

Installing Security Management Server

Introduction

we will cover installation and initial configuration of a new Security Management Server.

Deployment Options

Security Management Server (SMS) can be deployed in two different options: Smart-1 Appliance or Open Server.

Let talk about both options in more detail.

1. Smart-1 Appliance

Check Point provides a wide range of Smart-1 appliances that are divided into two groups:

- Enterprise (Smart-1 405, 410, 225, 525)
- High End Enterprise (Smart-1 3050, 5050, 3150, 5150)



The main difference between two categories is about amount of Security Gateways such appliance can manage. The more firewalls to manage, the bigger the performance requirements for the management server appliance in CPU, RAM, and hard disk size.

2. Open Server

In case of the Open Server deployment, you install SMS on a dedicated physical server or as a virtual machine, with Gaia OS. If the physical server is your choice, check the [Hardware Compatibility List](#).

Deploying SMS as a virtual machine is also a popular option. SMS VM production deployment is supported on several ESX versions, Hyper-V and KVM. See [Hardware Compatibility List, tab "Virtual Machines"](#) for more details.

We are deploying SMS as a VM in our lab.

Installation Procedure

Smart-1 and Open Servers installation procedures lightly differ in details. Let's talk about appliance deployment in brief before covering the Open Server option.

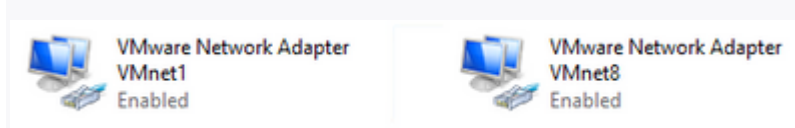
Smart-1 Deployment

By default, Smart-1 appliance comes preinstalled with at least one version of Check Point Gaia software. In most cases, all you need is to initialize it. However, if you want to re-image the appliance or install a software version different from the available factory defaults, look into [sk65205](#) for tools and details.

Deployng SMS as a VM

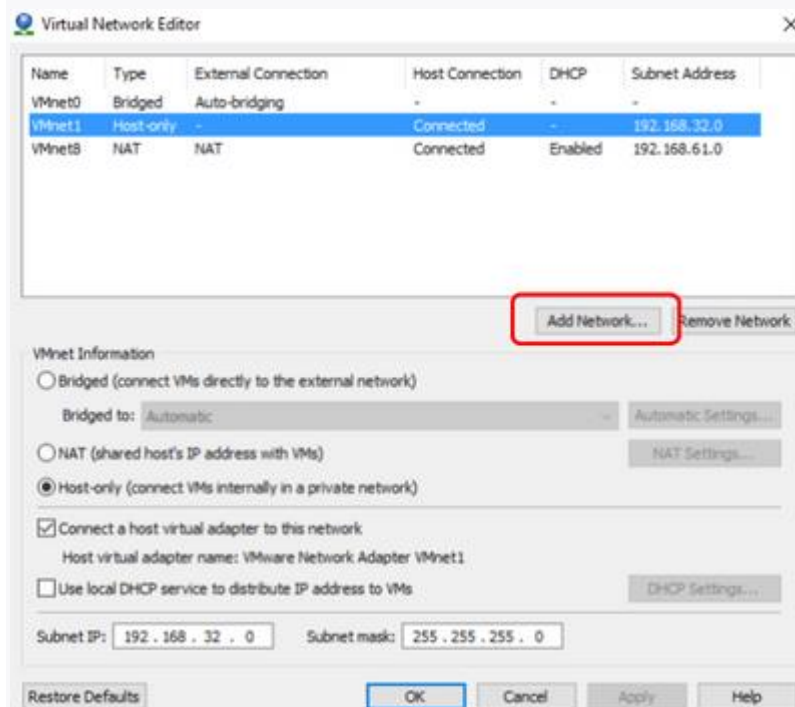
Our first lab starts here. To install a Security Management Server, we will be using a Windows based VMware Workstation.

By default, with VMware Workstation installed on your PC, you have two additional network adapters related to VMware Workstation networks: VMnet1 (Host-only) и VMnet8 (NAT).



