal data to Check Point. | [more >](#)

< Back **Finish** Cancel

Click on Finish button. Then you will see installation process going on wait until completion.  
After complete it will ask to **reboot** your firewall then click on **Yes**.



Now again Access Checkpoint firewall from your browser with Management IP Address (<https://192.168.100.50>). Then put User name and password then Login.



The image shows the Checkpoint Gaia Portal login interface. On the left is a dark blue sidebar with the Check Point logo, 'Gaia Portal', and 'GW-FW'. The main area is light gray and contains a message 'This system is for authorized use only.', a login form with 'Username: admin' and 'Password: .....,', a red error message 'Your session has expired or you have logged out.', and a green 'LOGIN →' button.

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.  
Gaia Portal  
GW-FW

**This system is for authorized use only.**

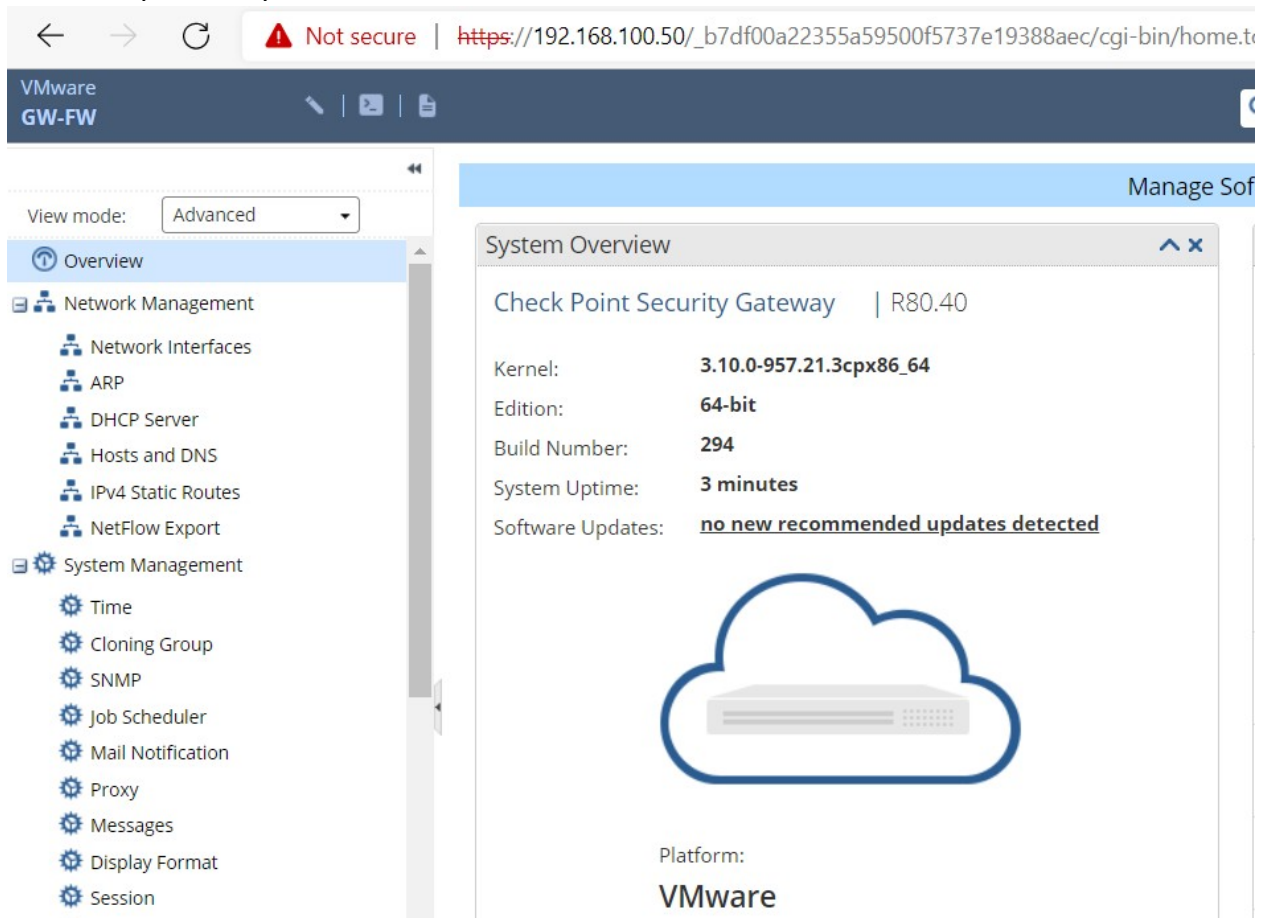
Username:

Password:

Your session has expired or you have logged out.