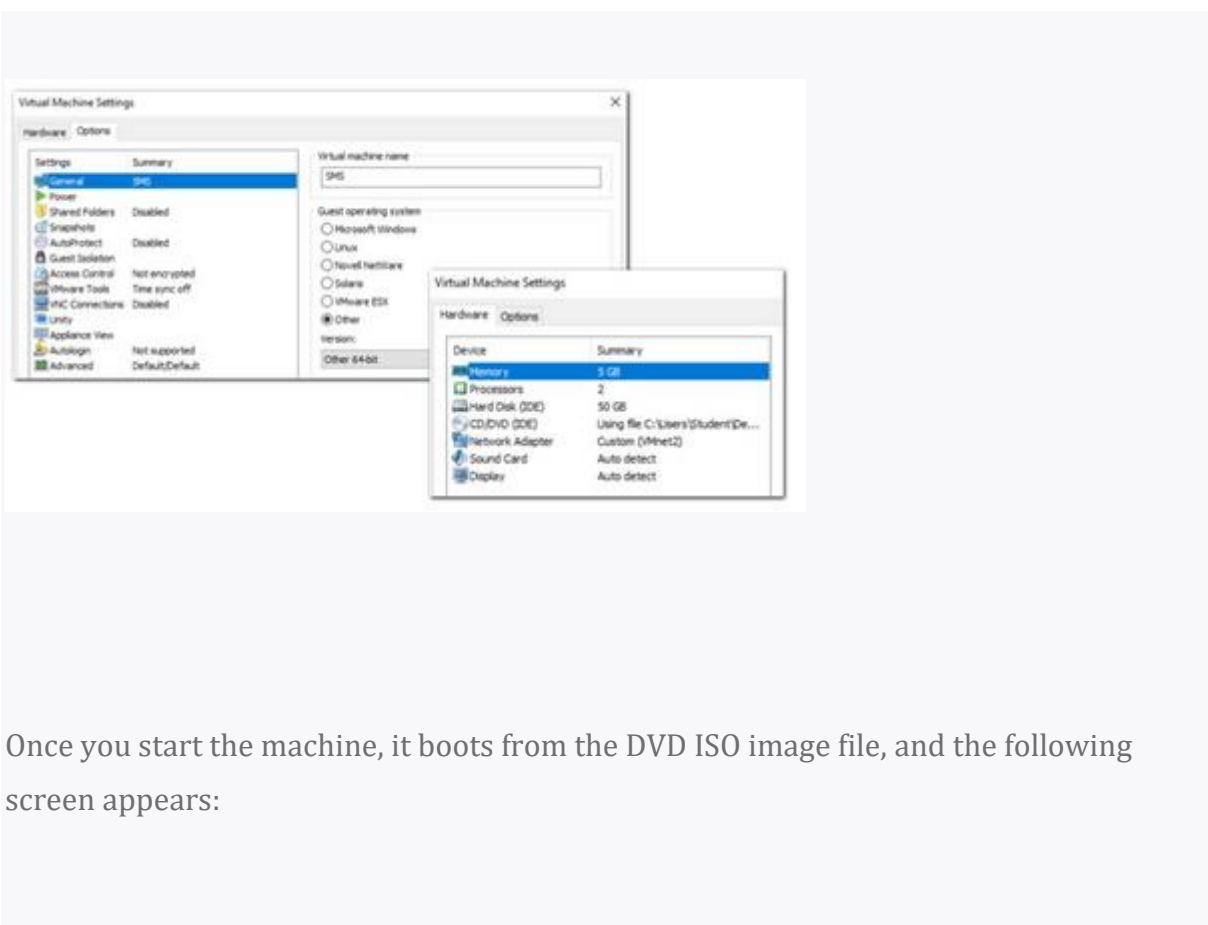
We need one more virtual network adapter: - VMnet2. To create it, in the VMware Workstation menu choose Edit -> Virtual Network Editor -> Add Network

After creating a new network, uncheck - "Use local DHCP service..." setting to disable DHCP on it.



Now we can create a new Virtual Machine with the following parameters:

- Virtual Machine Name - SMS
- Guest operating system - Other 64-bit
- RAM - 8GB [\[i\]](#)
- Processors - 2
- HDD - 50
- CD/DVD - Check_Point_R80.10_T462_Gaia.iso
- Network Adapter - VMnet2