**LOGIN →**

Now we successfully Install and Configured Checkpoint Firewall Security Gateway. Now we are on Security Gateway Dashboard.



The image is a screenshot of a web browser displaying the Checkpoint Security Gateway dashboard. The browser's address bar shows a 'Not secure' warning and a long URL. The dashboard has a left sidebar with a tree view containing 'Overview' (selected), 'Network Management' (with sub-items like Network Interfaces, ARP, DHCP Server, etc.), and 'System Management' (with sub-items like Time, Cloning Group, etc.). The main content area is titled 'System Overview' and shows details for 'Check Point Security Gateway | R80.40', including Kernel, Edition, Build Number, System Uptime, and Software Updates. A graphic of a server in a cloud is shown, and the platform is identified as 'VMware'.

← → ↻ **Not secure** | [https://192.168.100.50/\\_b7df00a22355a59500f5737e19388aec/cgi-bin/home.t](https://192.168.100.50/_b7df00a22355a59500f5737e19388aec/cgi-bin/home.t)

VMware  
GW-FW

View mode: **Advanced**

**Overview**

- Network Management
  - Network Interfaces
  - ARP
  - DHCP Server
  - Hosts and DNS
  - IPv4 Static Routes
  - NetFlow Export
- System Management
  - Time
  - Cloning Group
  - SNMP
  - Job Scheduler
  - Mail Notification
  - Proxy
  - Messages
  - Display Format
  - Session

**System Overview**

Check Point Security Gateway | R80.40

Kernel: **3.10.0-957.21.3cpx86\_64**

Edition: **64-bit**

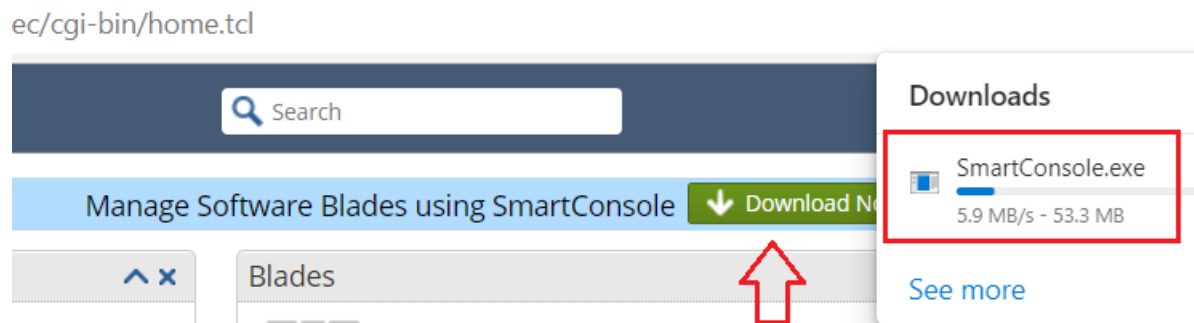
Build Number: **294**

System Uptime: **3 minutes**

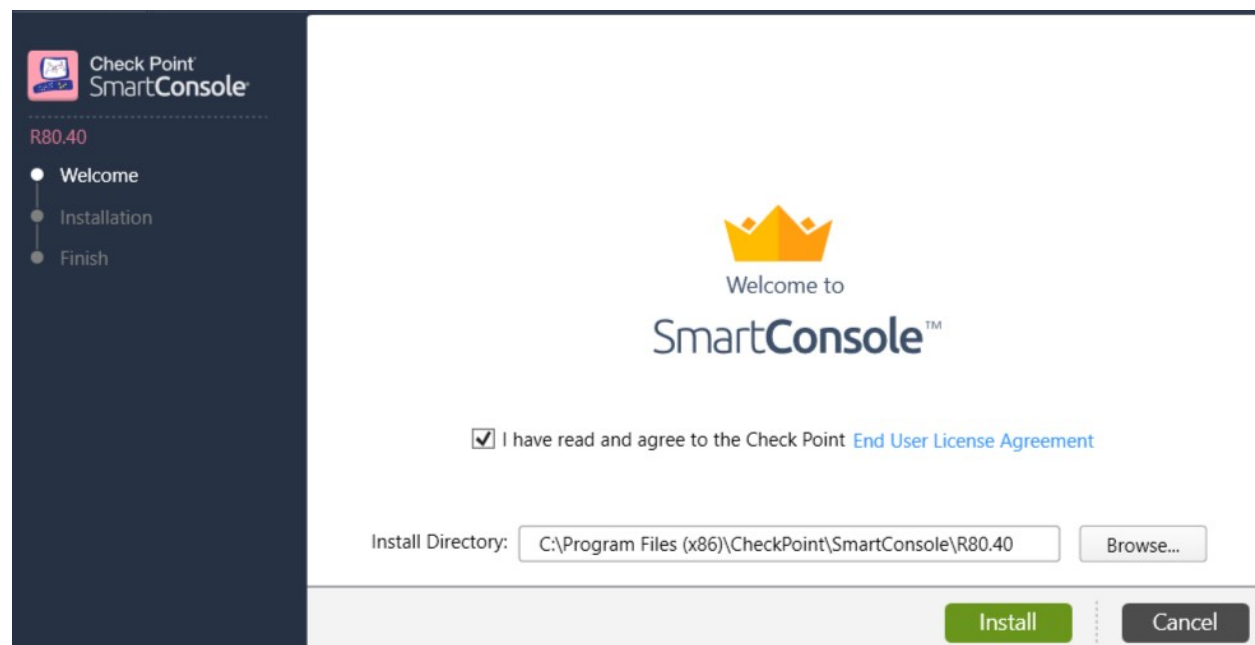
Software Updates: **no new recommended updates detected**

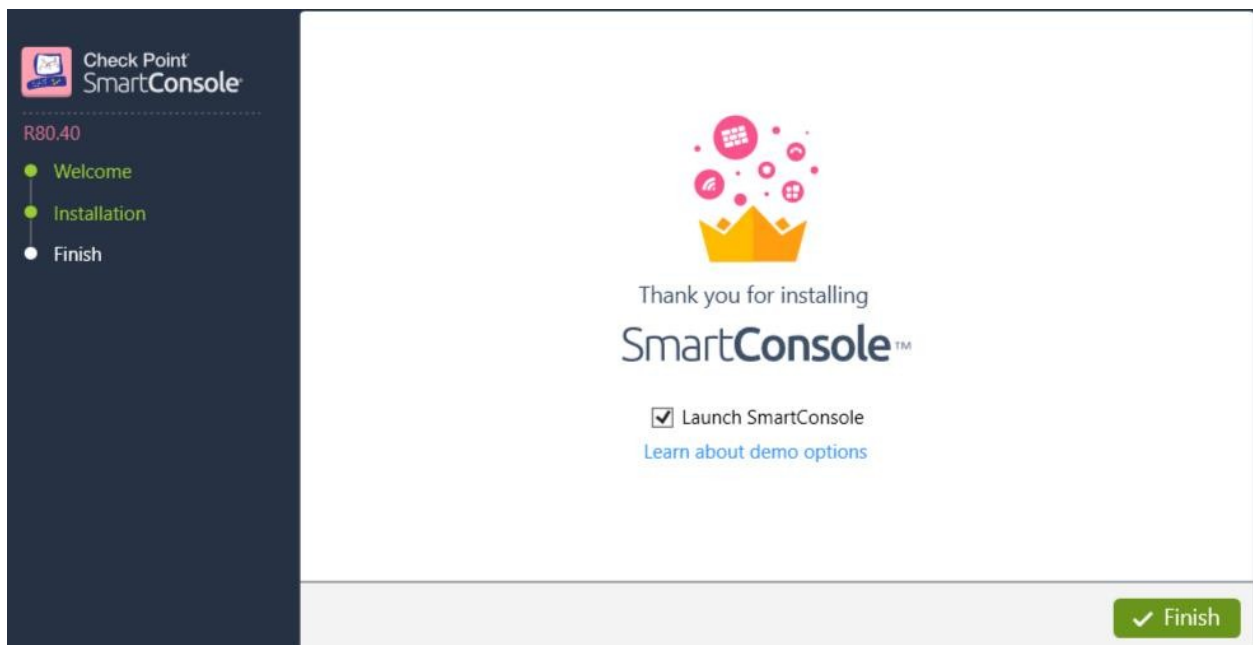
Platform: **VMware**

Now download the **Smart Console** software from the dashboard.



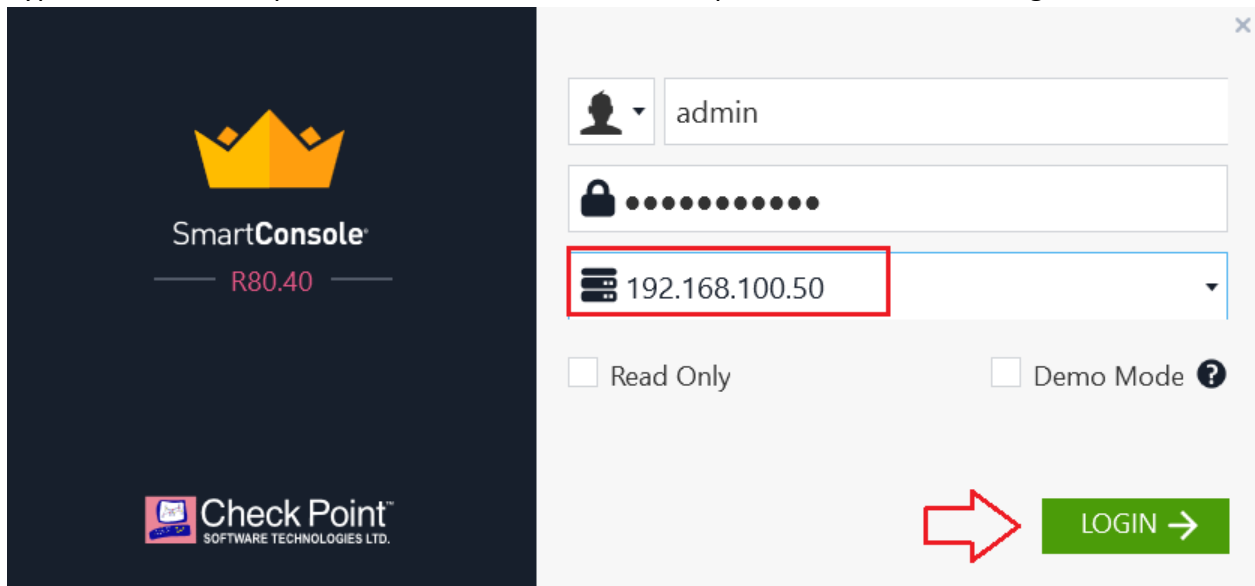
Install the Smart Console software on your PC.





Now you are able to manage your checkpoint GAIA firewall with Smart Dashboard.

Type the username, password and IP address of Checkpoint firewall click on Login.



The image shows the SmartConsole R80.40 login interface. On the left is a dark blue sidebar with the SmartConsole logo and Check Point Software Technologies Ltd. branding. The main area is light gray and contains a login form. The form has three input fields: a username field with 'admin', a password field with masked characters, and an IP address field with '192.168.100.50' highlighted by a red rectangle. Below the IP field are two checkboxes: 'Read Only' and 'Demo Mode'. A red arrow points to a green 'LOGIN' button with a right-pointing arrow.

SmartConsole<sup>®</sup>  
R80.40

Check Point<sup>™</sup>  
SOFTWARE TECHNOLOGIES LTD.

admin

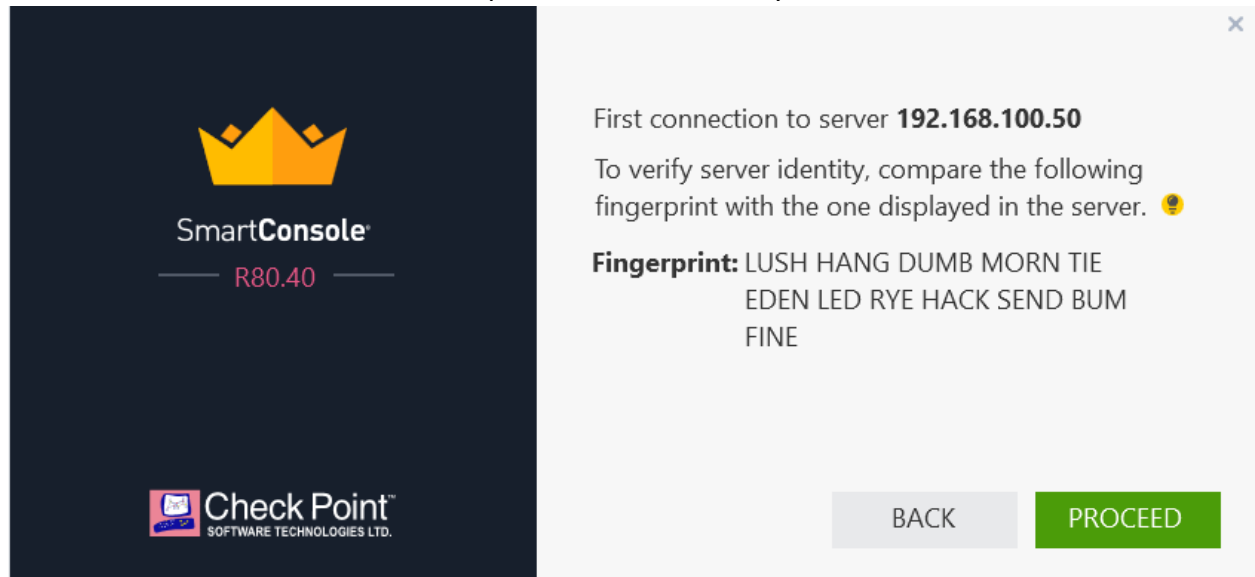
.....

192.168.100.50

☐ Read Only ☐ Demo Mode ?

LOGIN →

Click on Proceed to connect to Checkpoint Firewall Gateway.



The image shows the SmartConsole R80.40 fingerprint verification screen. The left sidebar is the same as the login screen. The main area is light gray and contains a message about the first connection to the server. The message says: 'First connection to server 192.168.100.50. To verify server identity, compare the following fingerprint with the one displayed in the server.' followed by a fingerprint string: 'LUSH HANG DUMB MORN TIE EDEN LED RYE HACK SEND BUM FINE'. At the bottom right are two buttons: 'BACK' and 'PROCEED'.

SmartConsole<sup>®</sup>  
R80.40

Check Point<sup>™</sup>  
SOFTWARE TECHNOLOGIES LTD.

First connection to server **192.168.100.50**

To verify server identity, compare the following fingerprint with the one displayed in the server. 🧐

**Fingerprint:** LUSH HANG DUMB MORN TIE  
EDEN LED RYE HACK SEND BUM  
FINE

BACK PROCEED

**GATEWAYS & SERVICES**

Discard | Session | Publish

Columns: General

| Status | Name  | IP             | Versi... | Active Blades | Hardware    | CPU Usa... | Recommended Updat... | Recommended Jumbo          |
|--------|-------|----------------|----------|---------------|-------------|------------|----------------------|----------------------------|
|        | GW-FW | 192.168.100.50 | R80.40   |               | Open server | 32%        | 6 updates available  | Check_Point_R80_40_JUMB... |

**Summary** | Tasks | Errors

**GW-FW**

IPv4 Address: **192.168.100.50**

OS: **Gaia**

Version: **R80.40**

License Status: Not Activated

Open server

Access Blades

- Firewall

Management Blades

- Network Policy Management
- Logging & Status