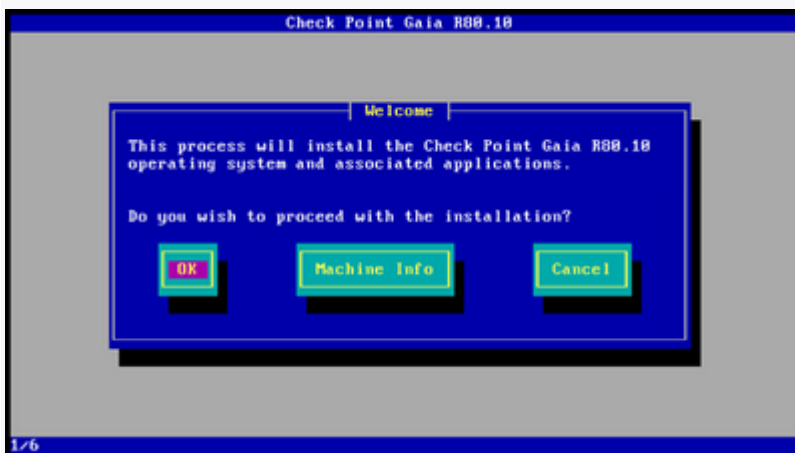


Once you start the machine, it boots from the DVD ISO image file, and the following screen appears:



Choose "Install Gaia on this system" to start the installation process. It includes six steps:

Proceed with the installation by pressing OK

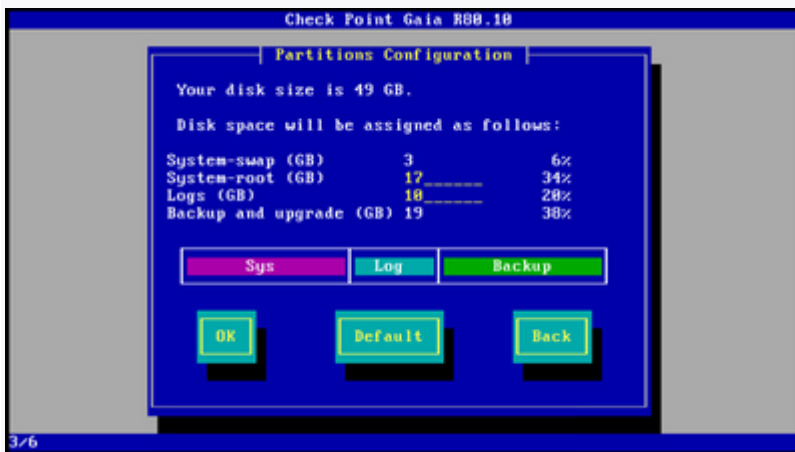


Choose the keyboard locale from the menu (we are using US) and press OK again

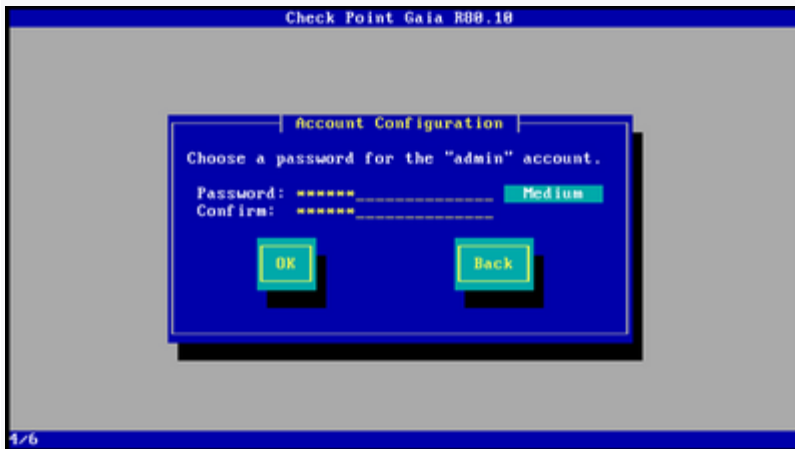


Partition the hard drive. In the real world when deploying an Open Server, it is usually safe to rely default Gaia partitioning. Yet, if require, you can change sizes for System-root and Logs partitions.

In production SMS deployment, always set up Logs as the biggest partition. For lab purposes only, we will set up System-root for 17GB, leaving only 10GB for the Logs.



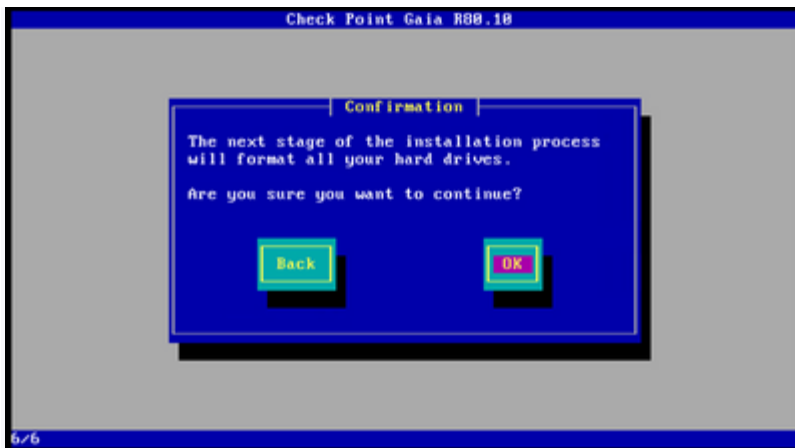
Set up the initial admin password. You can chose your own, but we are setting “vpn123” password at this step.



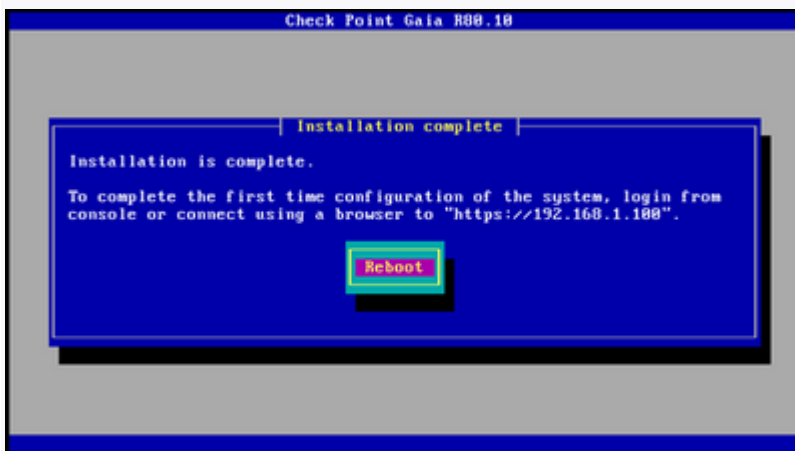
Set up IP address, network mask, and the default gateway.



Confirm the setup parameters and start installation by pressing OK.



At the end of installation procedure, you will see the note about first time configuration accessible via <https://192.168.1.100>. Press reboot and wait until the VM is fully up.

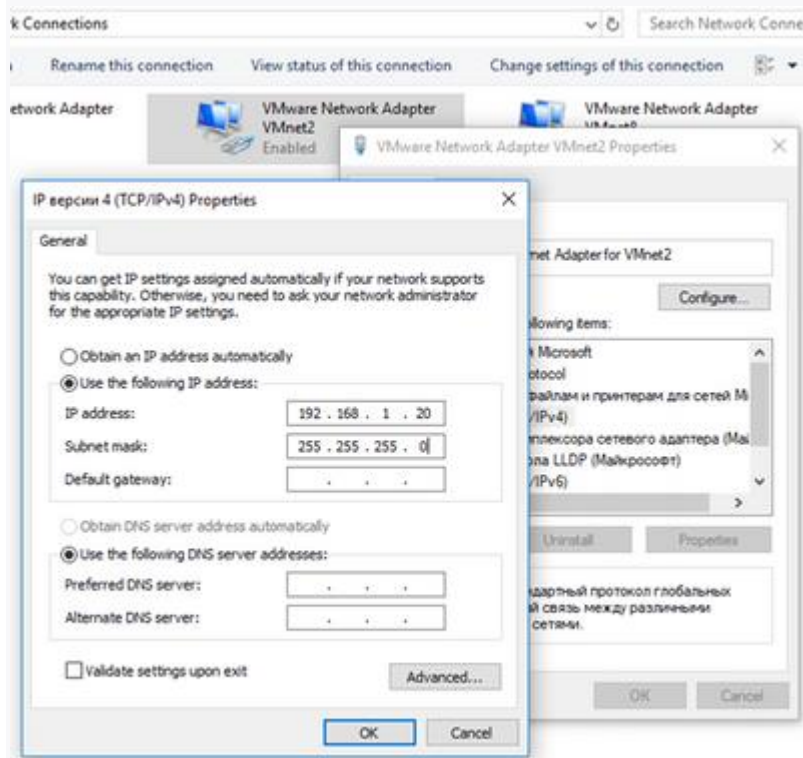


At this point, we have finished the installation. Let's run a First Time Wizard to complete configuration of our SMS.

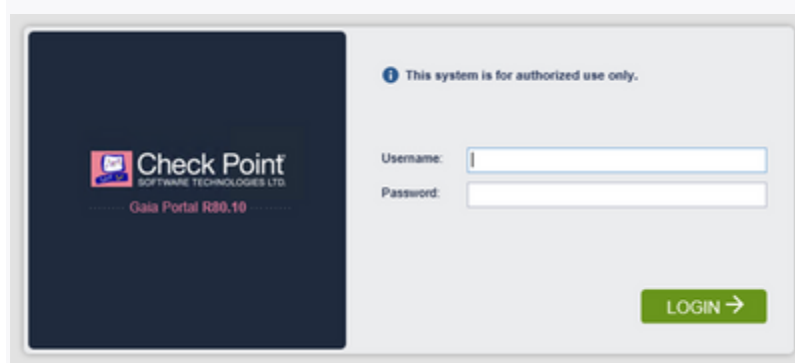
Initializing

Although, as mentioned above, installation / re-imaging of Smart-1 appliance and Open Server differ, First Time Wizard flow is identical in both cases.

To continue, we need to set up an IP address on virtualization host (your PC) VMnet2 adapter as 192.168.20 and network mask for class C (255.255.255.0).



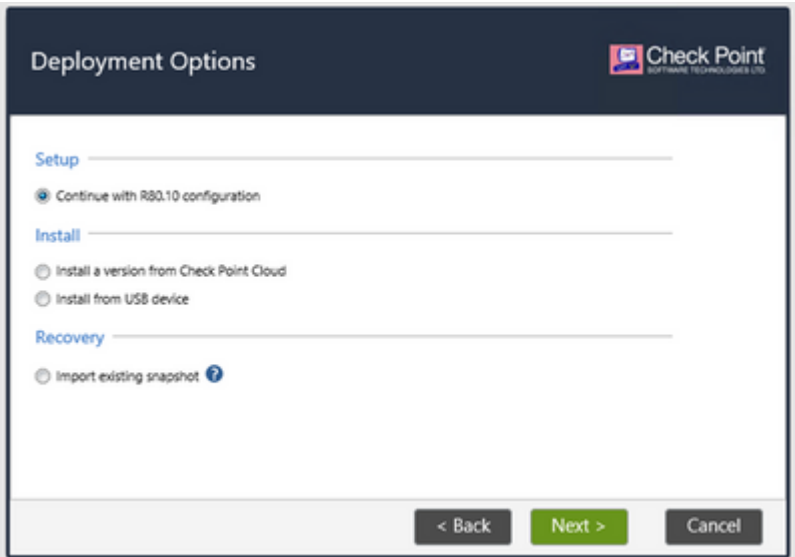
Once the IP address is set, you can connect with a browser to <https://192.168.1.100>. Most probably, you will see “Invalid Certificate” security warning. Default Gaia installation uses self-signed certificates, so you can ignore the message and connect. You will see an authentication prompt.



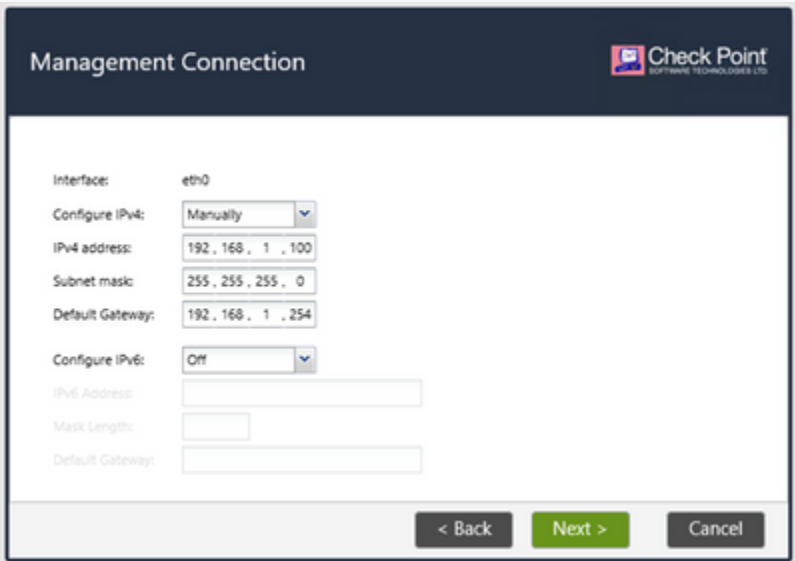
Type in username admin and the password you chose previously (vpn123). You will see the First Time Wizard Welcome screen. Press Next button:



Choose "Continue with R80.10 configuration" and press Next:



Do not change Management Connection settings and continue by pressing Next:



Set up a Host Name - SMS, Domain Name - testlab.local, and DNS server – 8.8.8.8, then press Next:

Device Information

Host Name: SMS

Domain Name: testlab.local

Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings

Use a Proxy server

Address:

Port: 8080

< Back Next > Cancel

You can leave default time and date settings:

Date and Time Settings

Set time manually:

Date: Wednesday, October 17, 2016

Time: 12 : 00

Time Zone: Moscow, Europe (GMT +3:00)

Use Network Time Protocol (NTP):

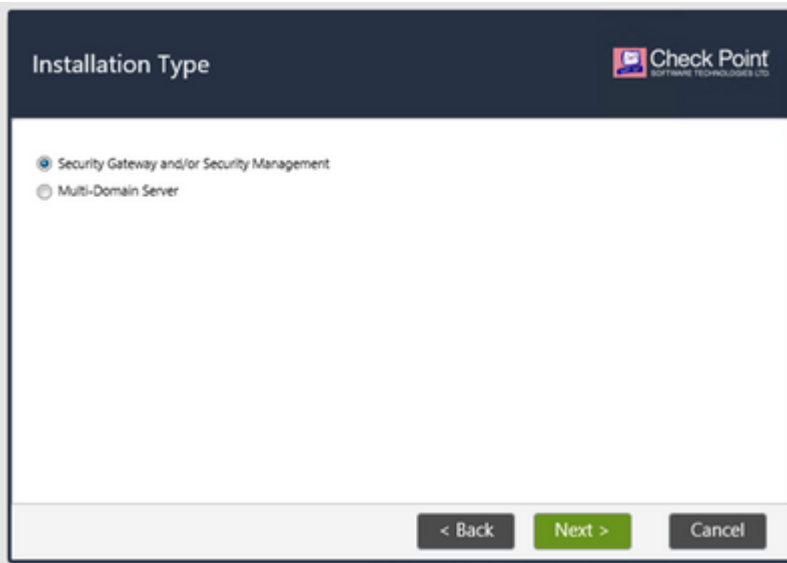
Primary NTP server: Example.com:12345 Version: 1.0

Secondary NTP server: Version: 1.0

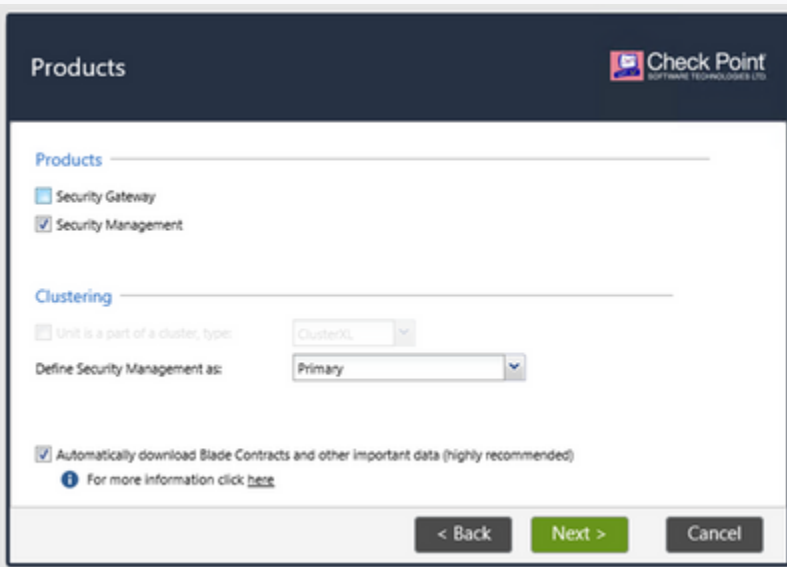
Time Zone: Moscow, Europe (GMT +3:00)

< Back Next > Cancel

On Installation Type screen chose the first option – Security Gateways and/or Security Management, then press Next:



On the Products screen chose only Security Management option and press Next:



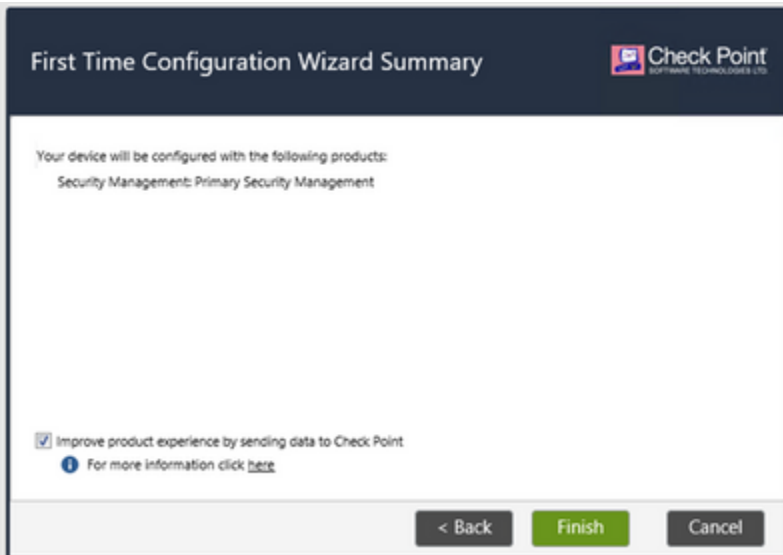
We will be using Gaia administrator settings for Security Management default Administrator account:

The screenshot shows the 'Security Management Administrator' configuration window. At the top, there is a dark blue header with the text 'Security Management Administrator' on the left and the 'Check Point SOFTWARE TECHNOLOGIES LTD' logo on the right. Below the header, there are two radio button options: 'Use Gaia administrator: admin' (which is selected) and 'Define a new administrator'. Under the 'Define a new administrator' option, there are three input fields: 'Administrator Name:', 'New Password:', and 'Confirm Password:'. At the bottom of the window, there are three buttons: '< Back', 'Next >' (highlighted in green), and 'Cancel'.

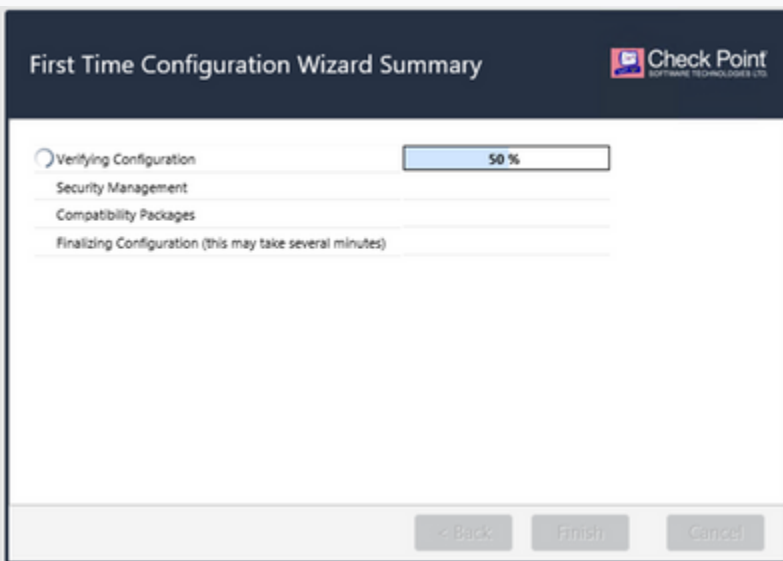
We will also leave the default “Any IP Address” settings for GUI clients list:

The screenshot shows the 'Security Management GUI Clients' configuration window. At the top, there is a dark blue header with the text 'Security Management GUI Clients' on the left and the 'Check Point SOFTWARE TECHNOLOGIES LTD' logo on the right. Below the header, the text 'GUI clients can log into the Security Management from:' is displayed. There are four radio button options: 'Any IP Address' (selected), 'This machine', 'Network', and 'Range of IPv4 addresses'. Under 'This machine', there is an 'IP address:' field with the value '192.168.1.50'. Under 'Network', there are 'IP Address:' and 'Subnet:' fields. Under 'Range of IPv4 addresses', there are two input fields separated by a hyphen. At the bottom of the window, there are three buttons: '< Back', 'Next >' (highlighted in green), and 'Cancel'.

Finally, confirm all the settings and press Finish to start configuration process.



The process takes 10 to 15 minutes:



Once it is finished, we get access to Gaia OS WebUI:

