Absolute Beginner's Guide to R80.x

Table of Contents

Absolute Beginner's Guide to R80.x 1

Introduction 2

Downloading GAIA R80.10 Installation Media and Documentation Package 3

VMware Workstation – Virtual Machine Creation 8

The VMWare Workstation GUI 8

VirtualBox – VM Creation 19

GAIA Installation 27

GAIA First Time Wizard 34

R80.10 SmartConsole Installation 43

R80.10 Hands-on Demo 46

Launching SmartConsole 46

Navigate the Four Main Tabs 51

Create a Security Policy Package 54

Create a New Rule 59

Create a Host Object and add it to a Rule 60

Search for Services and add them to a Rule 63

Sessions, changes, and Publishing 64

Publish Changes to the Security Policy 65

Install the Security Policy 66

Add Section Titles to the Policy 68

Revisions and Sessions 70

Looking at Logs 71

Introduction

This document is intended for people who wish to get some hands-on experience with Check Point R80.x even if they have never touched it before. We will start by downloading the GAIA ISO and creating a Virtual Machine using either VMware Workstation or VirtualBox on your PC. Use your Windows PC as the host for the Virtual Machine and as the client for running SmartConsole.

Note: This lab has a Check Point device with a single interface. There is no “passing of traffic” through the security gateway in this lab. This is intended to keep it simple. The following exercises are simply a way to get hands-on experience with the basics of R80 (ISO installation, SmartConsole basics, object creation, rule creation, etc). You will see some traffic & logs based on the traffic between your host computer and the interface on the Check Point virtual machine. This is enough to get the basics.

You can share this document with colleagues and friends, who has never installed GAIA before, and they should be able to follow these instructions to get started on their path to Check Point greatness.

Some knowledge of Windows networking and software installation is assumed. While I have included the steps for installing SmartConsole, it is up to the reader to provide a copy of VMware Workstation or Oracle’s VirtualBox software. VirtualBox is a free download, and is a great alternative to expensive commercial software. *Be sure to check with your IT Department before you install any software on a computer that you do not own!*

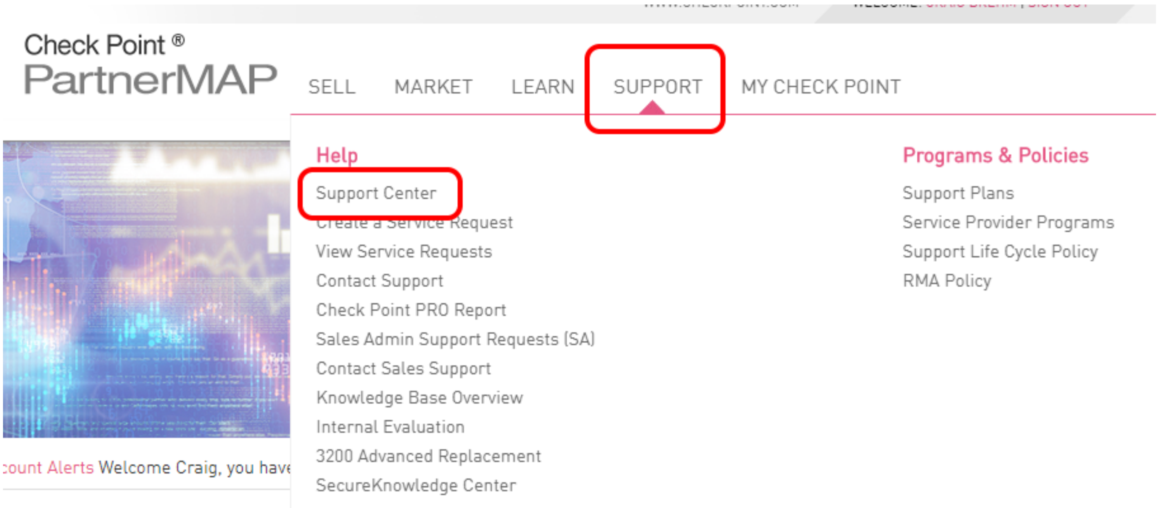
This is a very basic exercise that will lead you step-by-step through the process of locating and downloading the GAIA operating system, creating a Virtual Machine, completing the GAIA installation, and configuring a Standalone system you can use to get your introduction to R80.10[1].

[1] **Editor Note**: This guide is originally written for R80.10 version. However, it is also applicable to any newer version. At the moment of making this note, the latest Check Point GA version is R80.30. You can download R80.30 installation media instead of R80.10, and continue with the lab flow without any issue.

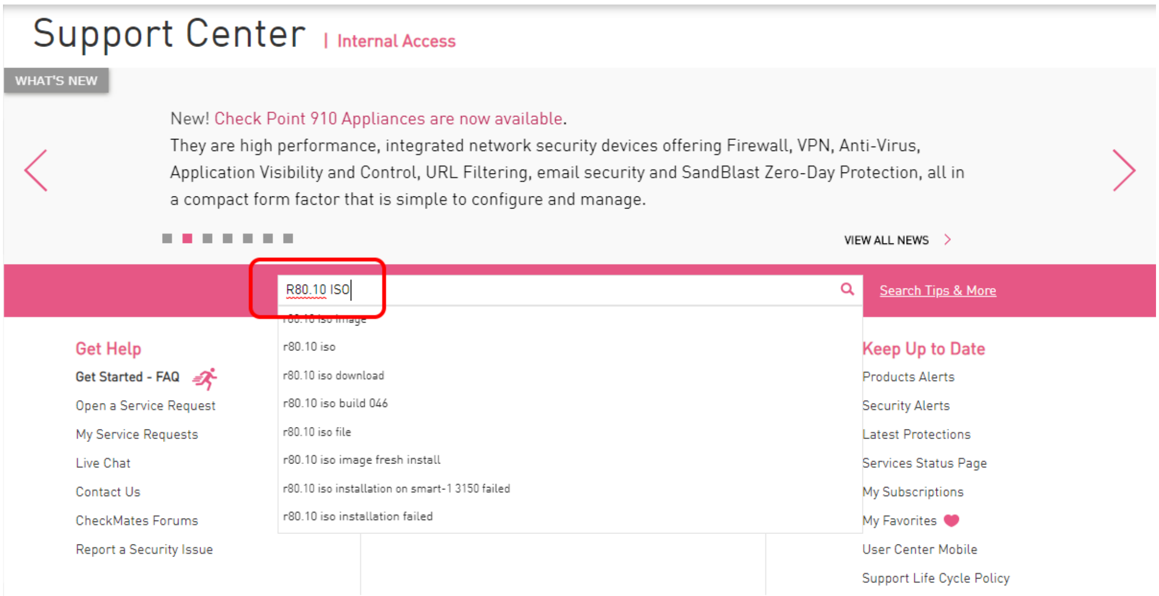
Downloading GAIA R80.10 Installation Media and Documentation Package

Before you begin, you will need a copy of the latest R80.x Installation Media (aka the latest take of the Check Point GAIA "Fresh Install" ISO). Point your web browser of choice to Check Point's PartnerMAP (also known as UserCenter.CheckPoint.com). You must have a User Center account with the proper permissions to download software from Support Center. Talk to your Check Point Partner or Account Team if you don't already have a User Center account.

Hover your mouse over the **SUPPORT** menu and select **Support Center** in the "Help" section. Your browser will load SupportCenter.CheckPoint.com. In the search bar, type in "R80.10 ISO" and hit ENTER.



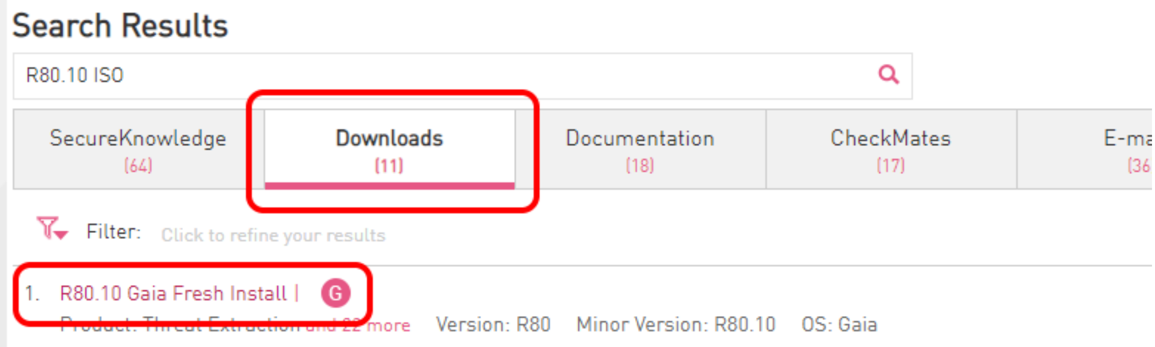
In the search bar, type in "R80.10 ISO" and hit ENTER (or click on the Magnifying glass).



New! Check Point 910 Appliances are now available.
They are high performance, integrated network security devices offering Firewall, VPN, Anti-Virus, Application Visibility and Control, URL Filtering, email security and SandBlast Zero-Day Protection, all in a compact form factor that is simple to configure and manage.

You will see a page of search results.

Click on the **Downloads** tab to see the list of available software downloads. Look for the **R80.10 Gaia Fresh Install** link, and click it.



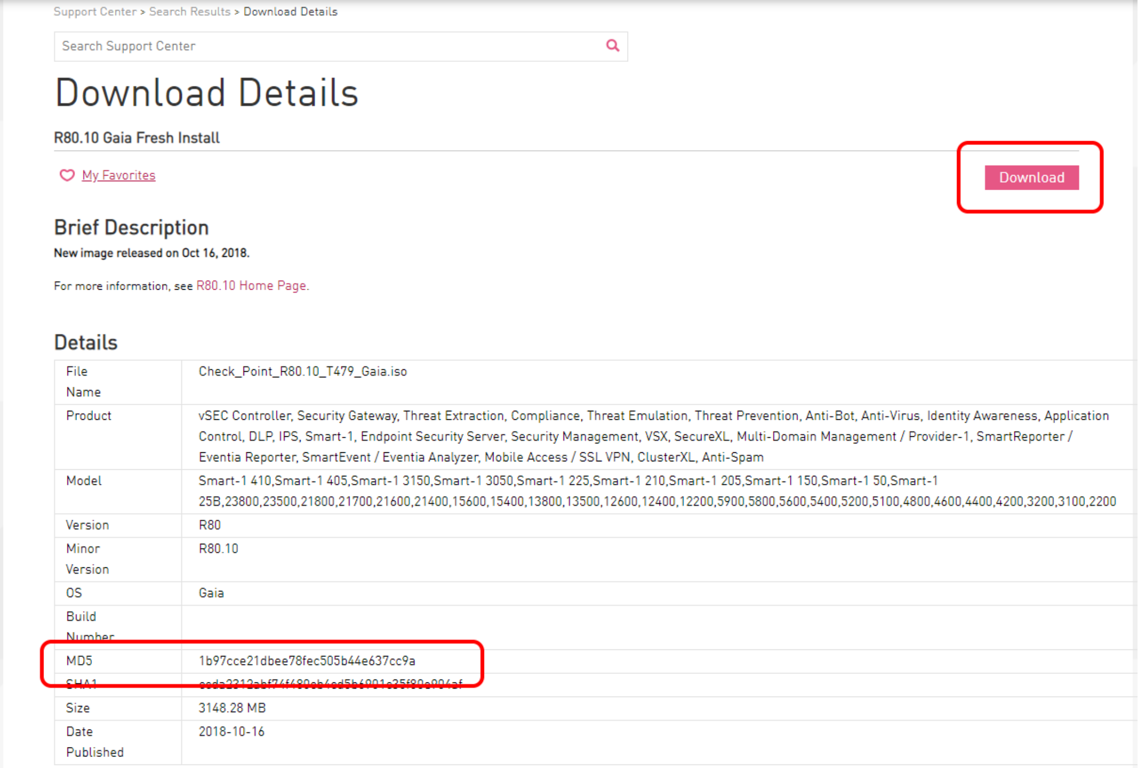
Search Results

R80.10 ISO

Filter: Click to refine your results

1. R80.10 Gaia Fresh Install | G
Product: Threat Extraction and 22 more Version: R80 Minor Version: R80.10 OS: Gaia

Click on the pink **Download** button to start the download.



Support Center > Search Results > Download Details

Search Support Center

Download Details

R80.10 Gaia Fresh Install

Brief Description

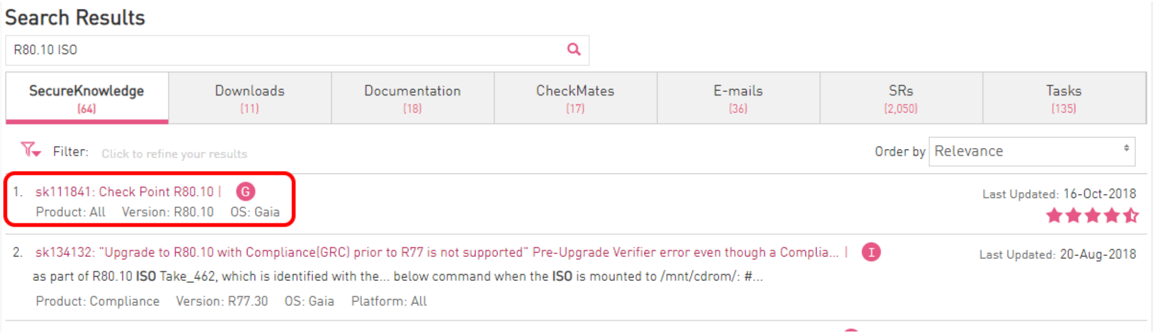
New image released on Oct 16, 2018.

For more information, see R80.10 Home Page.

Details

File Name	Check_Point_R80.10_T479_Gaia.iso
Product	vSEC Controller, Security Gateway, Threat Extraction, Compliance, Threat Emulation, Threat Prevention, Anti-Bot, Anti-Virus, Identity Awareness, Application Control, DLP, IPS, Smart-1, Endpoint Security Server, Security Management, VSX, SecureXL, Multi-Domain Management / Provider-1, SmartReporter / Eventia Reporter, SmartEvent / Eventia Analyzer, Mobile Access / SSL VPN, ClusterXL, Anti-Spam
Model	Smart-1 410,Smart-1 405,Smart-1 3150,Smart-1 3050,Smart-1 225,Smart-1 210,Smart-1 205,Smart-1 150,Smart-1 50,Smart-1 25B,23800,23500,21800,21700,21600,21400,15600,15400,13800,13500,12600,12400,12200,5900,5800,5600,5400,5200,5100,4800,4600,4400,4200,3200,3100,2200
Version	R80
Minor Version	R80.10
OS	Gaia
Build Number	
MD5	1b97cce21dbee78fec505b44e637cc9a
SHA1	[illegible]
Size	3148.28 MB
Date Published	2018-10-16

For the Documentation package, SmartConsole download, and other information, let’s look at the R80.10 Gaia Product page. Click on the **SecureKnowledge** tab. Look for the **R80.10 Gaia** link, and click it.



Search Results

R80.10 ISO

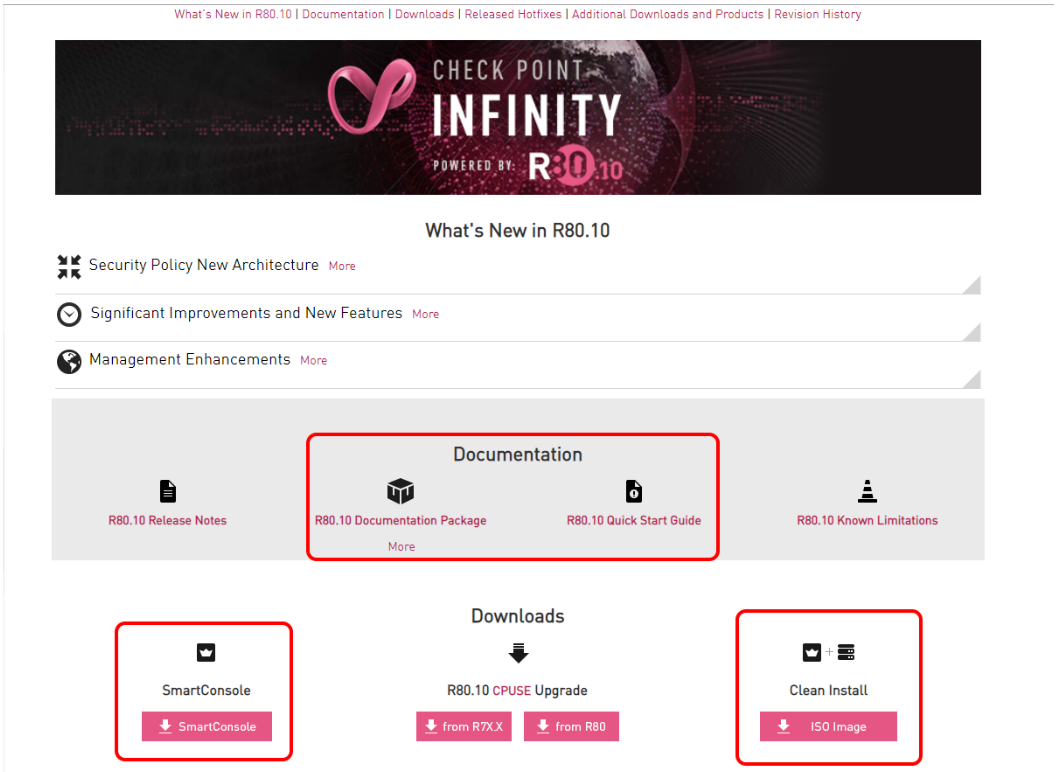
SecureKnowledge	Downloads	Documentation	CheckMates	E-mails	SRs	Tasks
(64)	(11)	(18)	(17)	(36)	(2,050)	(135)

Filter: Click to refine your results   Order by Relevance

1. sk111841: Check Point R80.10 | G   Last Updated: 16-Oct-2018
   Product: All Version: R80.10 OS: Gaia

2. sk134132: "Upgrade to R80.10 with Compliance(GRC) prior to R77 is not supported" Pre-Upgrade Verifier error even though a Complia... | I   Last Updated: 20-Aug-2018
   as part of R80.10 **ISO** Take_462, which is identified with the... below command when the **ISO** is mounted to /mnt/cdrom/: #...
   Product: Compliance Version: R77.30 OS: Gaia Platform: All

You will see many different links on the R80.10 page. You can download documentation, installation media, the SmartConsole installation package, and other product information. The primary links for this guide are highlighted below. The GAIA Clean Install ISO is in the lower right. Documentation is in the middle (go ahead and grab it for reference). SmartConsole is in the lower left. Click the SmartConsole link to go to the download page.



What's New in R80.10 | Documentation | Downloads | Released Hotfixes | Additional Downloads and Products | Revision History

What's New in R80.10

Security Policy New Architecture More

Significant Improvements and New Features More

Management Enhancements More

Documentation

R80.10 Release Notes

R80.10 Documentation Package More

R80.10 Quick Start Guide

R80.10 Known Limitations

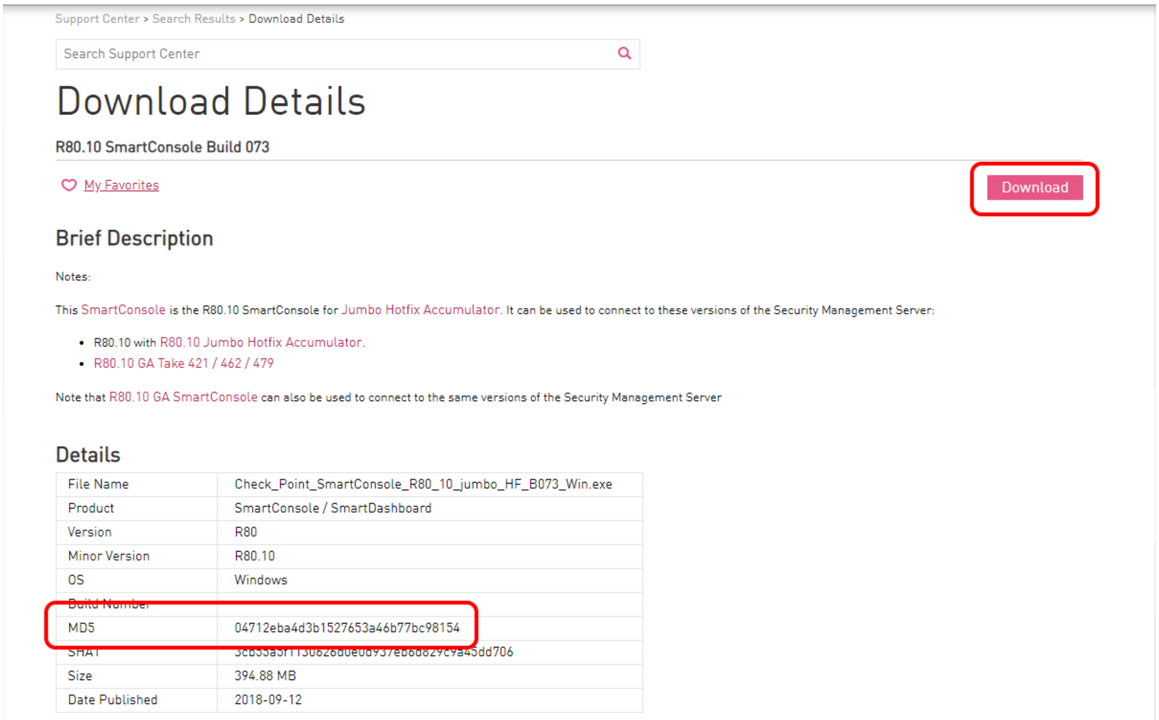
Downloads

SmartConsole

R80.10 CPUSE Upgrade

Clean Install

Click on the pink **Download** button to start the download. Take note of the md5sum & SHA1 sum. You can verify the ISO after the download completes.



Support Center > Search Results > Download Details

Search Support Center

Download Details

R80.10 SmartConsole Build 073

Brief Description

Notes:

This SmartConsole is the R80.10 SmartConsole for Jumbo Hotfix Accumulator. It can be used to connect to these versions of the Security Management Server:

- R80.10 with R80.10 Jumbo Hotfix Accumulator.
- R80.10 GA Take 421 / 462 / 479

Note that R80.10 GA SmartConsole can also be used to connect to the same versions of the Security Management Server

Details

File Name	Check_Point_SmartConsole_R80_10_jumbo_HF_B073_Win.exe
Product	SmartConsole / SmartDashboard
Version	R80
Minor Version	R80.10
OS	Windows
Build Number	
MD5	04712eba4d3b1527653a46b77bc98154
SHA1	3cb55a5f1130626d0e0d937eb6d829c9a45dd706
Size	394.88 MB
Date Published	2018-09-12

It may take a few minutes for the ISO to download, depending on your internet connection speed. After the download completes, you are ready to install Check Point's Gaia operating system. But first, you will need to start by creating a Virtual Machine. Let's walk through two very common, but different options, VMware Workstation and Oracle VirtualBox.

I do not recommend using both methods, as running them simultaneously on the same host computer could cause serious resource conflicts. If you have access to VMware, and that is what you use for your virtualization, go that route. If you do not have VMware, VirtualBox is a good alternative choice (especially if you're on a tight budget!). VirtualBox is also available for Mac OS X and Linux. If you decide to host the VMs on a Mac or Linux host, keep in mind you will still need to have a Windows computer for SmartConsole (you're on your own if you want to install Windows in a VM as it is outside of the scope of this guide, but it's not difficult).

We are not going to walk through the installation of VMware Workstation/Oracle VirtualBox in this document. If you require that much hand-holding, you might as well reconsider if you wish to continue with this exercise…

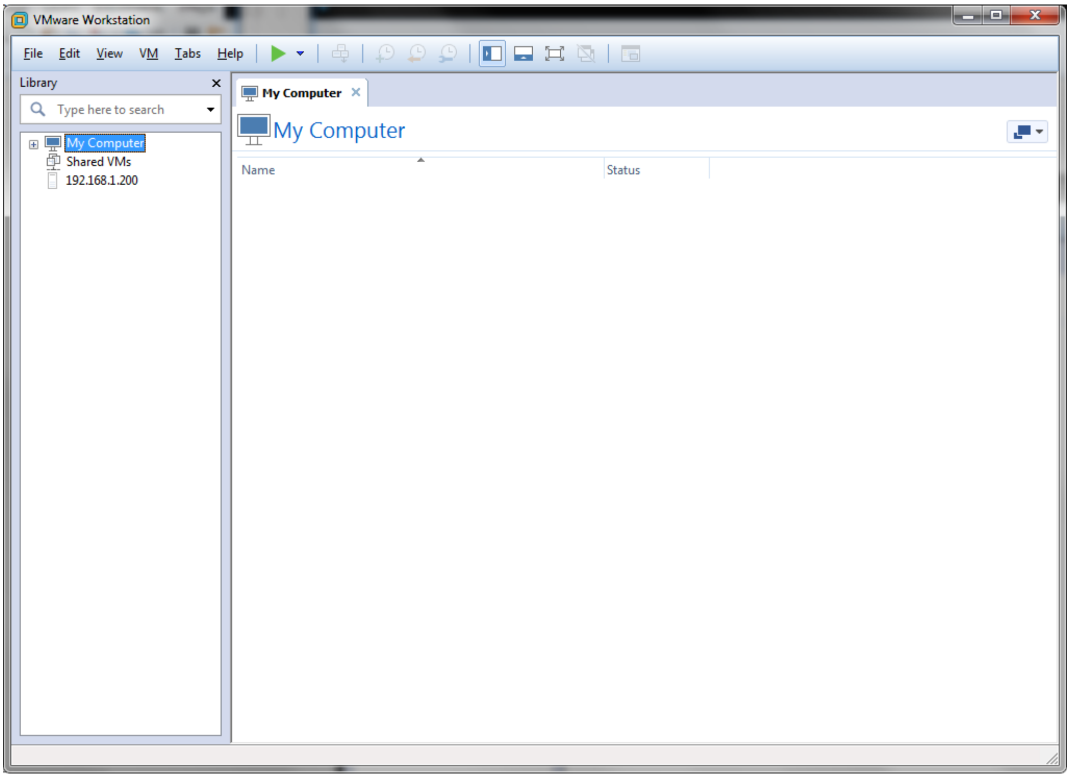
If you have never created Virtual Machines before, the steps are included in the next two sections. When creating a VM, you have to choose the resources that will be available to the "guest" operating system (aka GAIA). I have detailed the number of CPU cores, RAM, hard drive, etc. This is enough for a basic standalone installation. In the real world, I would recommend a much more powerful pool of resources. This is just enough to get a demo environment for you to play with.

You may notice some slowdown of your host computer, do not be alarmed. When you give resources to a second operating system, this is expected. If you “pause” or “power off” the guest VM, your computer will have those resources restored.

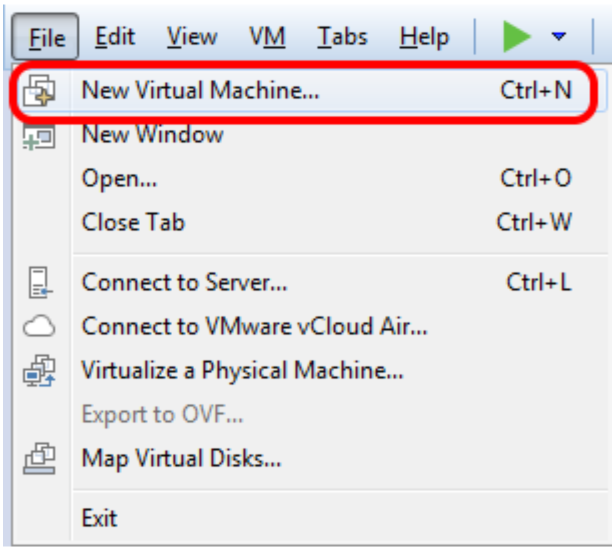
VMware Workstation – Virtual Machine Creation

NOTE: The following screenshots are from VMware Workstation 12 Pro
The steps for Workstation versions 8-10-12-etc should be very similar.

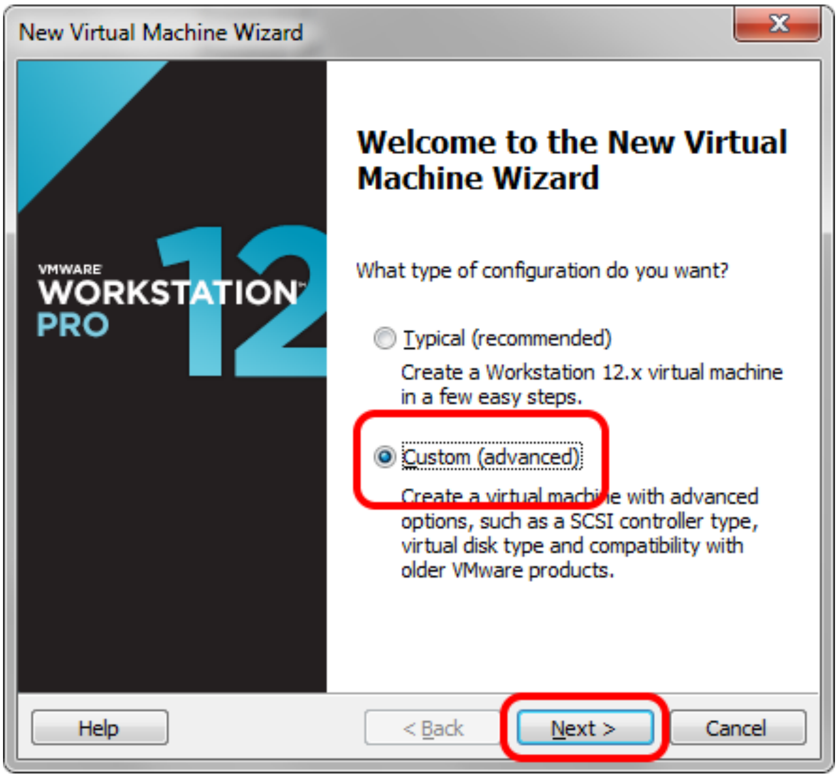
The VMWare Workstation GUI



In the File menu, choose **New Virtual Machine**.


File Edit View VM Tabs Help
New Virtual Machine... Ctrl+N
New Window
Open... Ctrl+O
Close Tab Ctrl+W
Connect to Server... Ctrl+L
Connect to VMware vCloud Air...
Virtualize a Physical Machine...
Export to OVF...
Map Virtual Disks...
Exit

The **New Virtual Machine Wizard** will walk through the process to create a VM for running the Gaia OS. Choose “Custom” and click **NEXT**.



New Virtual Machine Wizard

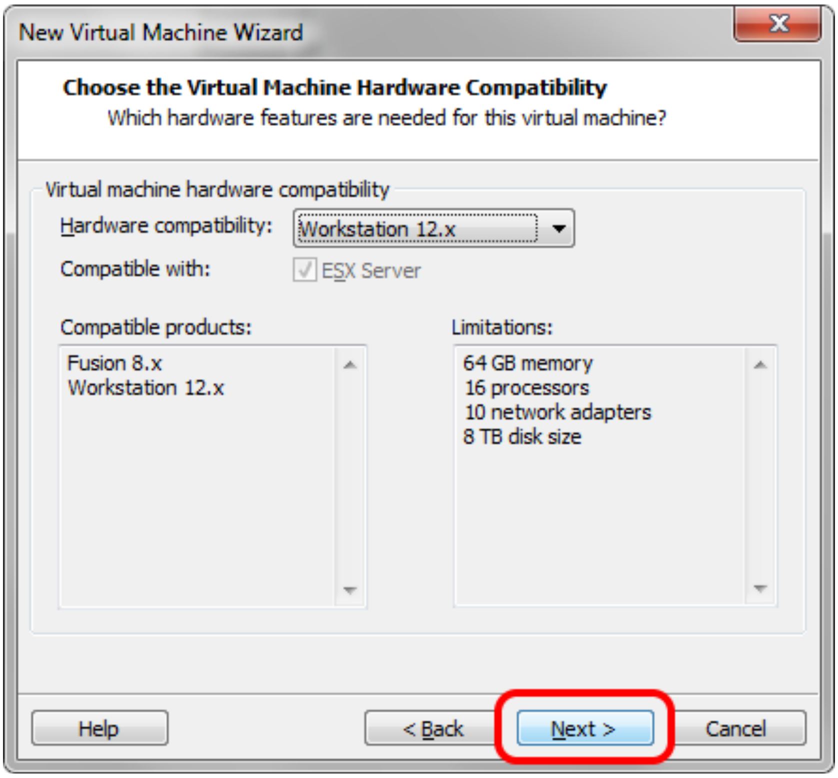
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

○ Typical (recommended)
Create a Workstation 12.x virtual machine in a few easy steps.

● Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Leave the default options on the Hardware Compatibility step, and click **NEXT** to continue.



New Virtual Machine Wizard

Choose the Virtual Machine Hardware Compatibility
Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

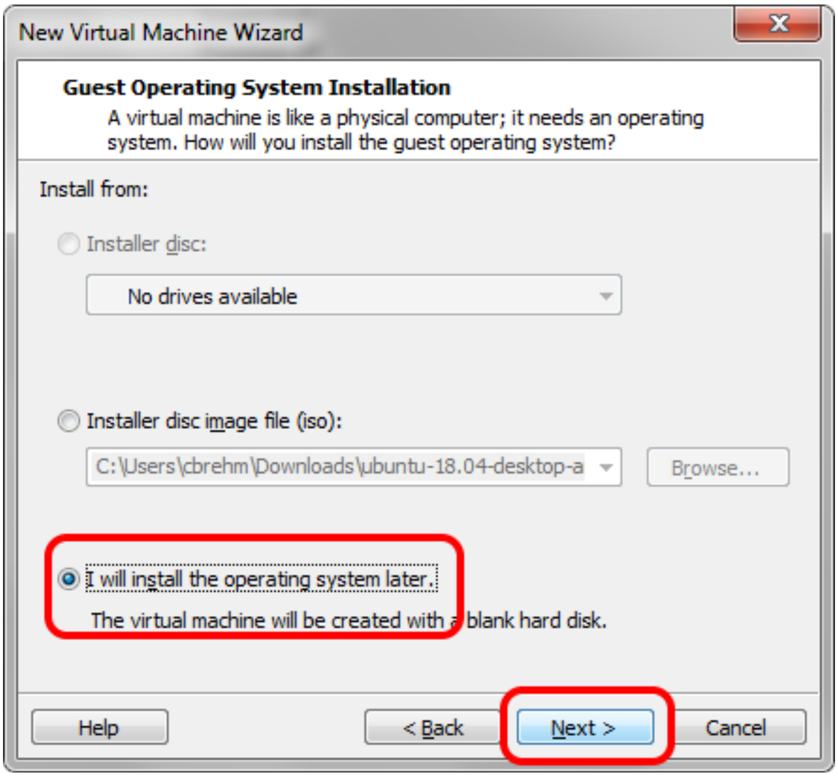
Hardware compatibility: Workstation 12.x

Compatible with: ☑ ESX Server

Compatible products:
Fusion 8.x
Workstation 12.x

Limitations:
64 GB memory
16 processors
10 network adapters
8 TB disk size

Choose “I will install the operating system later” and click **NEXT**.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

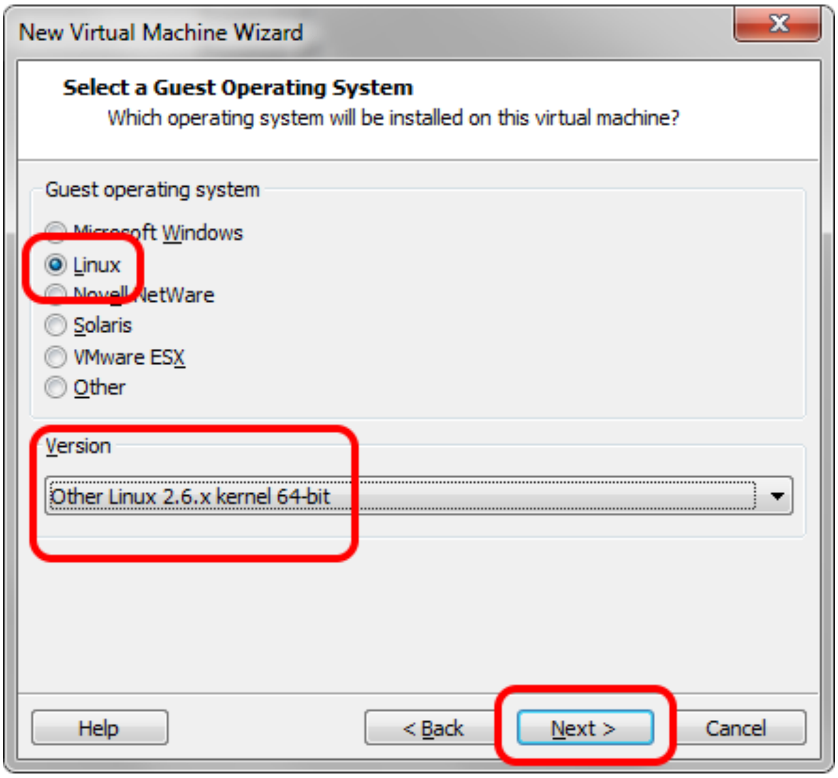
○ Installer disc image file (iso):

C:\Users\cbrehm\Downloads\ubuntu-18.04-desktop-a

● I will install the operating system later.

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

Choose “Linux”. Choose “Other Linux 2.6.x kernel 64-bit” from the Version drop-down list. Click **NEXT**.



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

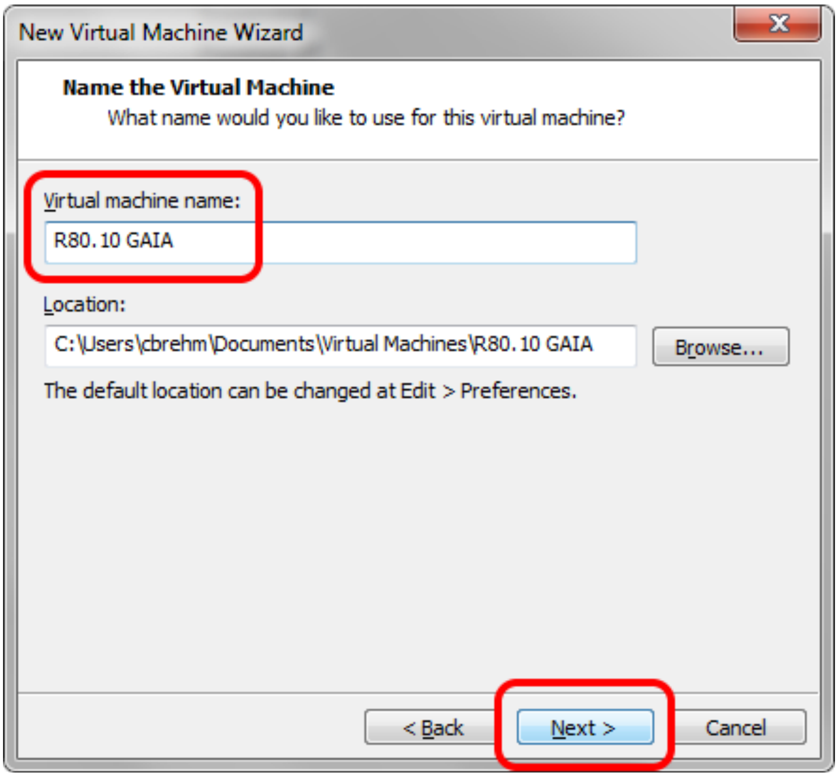
Guest operating system

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Solaris
○ VMware ESX
○ Other

Version

Other Linux 2.6.x kernel 64-bit

Name your Virtual Machine and click **NEXT**.



New Virtual Machine Wizard

Name the Virtual Machine

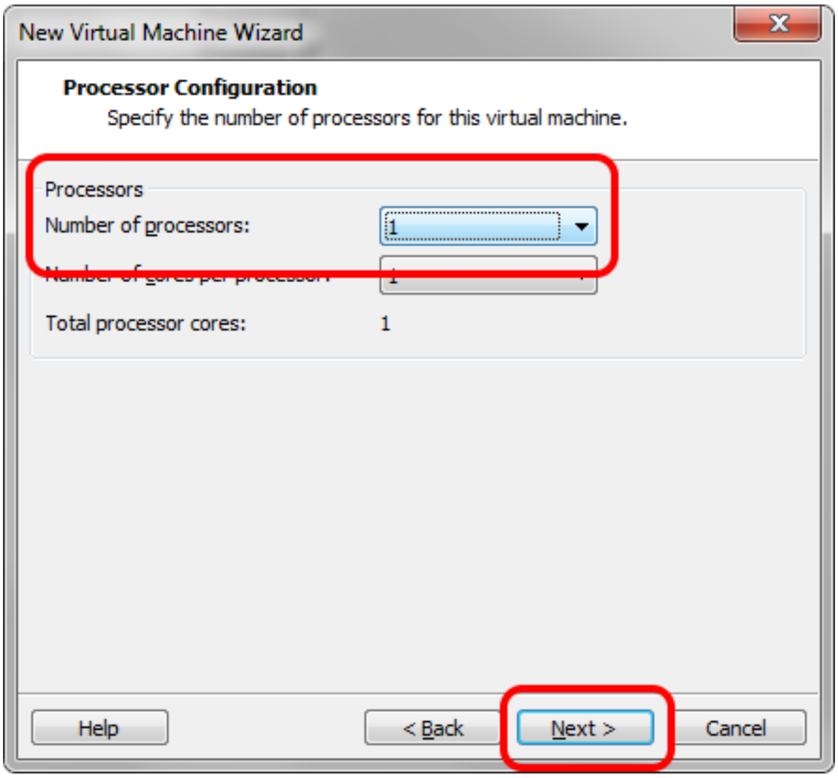
What name would you like to use for this virtual machine?

Virtual machine name: R80.10 GAIA

Location: C:\Users\cbrehm\Documents\Virtual Machines\R80.10 GAIA

The default location can be changed at Edit > Preferences.

Select "2" in "Number of Processors" and click **NEXT**.



New Virtual Machine Wizard

Processor Configuration

Specify the number of processors for this virtual machine.

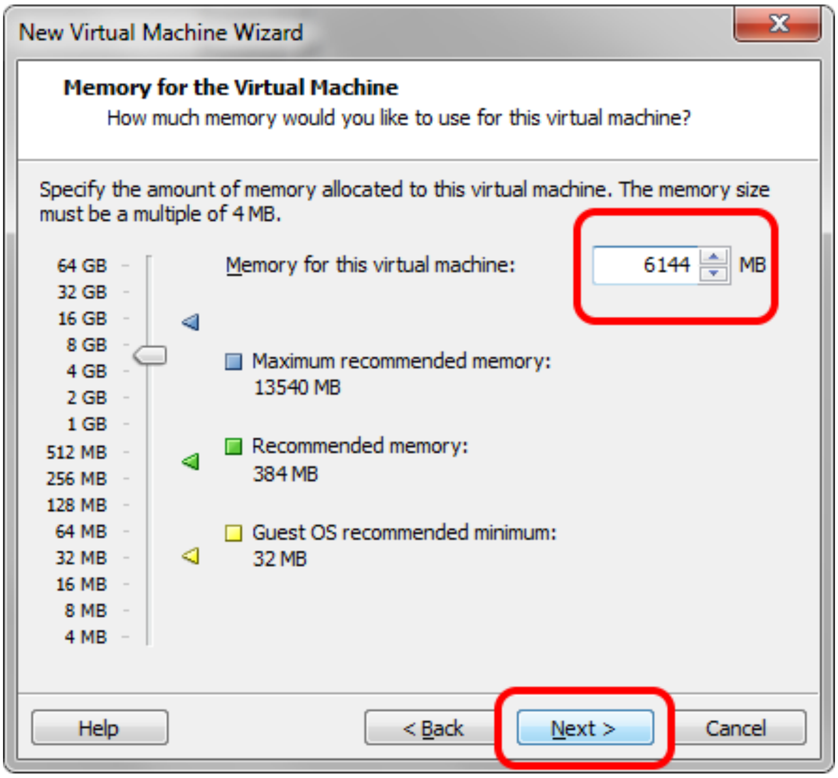
Processors

Number of processors: 1

Number of cores per processor: 1

Total processor cores: 1

Choose 6GB of RAM if your host computer has enough (you can also use 4GB of RAM if you have limited resources) and click **NEXT**.



New Virtual Machine Wizard

Memory for the Virtual Machine

How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

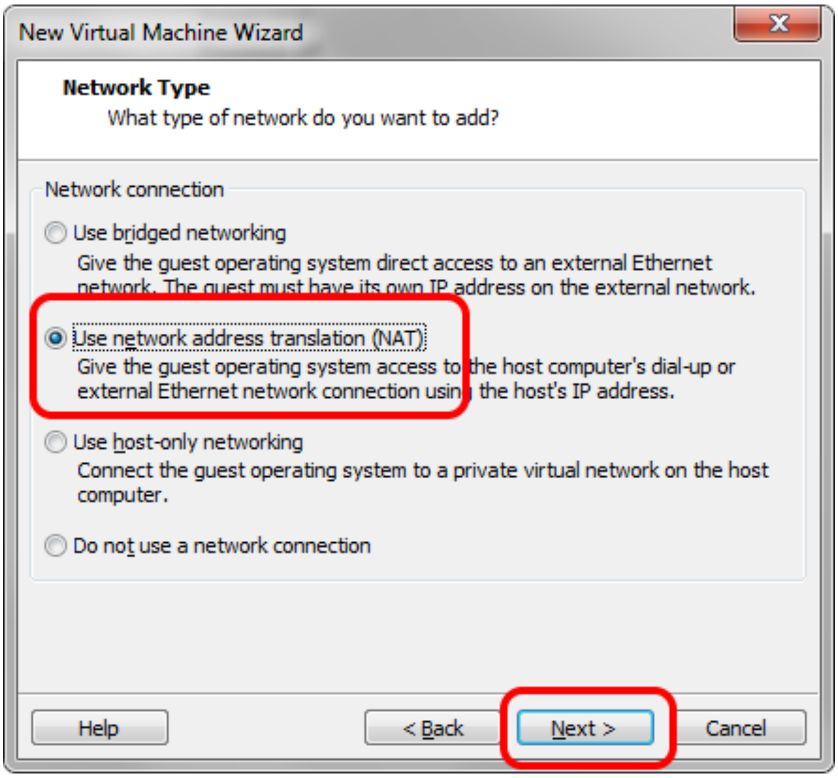
Memory for this virtual machine: 6144 MB

🟦 Maximum recommended memory: 13540 MB

🟩 Recommended memory: 384 MB

🟨 Guest OS recommended minimum: 32 MB

Select “Use Network Address Translation (NAT)” and click **NEXT**.



New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

○ Use bridged networking

Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

● Use network address translation (NAT)

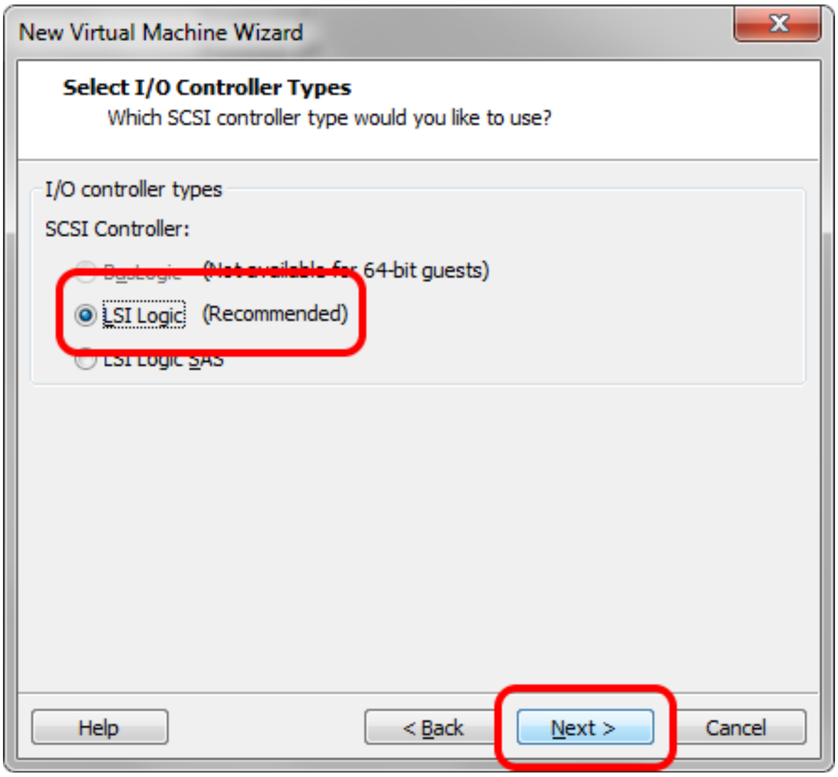
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking

Connect the guest operating system to a private virtual network on the host computer.

○ Do not use a network connection

Select "LSI Logic" and click **NEXT**.



New Virtual Machine Wizard

Select I/O Controller Types

Which SCSI controller type would you like to use?

I/O controller types

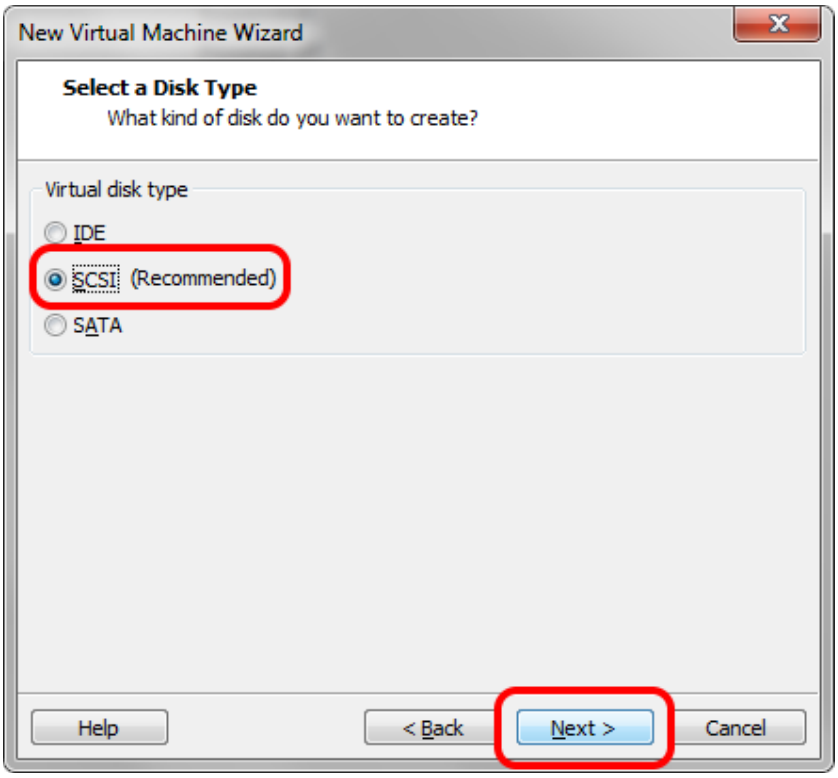
SCSI Controller:

○ BusLogic (Not available for 64-bit guests)

● LSI Logic (Recommended)

○ LSI Logic SAS

Select "SCSI" and click **NEXT**.



New Virtual Machine Wizard

Select a Disk Type

What kind of disk do you want to create?

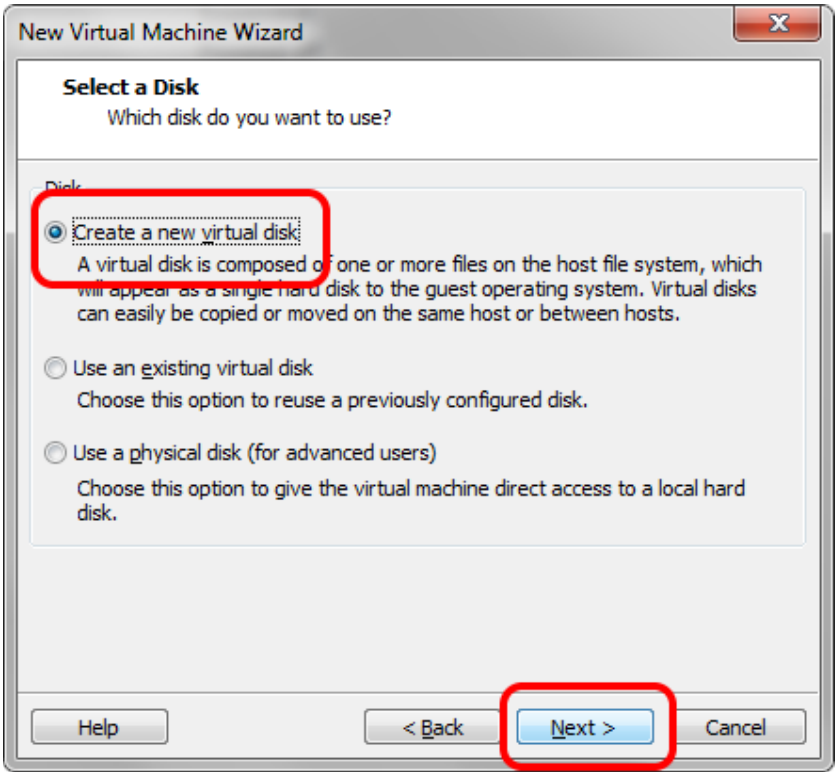
Virtual disk type

○ IDE

● SCSI (Recommended)

○ SATA

Select “Create a new virtual disk” and click **NEXT**.



New Virtual Machine Wizard

Select a Disk

Which disk do you want to use?

Disk

● Create a new virtual disk

A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

○ Use an existing virtual disk

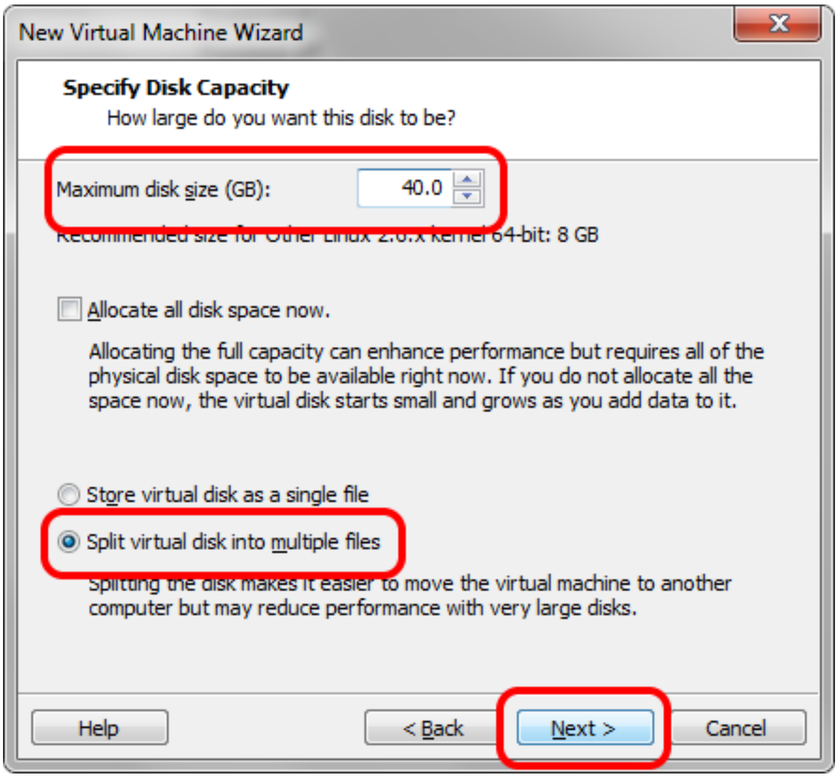
Choose this option to reuse a previously configured disk.

○ Use a physical disk (for advanced users)

Choose this option to give the virtual machine direct access to a local hard disk.

Configure “Maximum disk size” at 40GB (if your host computer has limited space, you can get by with 30GB). NOTE: If you leave “Allocate all disk space now”, the VM will only use as much drive space as needed, expanding up to the maximum size you have configured.

Select “Split virtual disk into multiple files” and click **NEXT**.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 40.0

Recommended size for Other Linux 2.6.x kernel 64-bit: 8 GB

□ Allocate all disk space now.

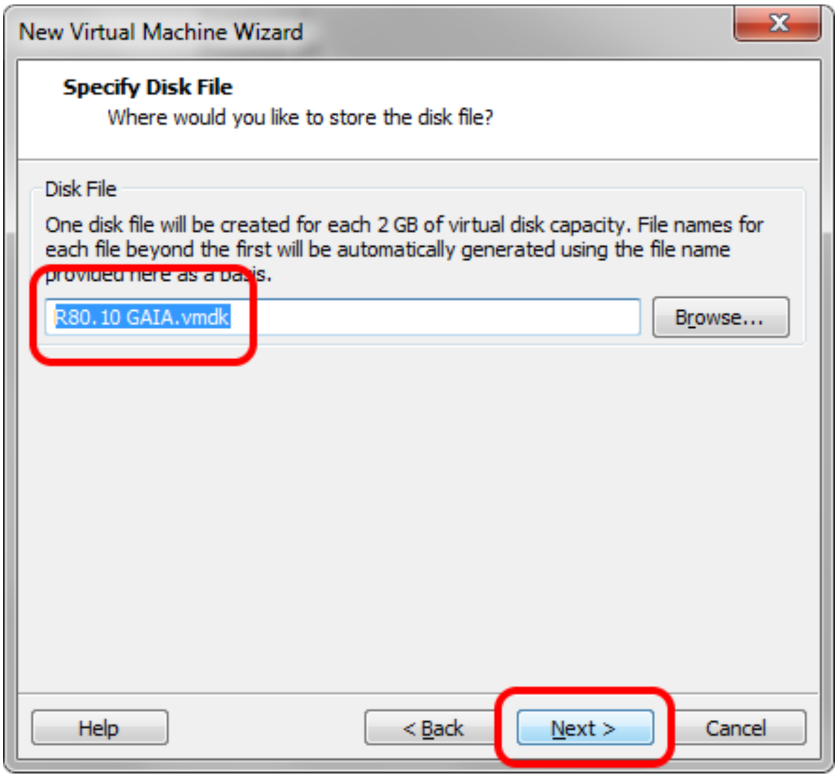
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ 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.

Leave the default Disk File name and click **NEXT**.



New Virtual Machine Wizard

Specify Disk File

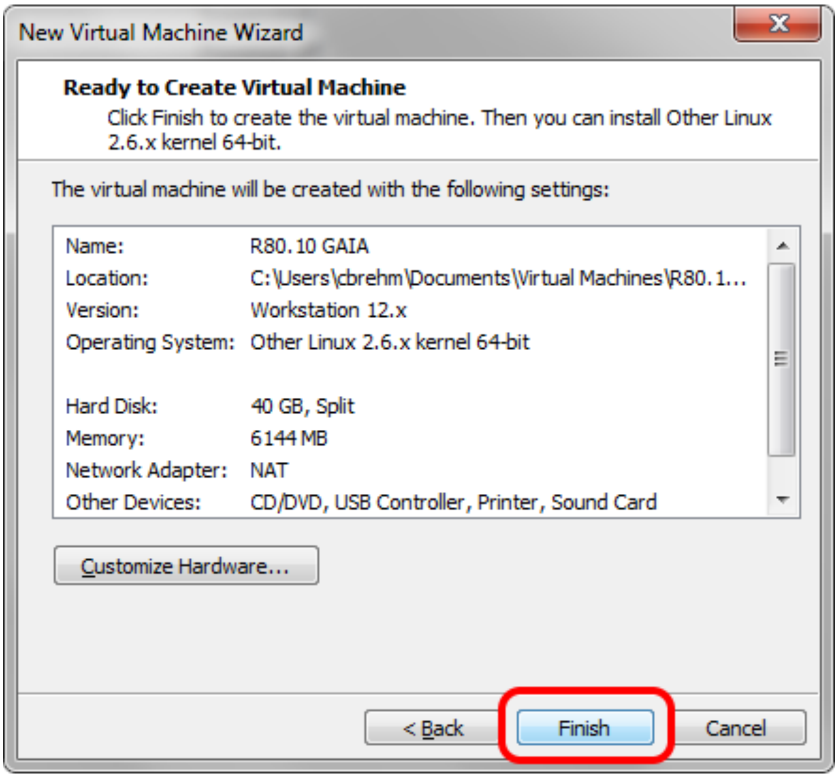
Where would you like to store the disk file?

Disk File

One disk file will be created for each 2 GB of virtual disk capacity. File names for each file beyond the first will be automatically generated using the file name provided here as a basis.

R80.10 GAIA.vmdk

Click **FINISH**.


New Virtual Machine Wizard

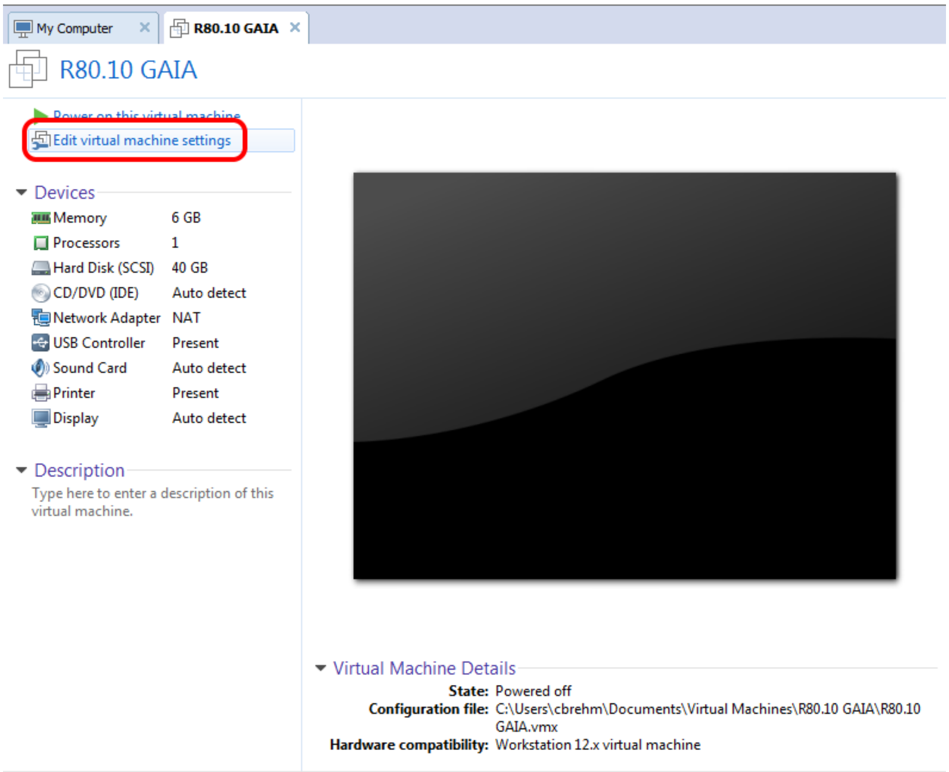
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Other Linux 2.6.x kernel 64-bit.

The virtual machine will be created with the following settings:

Name:	R80.10 GAIA
Location:	C:\Users\cbrehm\Documents\Virtual Machines\R80.1...
Version:	Workstation 12.x
Operating System:	Other Linux 2.6.x kernel 64-bit
Hard Disk:	40 GB, Split
Memory:	6144 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

VMware will not create your VM and open a new tab in your Workstation GUI. Click the Edit virtual machine settings **link.**



Devices

Memory	6 GB
Processors	1
Hard Disk (SCSI)	40 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description

Type here to enter a description of this virtual machine.

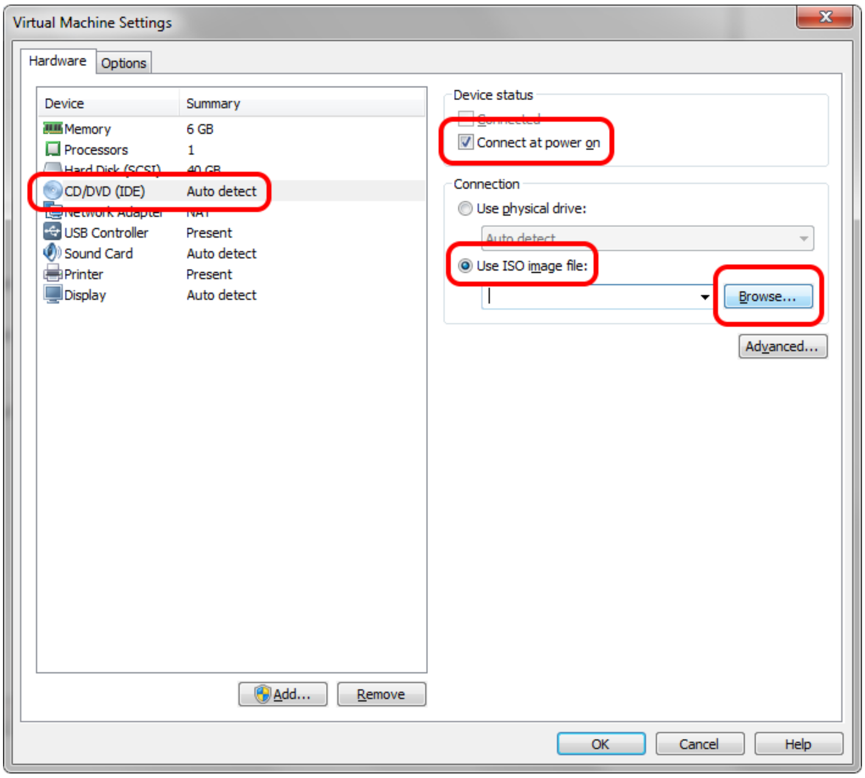
Virtual Machine Details

State: Powered off

Configuration file: C:\Users\cbrehm\Documents\Virtual Machines\R80.10 GAIA\R80.10 GAIA.vmx

Hardware compatibility: Workstation 12.x virtual machine

Click “CD/DVD (IDE)” and check “Connect at power on”. Click **Use ISO image** file: and click **Browse** to launch the file browser.



Device	Summary
Memory	6 GB
Processors	1
Hard Disk (SCSI)	40 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

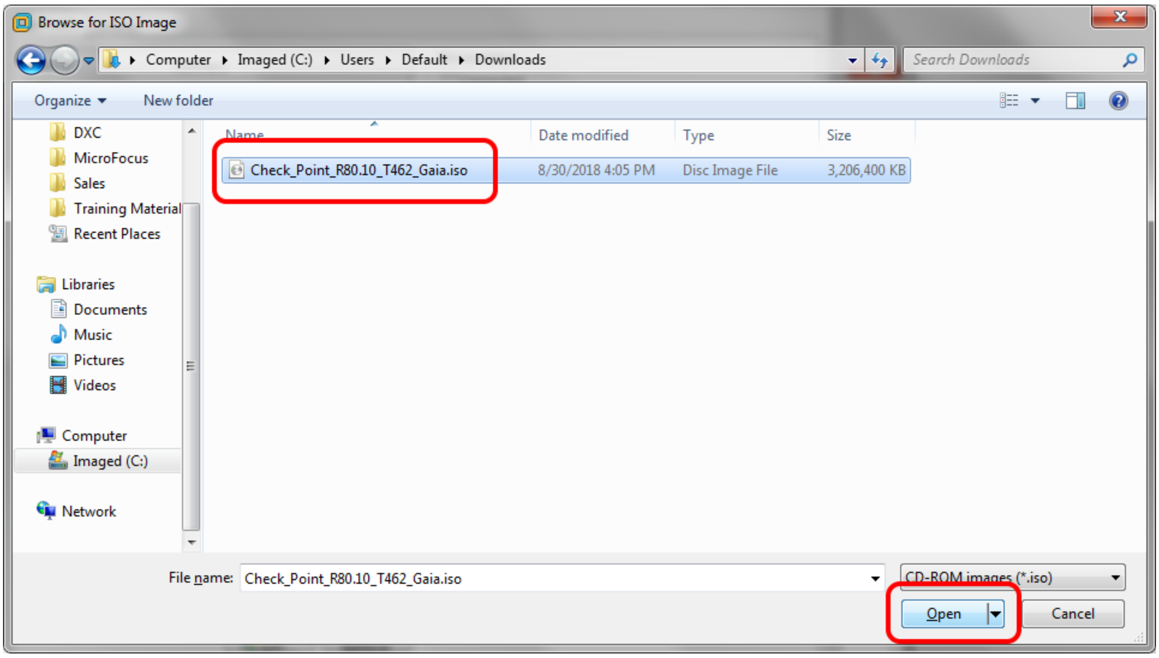
☐ Connected

☑ Connect at power on

○ Use physical drive: Auto detect

● Use ISO image file:

Navigate to the location where you downloaded the Gaia ISO. Select the Check_Point_R80.10_T462.ISO file and click **OPEN**.

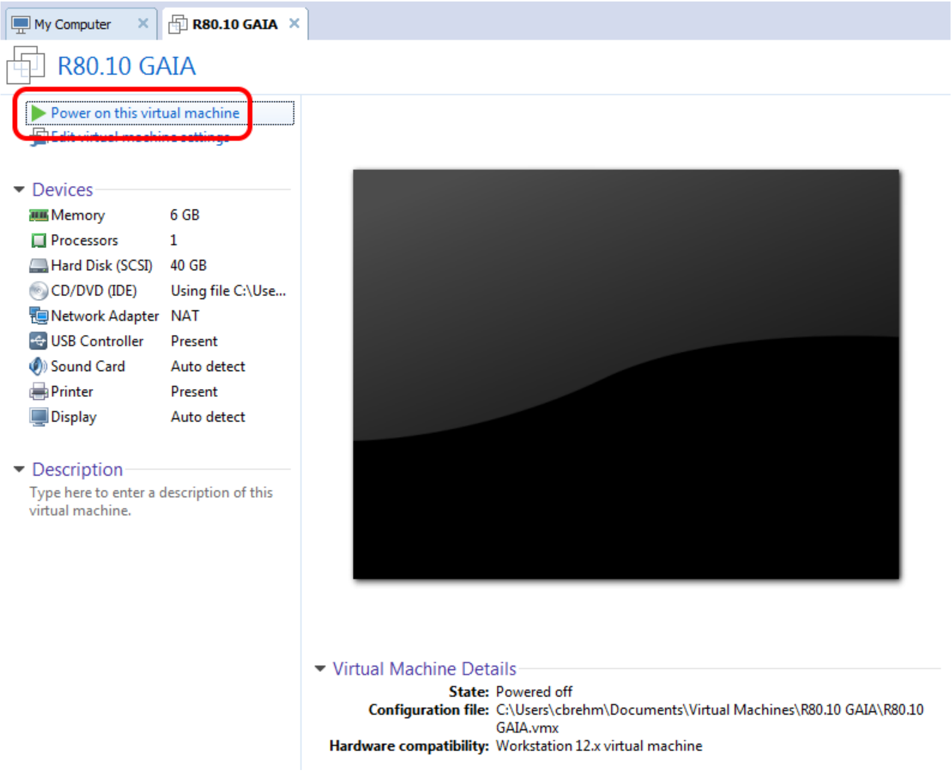


Name	Date modified	Type	Size
Check_Point_R80.10_T462_Gaia.iso	8/30/2018 4:05 PM	Disc Image File	3,206,400 KB

File name: Check_Point_R80.10_T462_Gaia.iso

CD-ROM images (*.iso)

Click **Power on the virtual machine**.



Devices

Memory	6 GB
Processors	1
Hard Disk (SCSI)	40 GB
CD/DVD (IDE)	Using file C:\Use...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description

Type here to enter a description of this virtual machine.

Virtual Machine Details

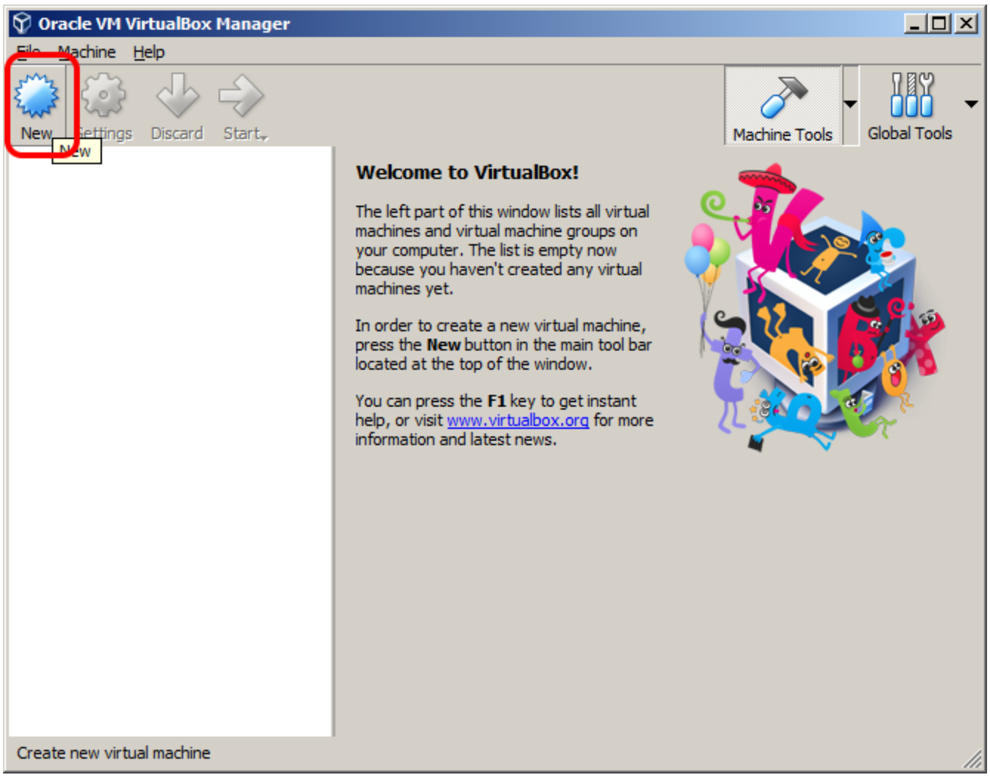
State: Powered off
Configuration file: C:\Users\cbrehm\Documents\Virtual Machines\R80.10 GAIA\R80.10 GAIA.vmx
Hardware compatibility: Workstation 12.x virtual machine

You should now see the Virtual Machine begin to boot. You can skip the VirtualBox section and move on to the GAIA Installation section.

VirtualBox – VM Creation

Note: The following screenshots are from Oracle VirtualBox 5.2.2
https://www.virtualbox.org/wiki/Downloads

The VirtualBox GUI. Click the **New** button to start the "Create Virtual Machine" wizard.



Welcome to VirtualBox!

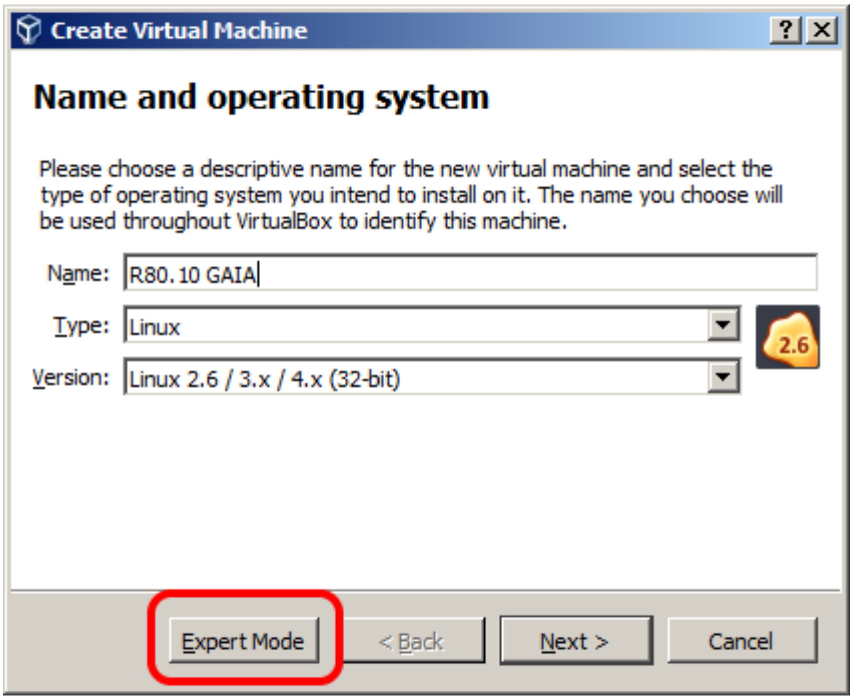
The left part of this window lists all virtual machines and virtual machine groups on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Create new virtual machine

Click the **Expert Mode** button.



Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: R80.10 GAIA

Type: Linux

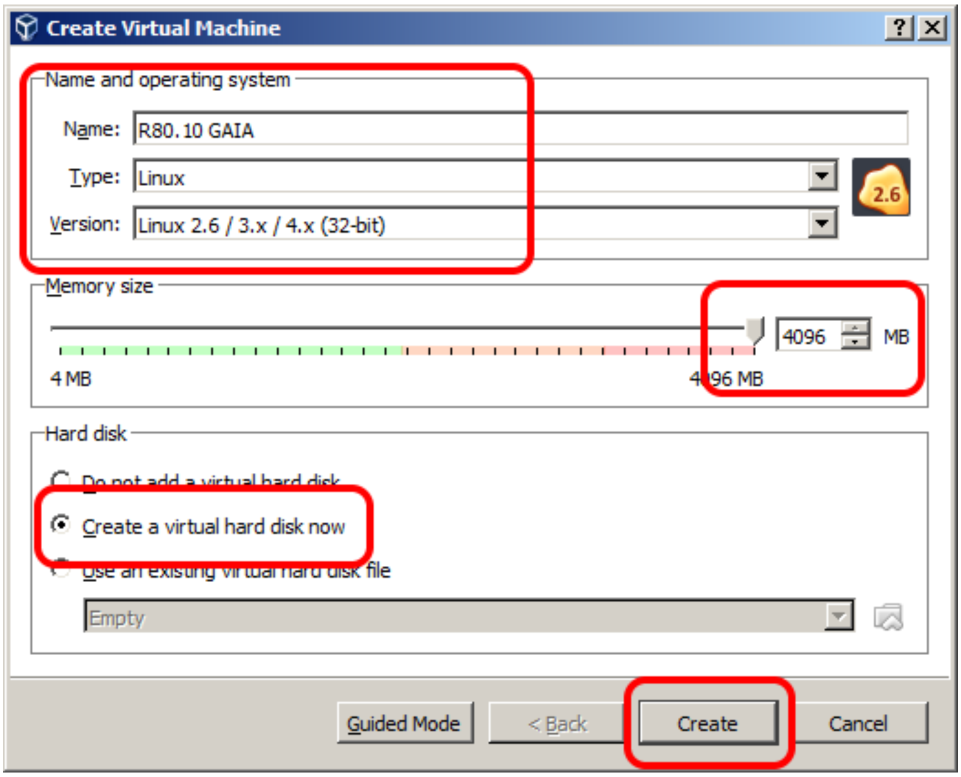
Version: Linux 2.6 / 3.x / 4.x (32-bit)

Type in a Name for your VM. Choose “Linux” for the “Type”. Choose “Linux 2.6 / 3.x / 4.x (32-bit)” for the “Version”.

Choose 6GB of RAM. [NOTE: In the screenshot below, I was working on system with limited resources, and 4GB is sufficient to get a working GAIA installation for this basic exercise.]

Select “Create a virtual hard disk now”.

Click **CREATE**.



Create Virtual Machine

Name and operating system

Name: R80.10 GAIA

Type: Linux

Version: Linux 2.6 / 3.x / 4.x (32-bit)

Memory size

4096 MB

4 MB — 4096 MB

Hard disk

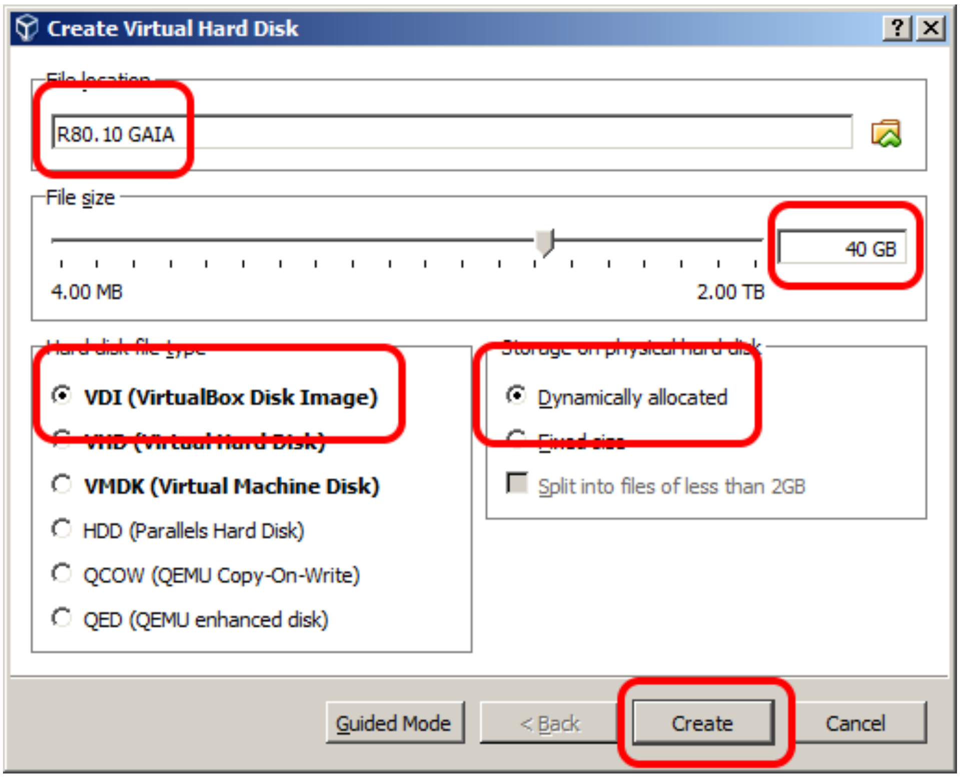
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Empty

Leave the default “File location” settings. Choose 40GB (30GB minimum if you have limited resources). Leave the default settings of “VDI” and “Dynamically Allocated” and Click **CREATE**.



Create Virtual Hard Disk

File location

R80.10 GAIA

File size

4.00 MB — 2.00 TB — 40 GB

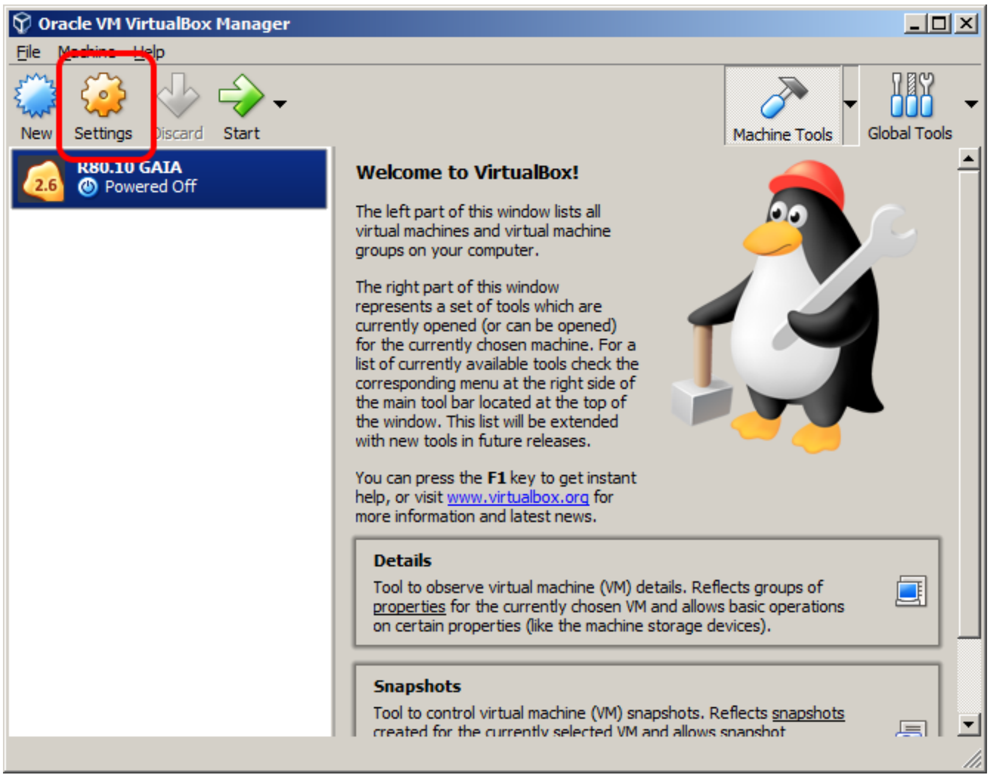
Hard disk file type

- ● VDI (VirtualBox Disk Image)
- ○ VHD (Virtual Hard Disk)
- ○ VMDK (Virtual Machine Disk)
- ○ HDD (Parallels Hard Disk)
- ○ QCOW (QEMU Copy-On-Write)
- ○ QED (QEMU enhanced disk)

Storage on physical hard disk

- ● Dynamically allocated
- ○ Fixed size
- □ Split into files of less than 2GB

Click the **Settings** button in the main VirtualBox GUI window to modify the settings of our new VM.



R80.10 GAIA
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

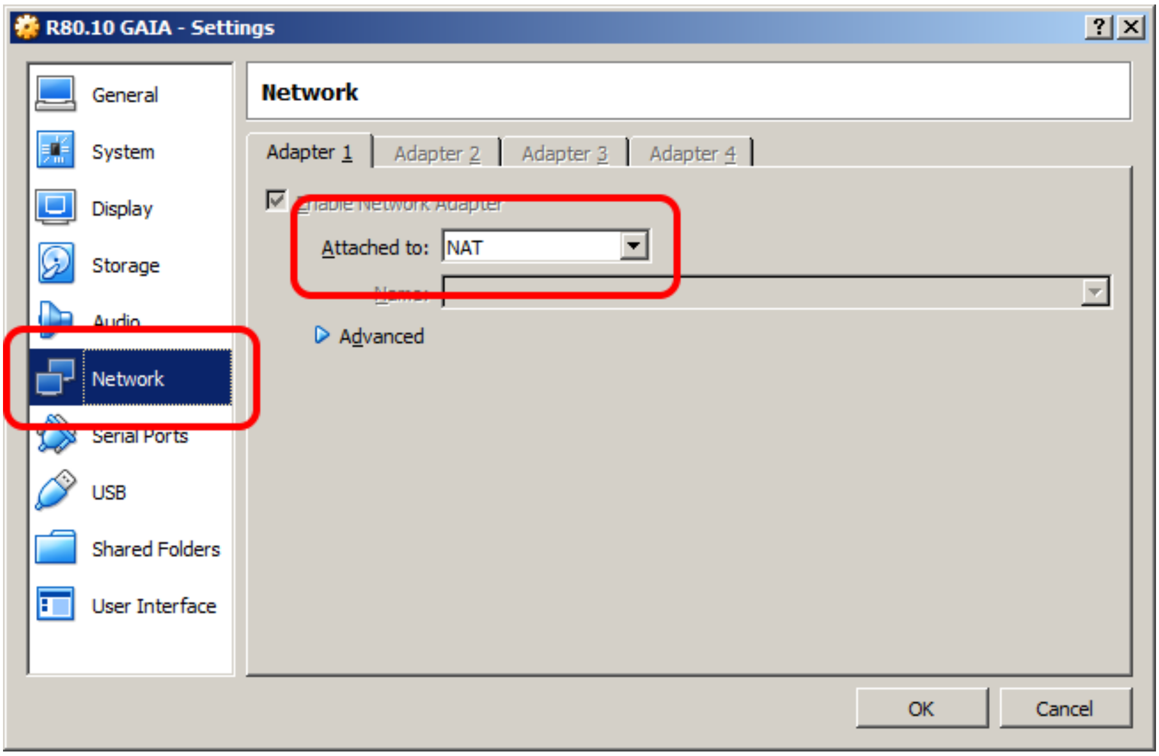
Details

Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).

Snapshots

Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot

Click **Network** and verify that “NAT” is selected for “Attached to”.



R80.10 GAIA - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

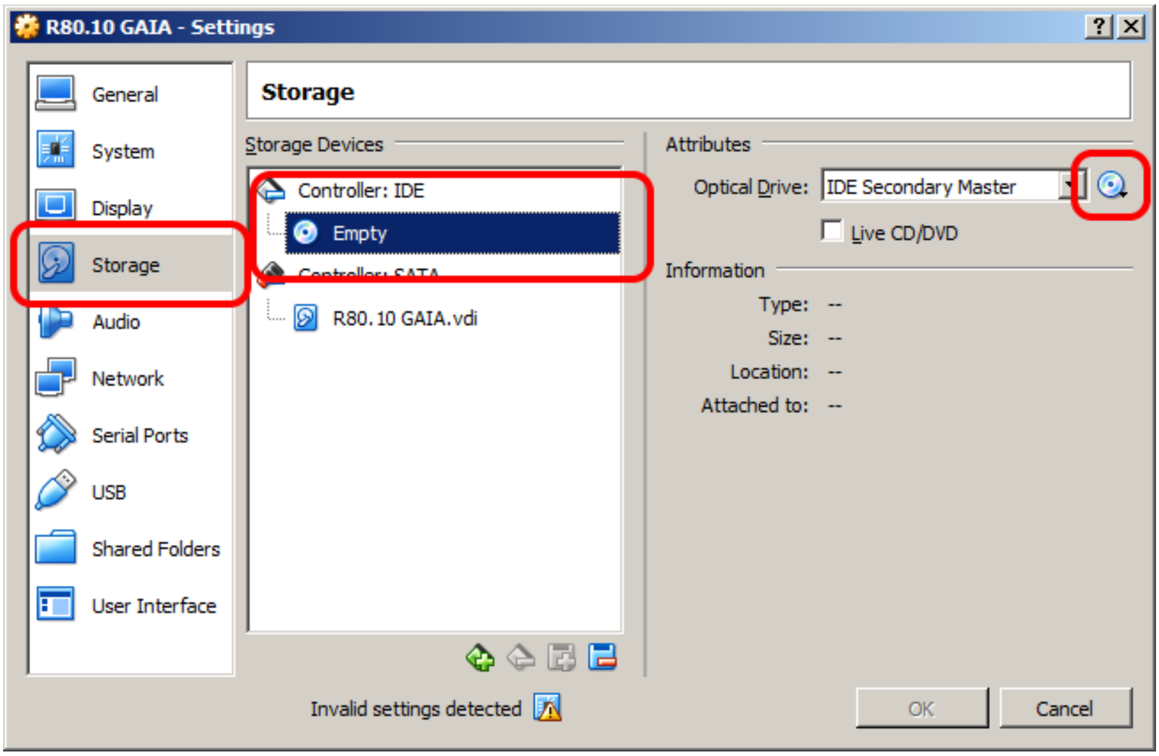
☑ Enable Network Adapter

Attached to: NAT

Name:

Advanced

Click **Storage** and click on the "Empty" CD/DVD icon. Click the "disk icon" on the left.



R80.10 GAIA - Settings

Storage

Storage Devices

Controller: IDE
Empty
Controller: SATA
R80.10 GAIA.vdi

Attributes

Optical Drive: IDE Secondary Master

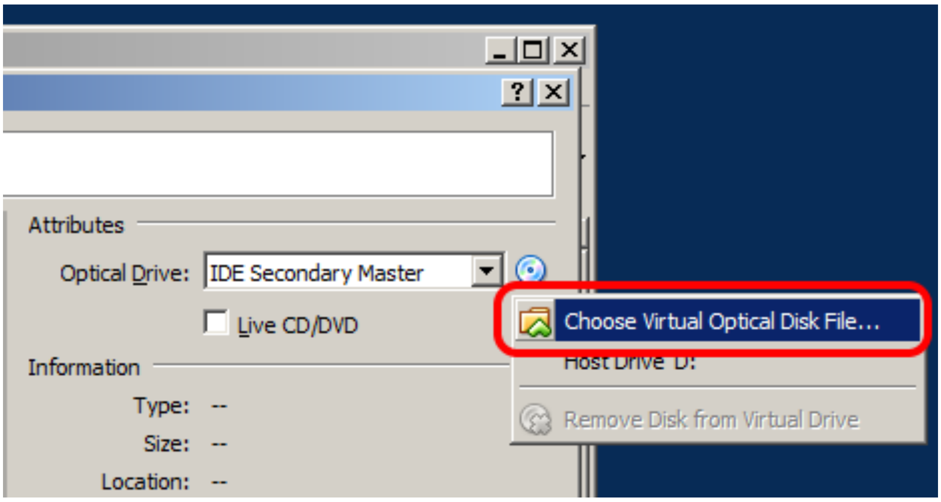
□ Live CD/DVD

Information

Type: --
Size: --
Location: --
Attached to: --

Invalid settings detected

Click **Choose Virtual Optical Disk File**…



Attributes

Optical Drive: IDE Secondary Master

□ Live CD/DVD

Information

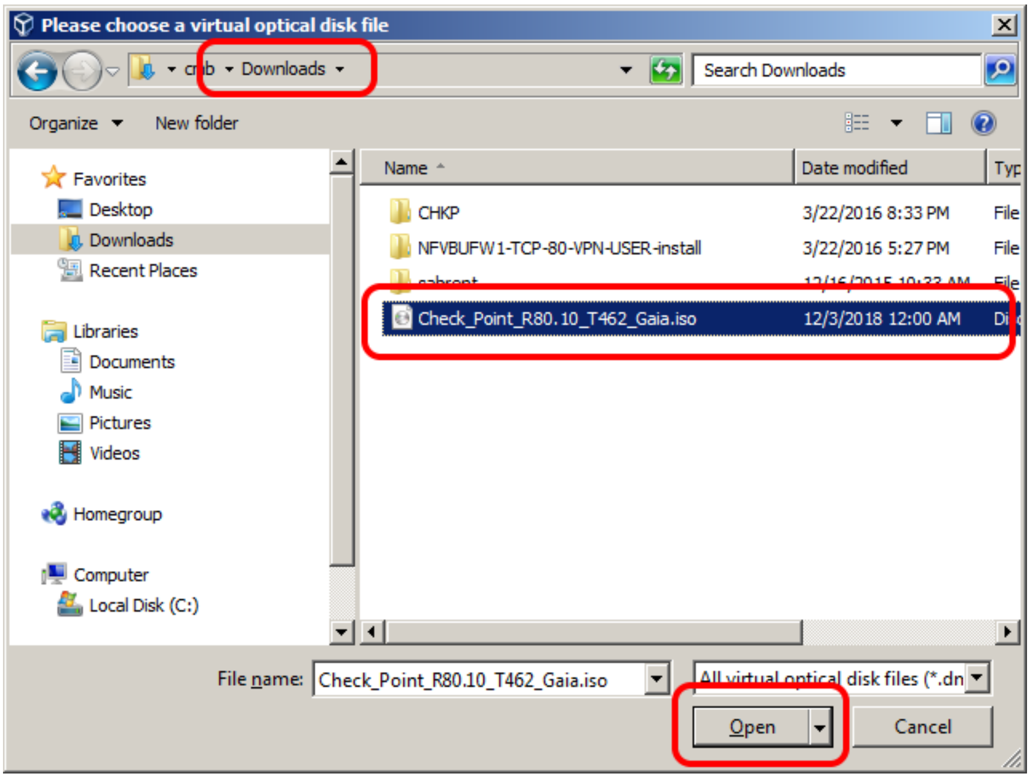
Type: --

Size: --

Location: --

Choose Virtual Optical Disk File…
Host Drive D:
Remove Disk from Virtual Drive

Navigate to the location where you downloaded the Gaia ISO. Select the Check_Point_R80.10_T462.ISO file and click **OPEN**.



Please choose a virtual optical disk file

Name	Date modified	Typ
CHKP	3/22/2016 8:33 PM	File
NFVBUFW1-TCP-80-VPN-USER-install	3/22/2016 5:27 PM	File
cabrent	12/16/2015 10:33 AM	File
Check_Point_R80.10_T462_Gaia.iso	12/3/2018 12:00 AM	Di

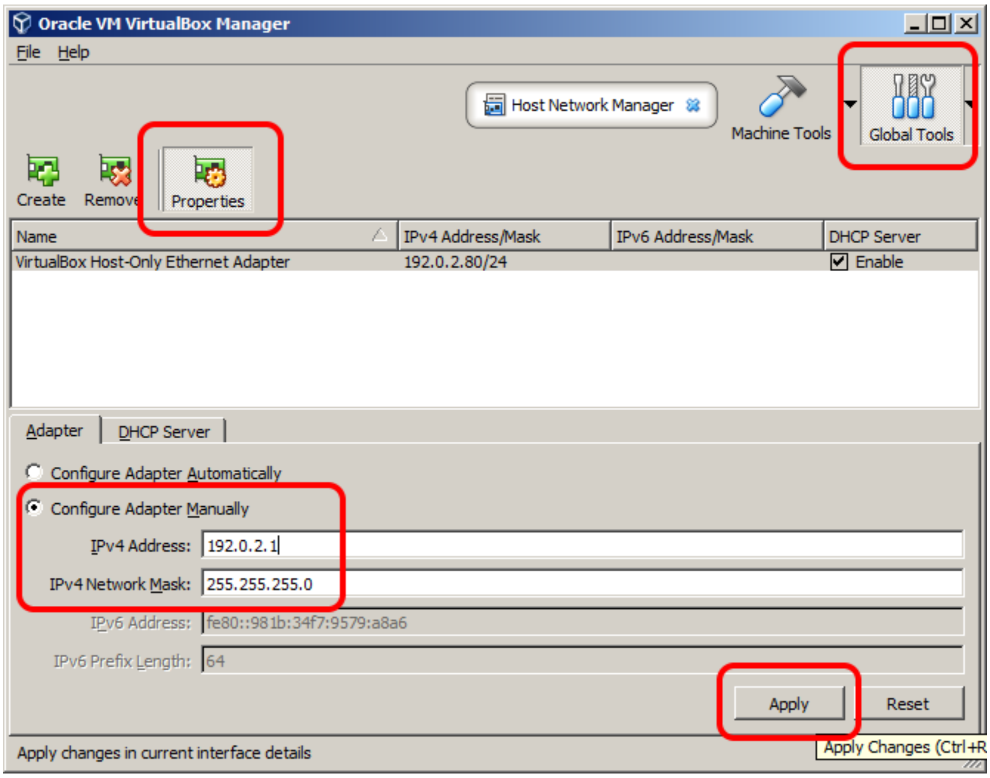
File name: Check_Point_R80.10_T462_Gaia.iso

All virtual optical disk files (*.dn

in the main VirtualBox GUI, click on the **Global Tools** button in the upper right. Click on the **Properties** button to view the global VirtualBox network configuration settings.

For this exercise, we are going to configure the following network adaptor settings:
IPv4 Address: 192.0.2.1
IPv4 Network Mask: 255.255.255.0

Click **APPLY**.



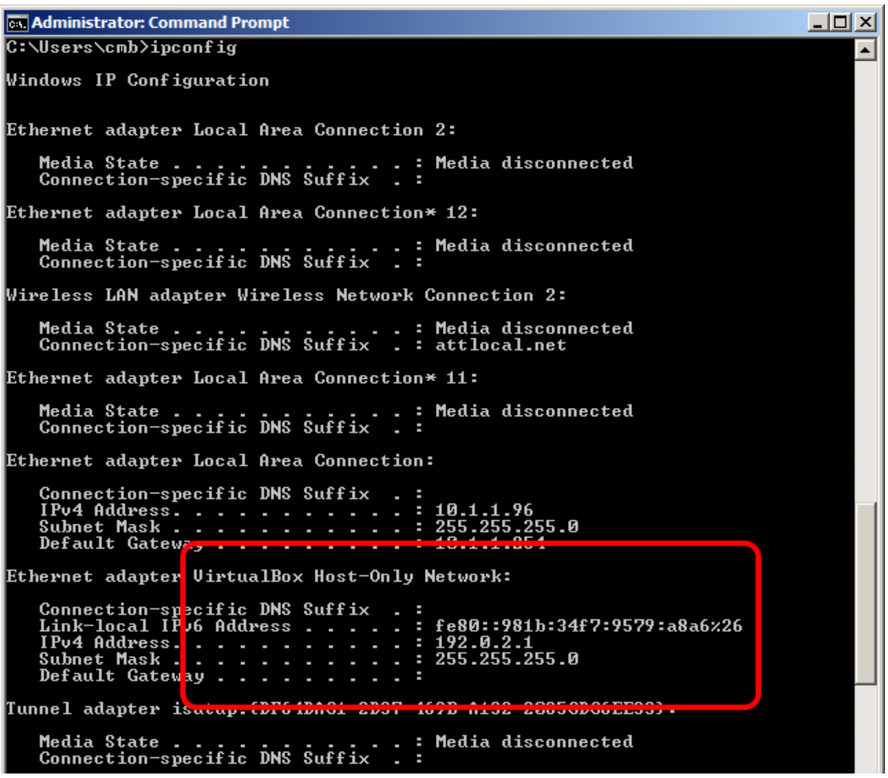
Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.0.2.80/24		☑ Enable

○ Configure Adapter Automatically
● Configure Adapter Manually
IPv4 Address: 192.0.2.1
IPv4 Network Mask: 255.255.255.0
IPv6 Address: fe80::981b:34f7:9579:a8a6
IPv6 Prefix Length: 64

Apply changes in current interface details
Apply Changes (Ctrl+R

To verify that you can see the VirtualBox Host-Only network Adaptor, open the “Command Prompt” (aka cmd.exe) on your Windows computer. There are multiple ways to open this utility in Windows 7 and 10. My personal favorite is to hold down the “Windows” key (aka “Start” key) and type “R” to open the run dialog. Type “cmd.exe” and hit the **ENTER** key. You can also click the Start button and type “cmd.exe” and click on the appropriate search result.

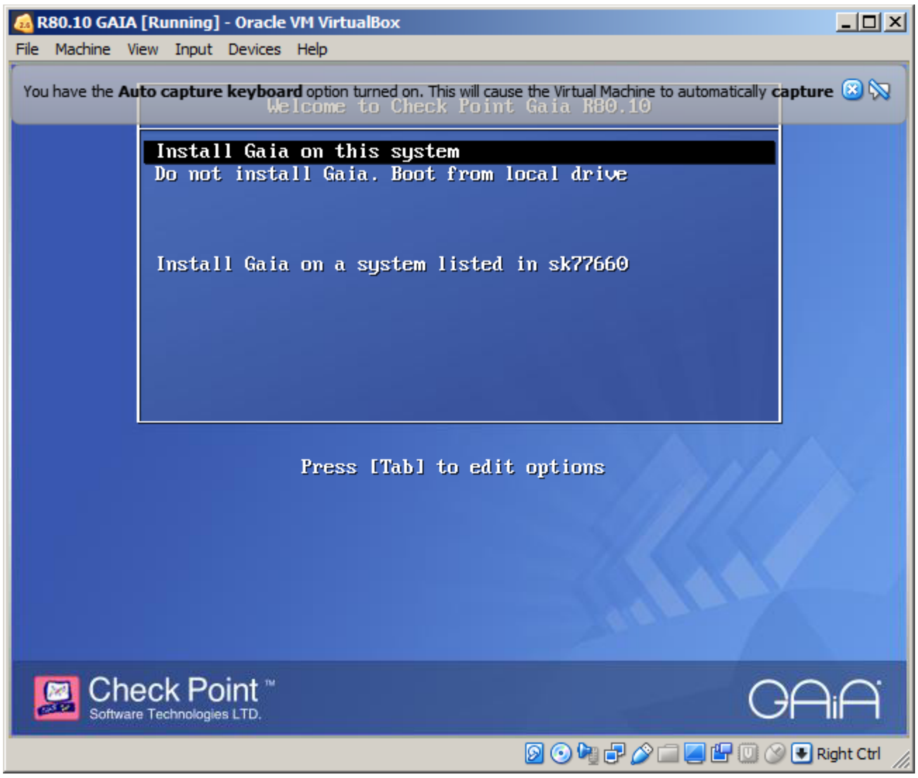
Once the Command Prompt is running, type “ipconfig” and hit **ENTER**. Look for “Ethernet adapter VirtualBox Host-Only Network”. It should match the settings entered in the previous step.



```
C:\Users\cmb>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : attlocal.net

Ethernet adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.1.1.96
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.1.254

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::981b:34f7:9579:a8a6%26
   IPv4 Address. . . . . . . . . . . : 192.0.2.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{DF64DA61-2D97-469B-A132-28850D06EE33}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Type “exit” to quit the **Command Prompt**.

From the main VirtualBox GUI, select the new GAIA VM and click the **Start** button. The R80.10 GAIA VM window will appear. Point your mouse cursor into the window and left-click the mouse to “capture” the Keyboard & Mouse controls (this means any typing you do will be done inside the VM).

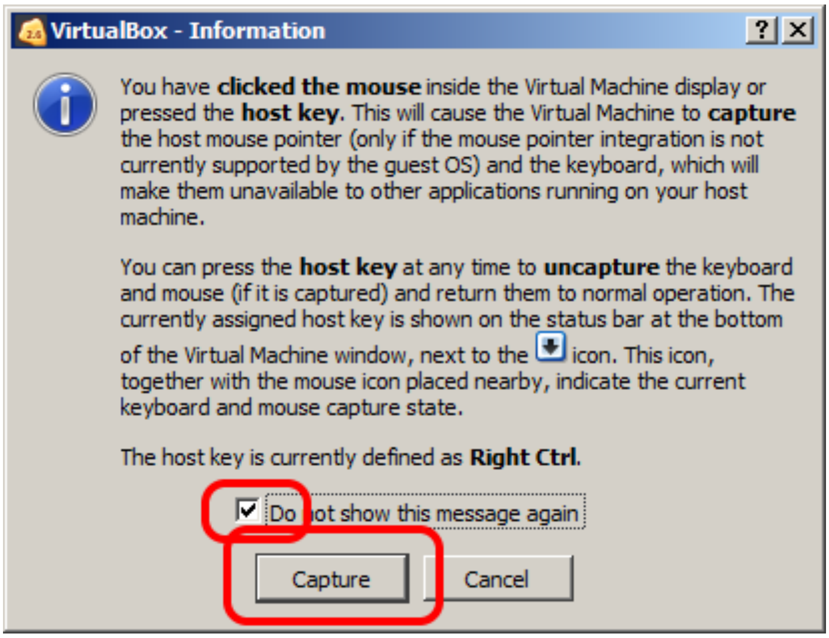


R80.10 GAIA [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Check Point™ Software Technologies LTD.
GAiA
Right Ctrl

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture**

```
Welcome to Check Point Gaia R80.10

 Install Gaia on this system
 Do not install Gaia. Boot from local drive


 Install Gaia on a system listed in sk77660


          Press [Tab] to edit options
```

You will see a pop-up with an explanation of mouse/keyboard capture and release.



You have **clicked the mouse** inside the Virtual Machine display or pressed the **host key**. This will cause the Virtual Machine to **capture** the host mouse pointer (only if the mouse pointer integration is not currently supported by the guest OS) and the keyboard, which will make them unavailable to other applications running on your host machine.

You can press the **host key** at any time to **uncapture** the keyboard and mouse (if it is captured) and return them to normal operation. The currently assigned host key is shown on the status bar at the bottom of the Virtual Machine window, next to the icon. This icon, together with the mouse icon placed nearby, indicate the current keyboard and mouse capture state.

The host key is currently defined as **Right Ctrl**.

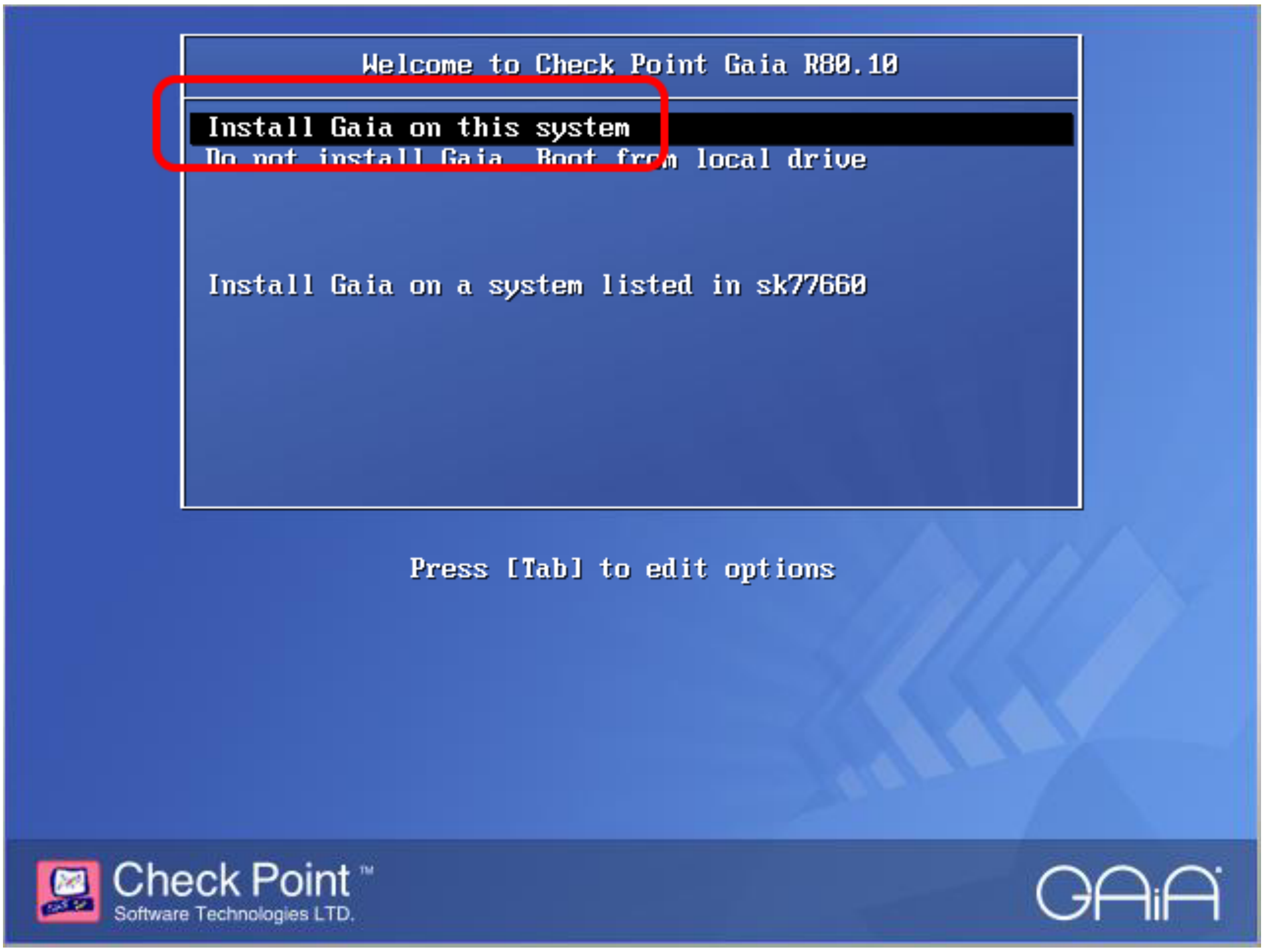
☑ Do not show this message again

You are now ready to move on to the **GAIA Installation** section…

GAIA Installation

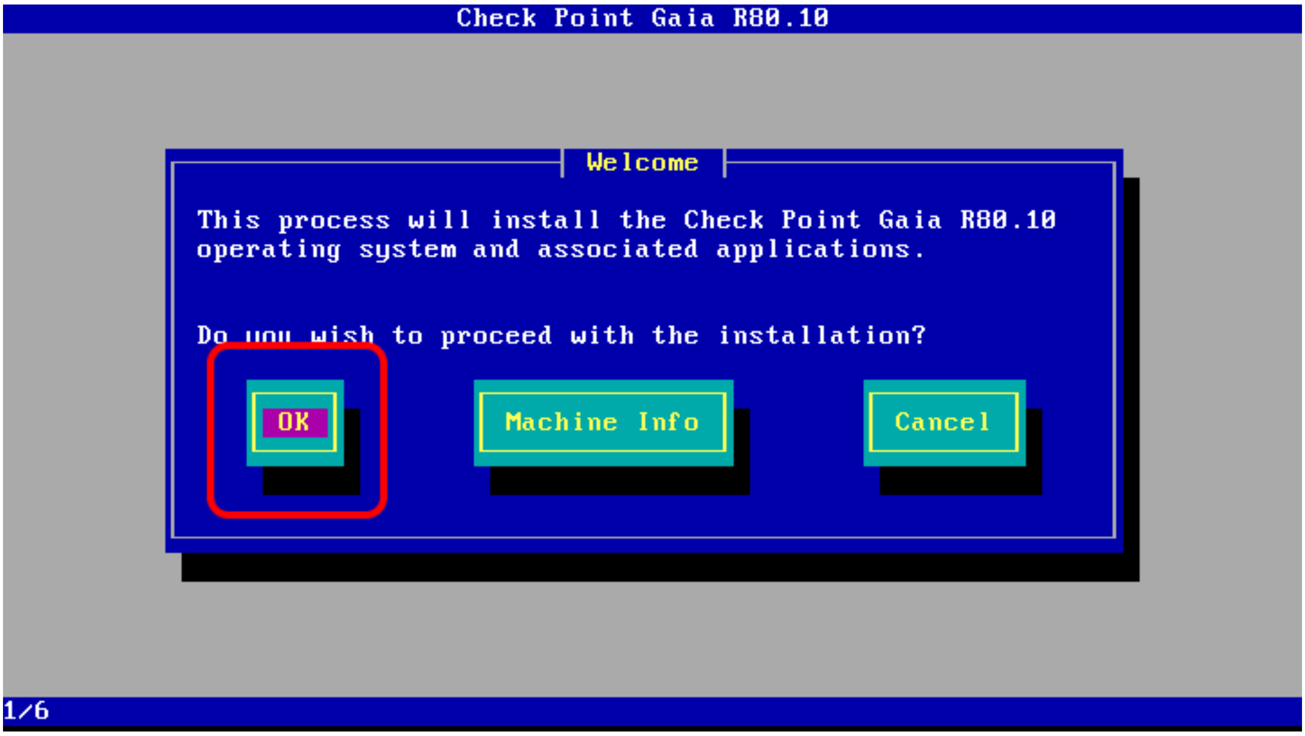
Note: During installation, you must use your ARROW KEYS & the TAB button to navigate, and the ENTER key to “click”. Your mouse will not work during installation.

Power on the Virtual Machine, wait for the ISO to boot. Use your UP ARROW key to highlight “INSTALL GAIA ON THIS SYSTEM”. Press the **ENTER** key.



```
Welcome to Check Point Gaia R80.10

Install Gaia on this system
Do not install Gaia  Boot from local drive


Install Gaia on a system listed in sk77660


Press [Tab] to edit options
```

Use the **ENTER** key to select **OK**



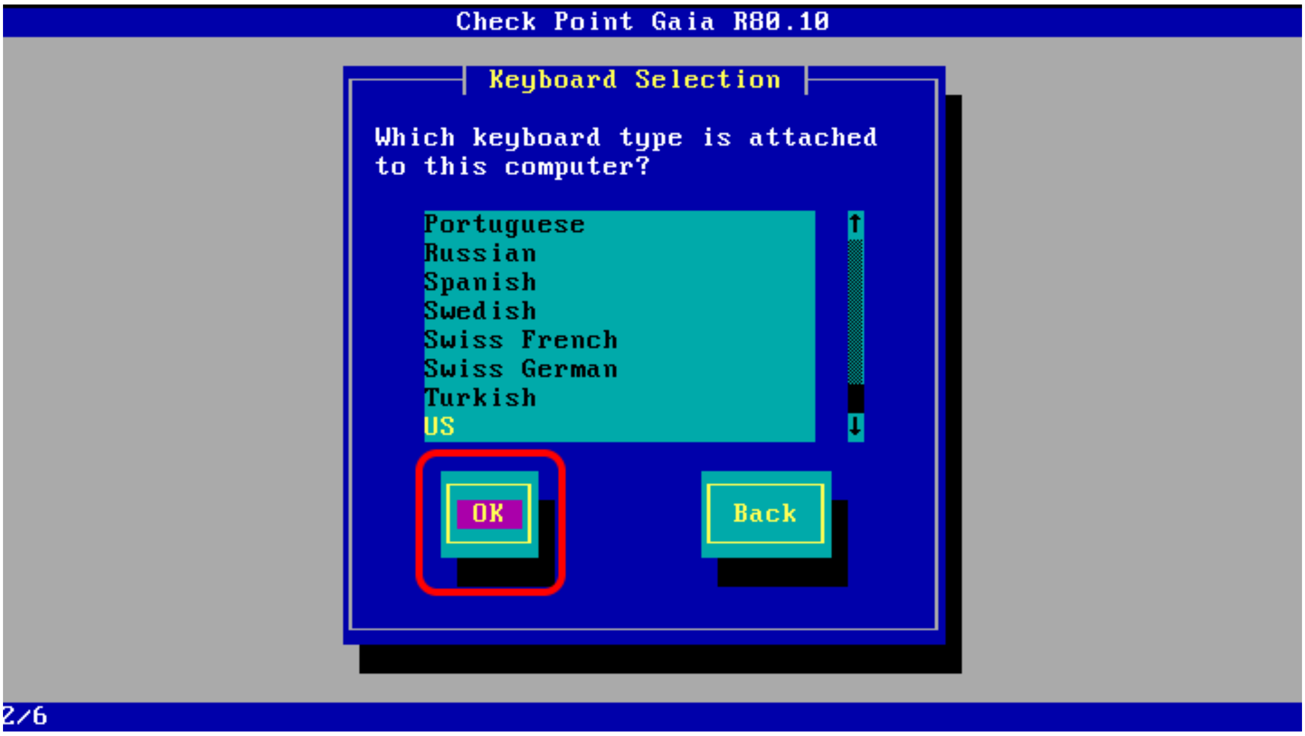
Check Point Gaia R80.10

Welcome

This process will install the Check Point Gaia R80.10 operating system and associated applications.

Do you wish to proceed with the installation?

Select your Keyboard Layout (Default is US). Press **TAB** to highlight **OK** and press **ENTER.**



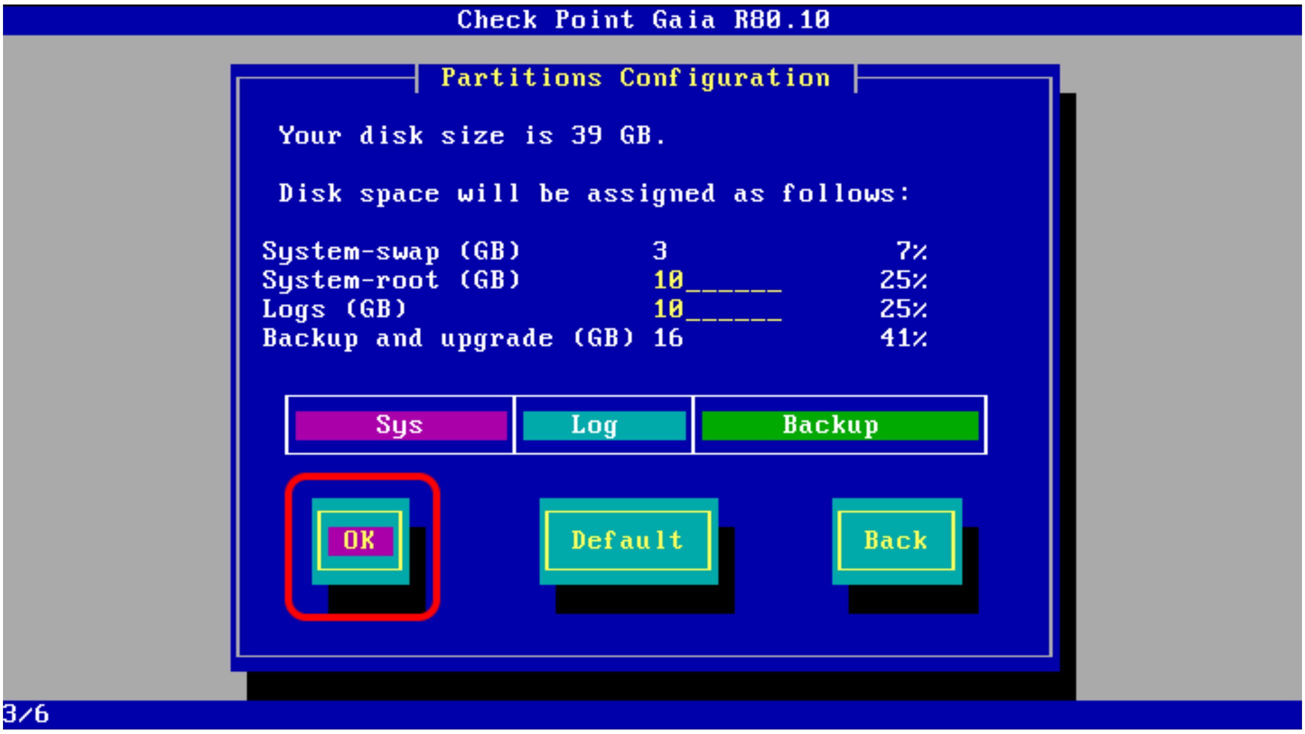
Check Point Gaia R80.10

Keyboard Selection

Which keyboard type is attached to this computer?

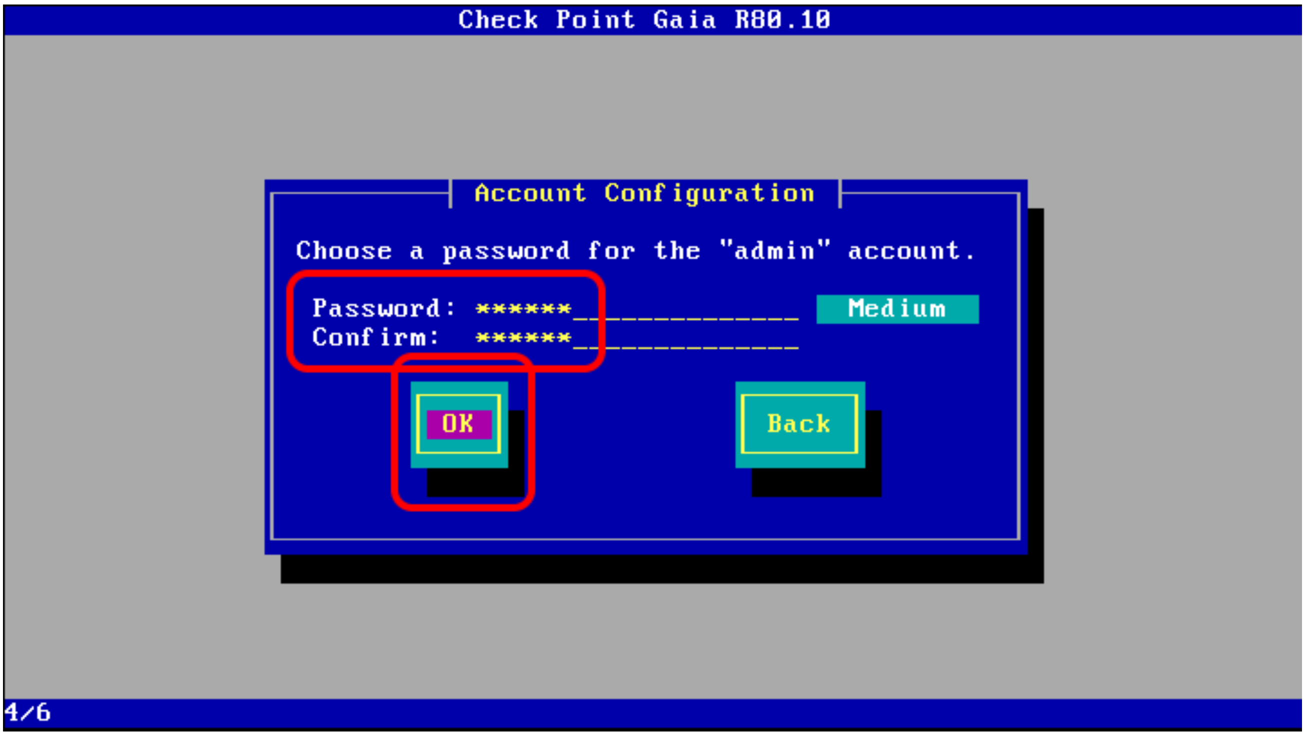
Portuguese
Russian
Spanish
Swedish
Swiss French
Swiss German
Turkish
US

Leave the default options and navigate to **OK.** Press **ENTER** to continue.



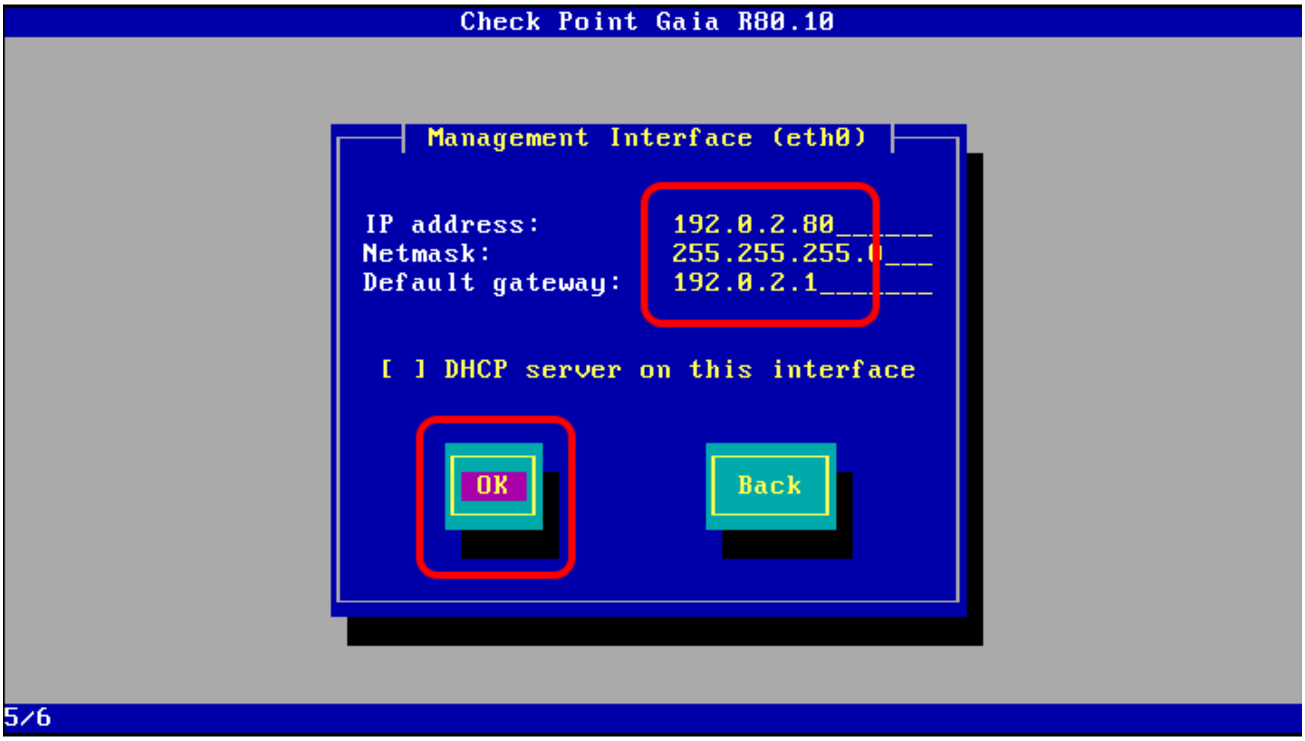
```
Check Point Gaia R80.10

Partitions Configuration

Your disk size is 39 GB.

Disk space will be assigned as follows:

System-swap (GB)         3           7%
System-root (GB)         10______   25%
Logs (GB)                10______   25%
Backup and upgrade (GB)  16         41%
```

Enter a password, hit **TAB**, and enter the password a second time. Hit **TAB** to select **OK** and hit **ENTER.**



```
Check Point Gaia R80.10

Account Configuration

Choose a password for the "admin" account.

Password: ******________________  Medium
Confirm:  ******________________
```

Type in the following settings for network connection eth0 settings. Hit **TAB** to move between fields. Hit **TAB** to highlight **OK.** Hit **ENTER** to continue.



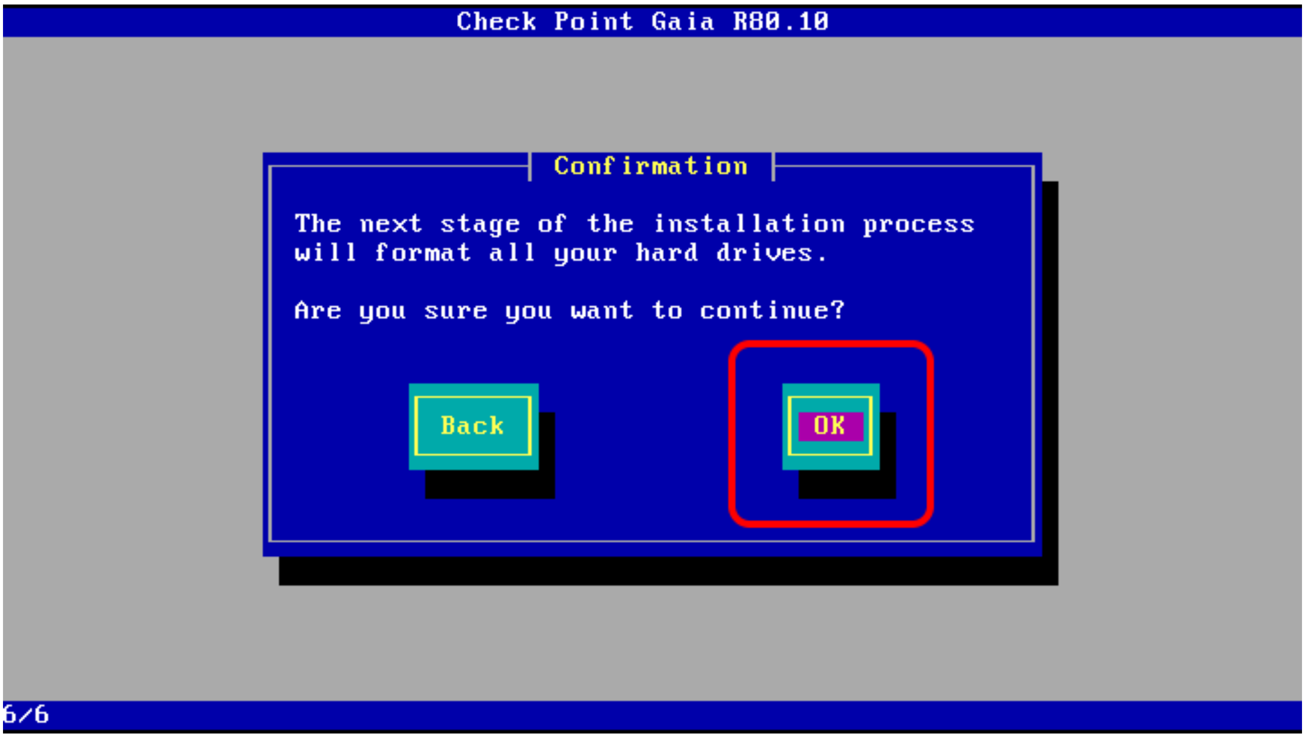
Check Point Gaia R80.10

Management Interface (eth0)

```
IP address:          192.0.2.80_______
Netmask:             255.255.255.0___
Default gateway:     192.0.2.1________
```

[ ] DHCP server on this interface

Hit **TAB** to highlight **OK.** Hit **ENTER** to continue.



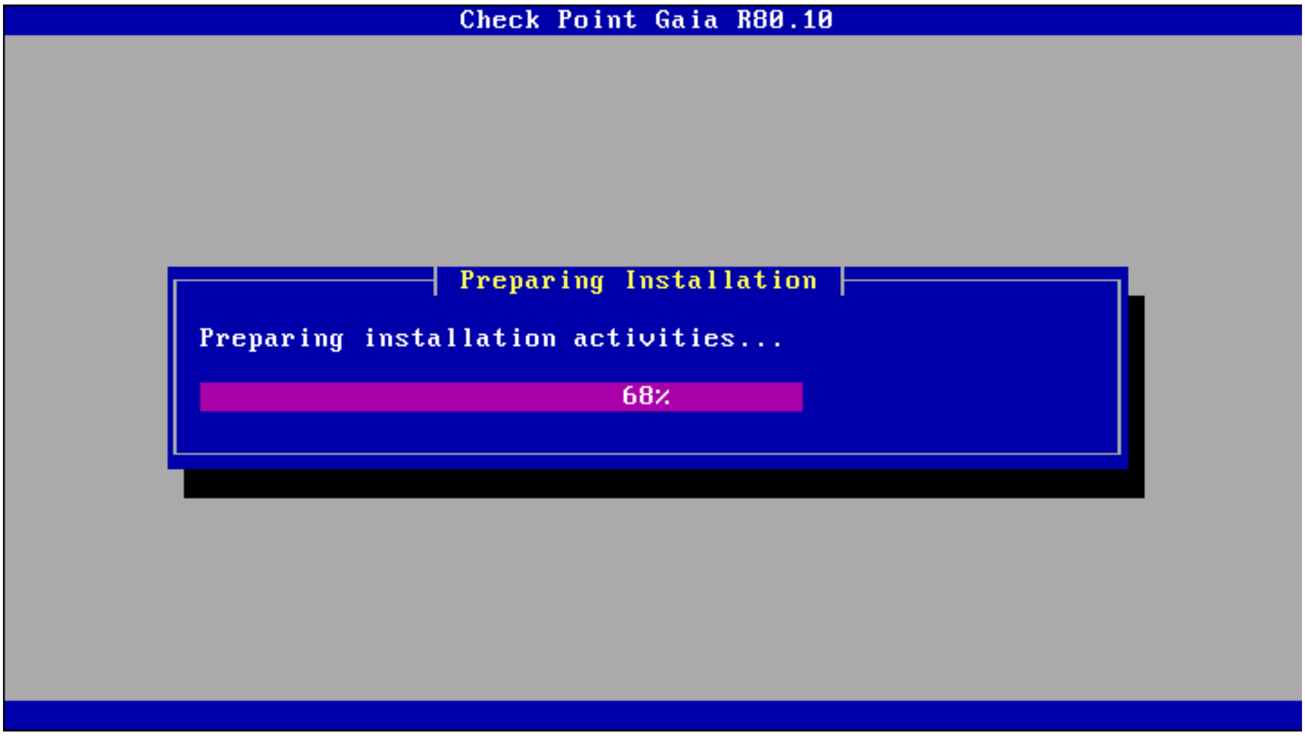
Check Point Gaia R80.10

Confirmation

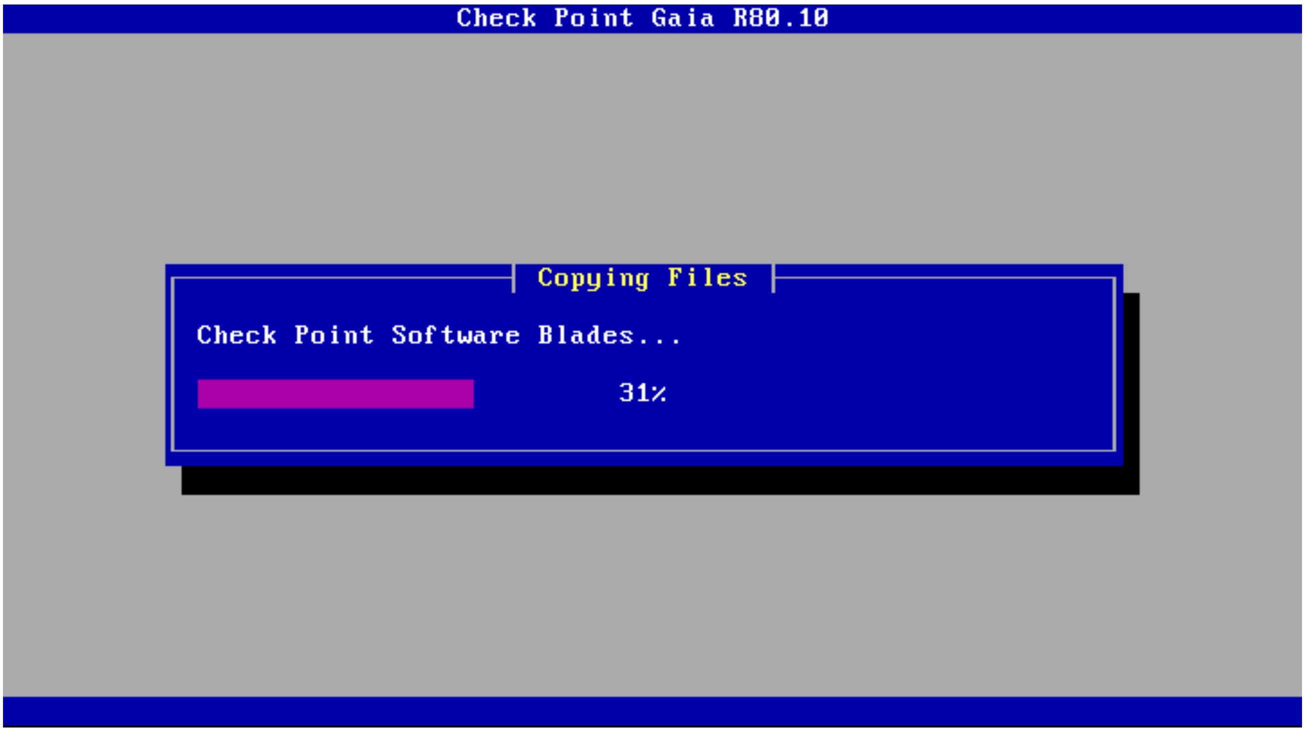
The next stage of the installation process will format all your hard drives.

Are you sure you want to continue?

You will see the status screens as installation progresses…

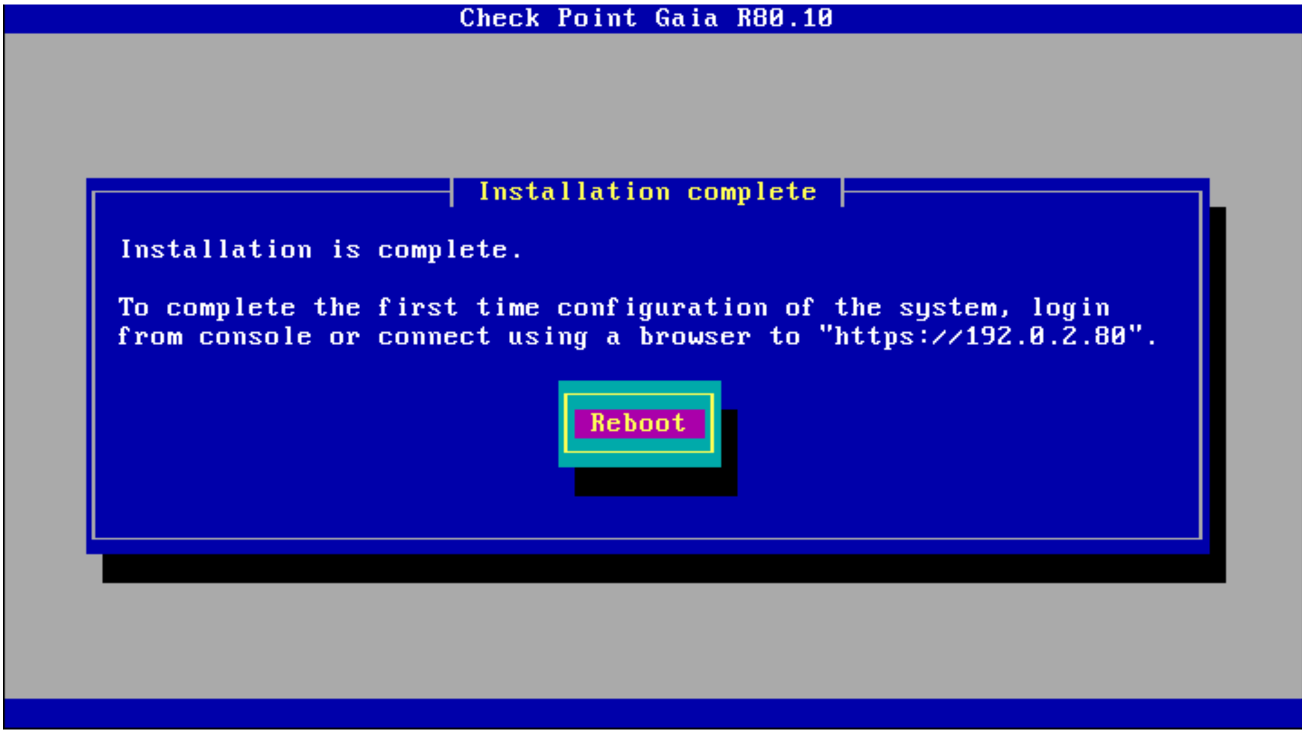


```
Check Point Gaia R80.10

Preparing Installation

Preparing installation activities...

68%
```



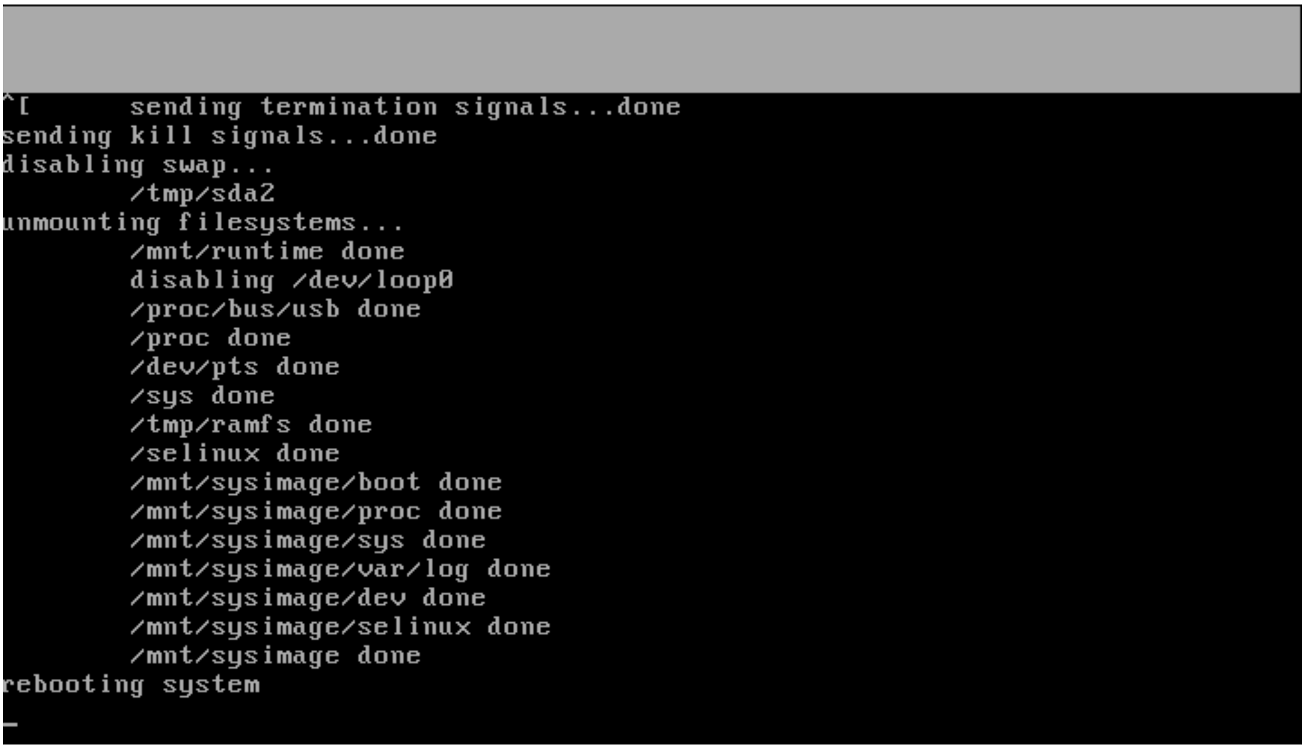
```
Check Point Gaia R80.10

Copying Files

Check Point Software Blades...

31%
```

Hit **ENTER** to reboot the system.



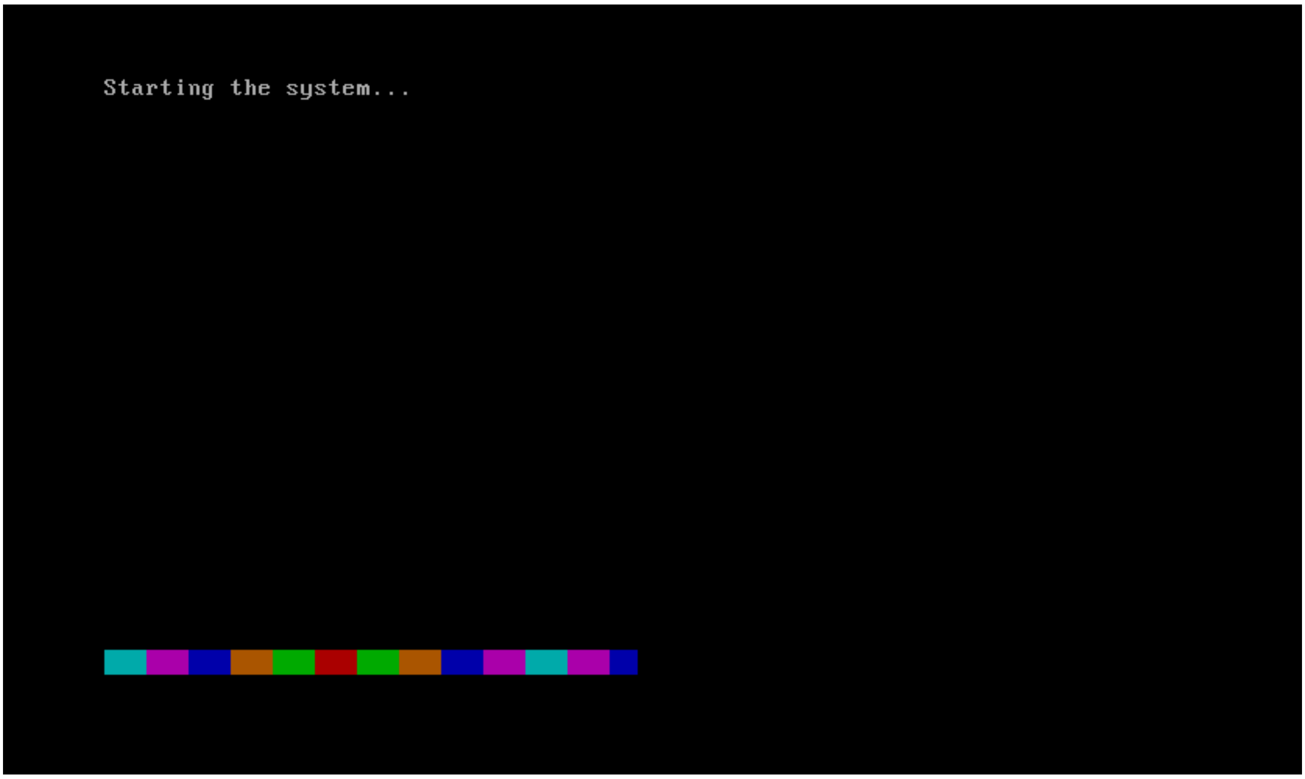
```
Check Point Gaia R80.10

Installation complete

Installation is complete.

To complete the first time configuration of the system, login
from console or connect using a browser to "https://192.0.2.80".
```

You will see some messages scroll by as Gaia shuts down…



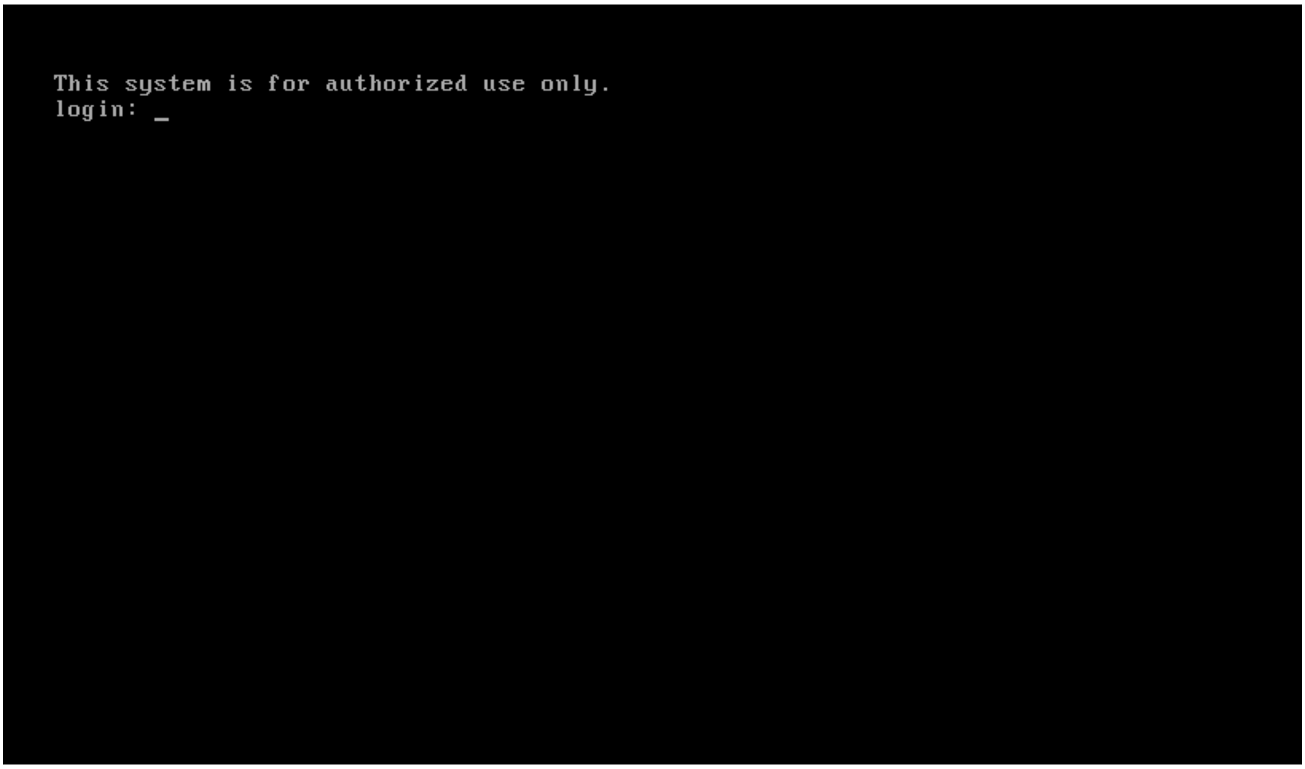
```
^[      sending termination signals...done
sending kill signals...done
disabling swap...
        /tmp/sda2
unmounting filesystems...
        /mnt/runtime done
        disabling /dev/loop0
        /proc/bus/usb done
        /proc done
        /dev/pts done
        /sys done
        /tmp/ramfs done
        /selinux done
        /mnt/sysimage/boot done
        /mnt/sysimage/proc done
        /mnt/sysimage/sys done
        /mnt/sysimage/var/log done
        /mnt/sysimage/dev done
        /mnt/sysimage/selinux done
        /mnt/sysimage done
rebooting system
_
```

You will see the progress bar as Gaia boots up…



```
Starting the system...
```

Hit **TAB** to highlight **OK.** Hit **ENTER** to continue.

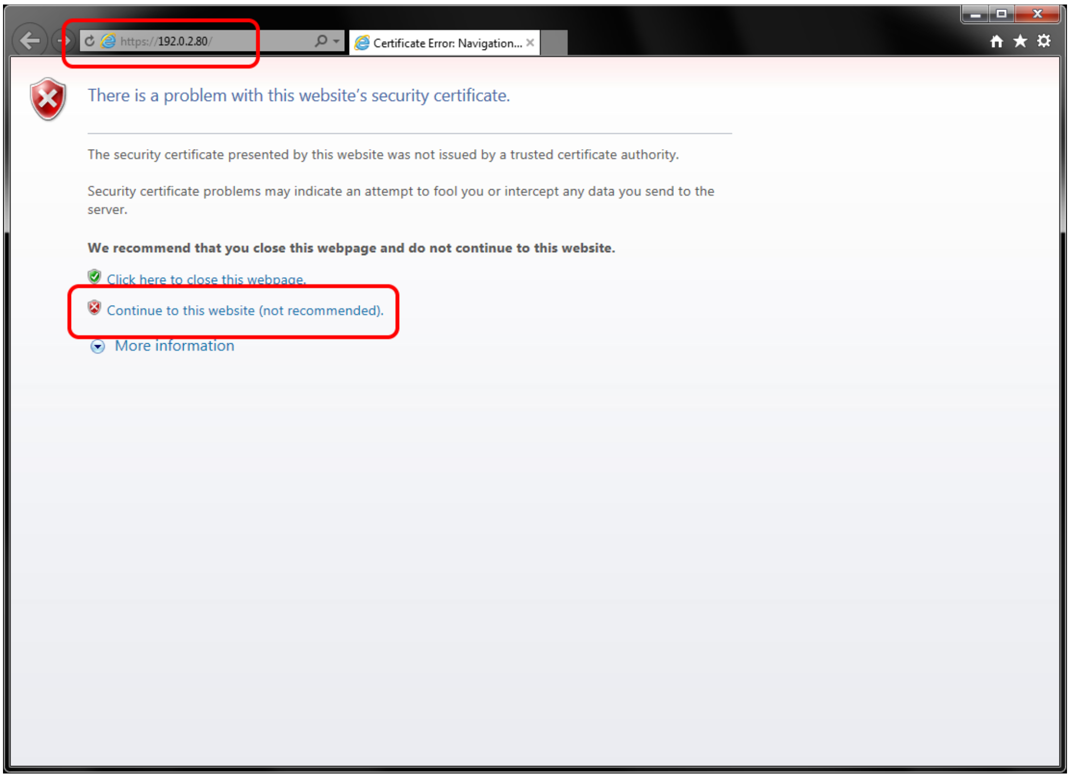


```
This system is for authorized use only.
login: _
```

You are now ready to move on to the **First Time Wizard** section…

GAIA First Time Wizard

Point your web browser to https://192.0.2.80. You will receive a warning for the self-signed certificate used for the SSL connection. Click on “Continue to the…”



There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

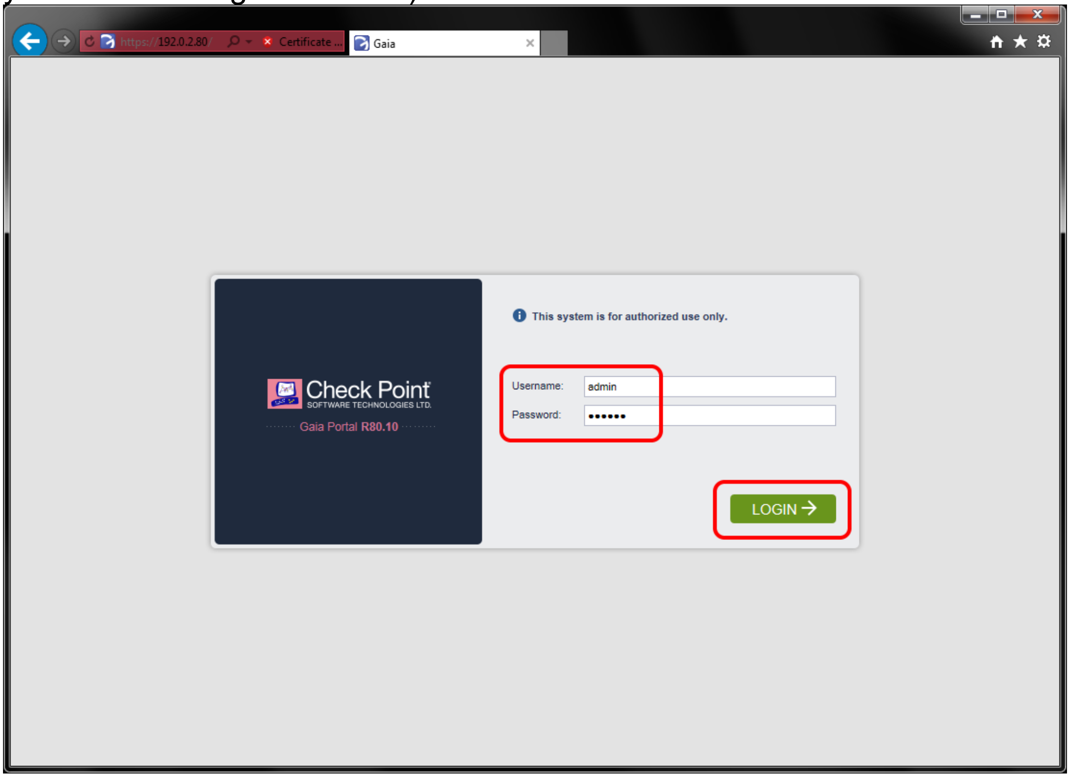
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Enter “admin” for the username, and “vpn123” for the password (or the password you chose during installation). Click **LOGIN**.

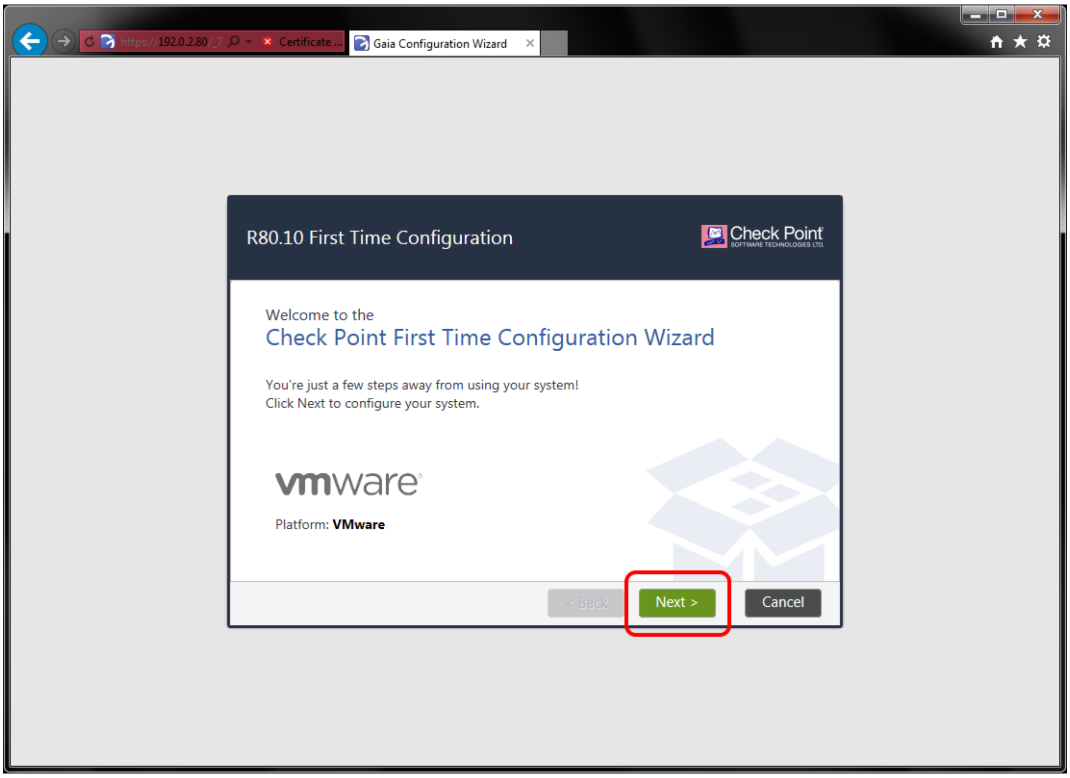


This system is for authorized use only.

Username: admin

Password: ••••••

If this is the first time you have connected to the WebUI (aka Gaia Portal), the First Time Wizard will begin. Click **Next** to continue.



R80.10 First Time Configuration

Welcome to the

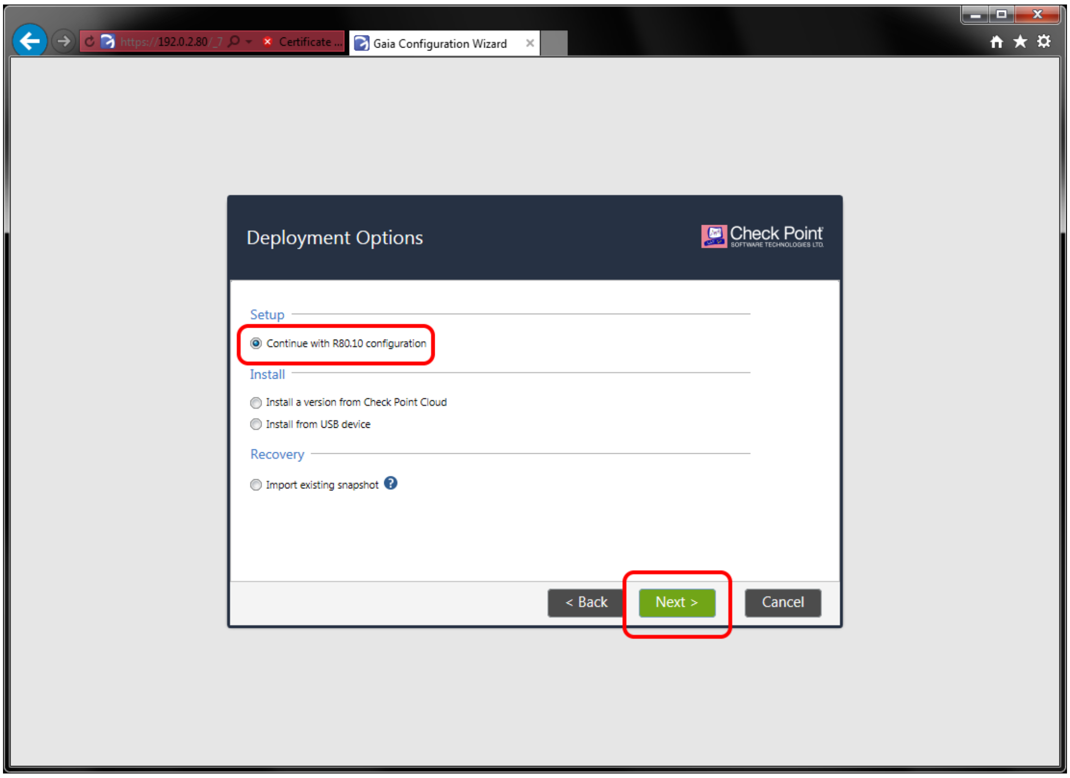
Check Point First Time Configuration Wizard

You're just a few steps away from using your system!
Click Next to configure your system.

Platform: **VMware**

Gaia Configuration Wizard
Certificate ...
Check Point SOFTWARE TECHNOLOGIES LTD.
vmware
< Back
Next >
Cancel

Select “Continue with R80.10 configuration” and click **Next**.



Deployment Options

Setup

● Continue with R80.10 configuration

Install

○ Install a version from Check Point Cloud

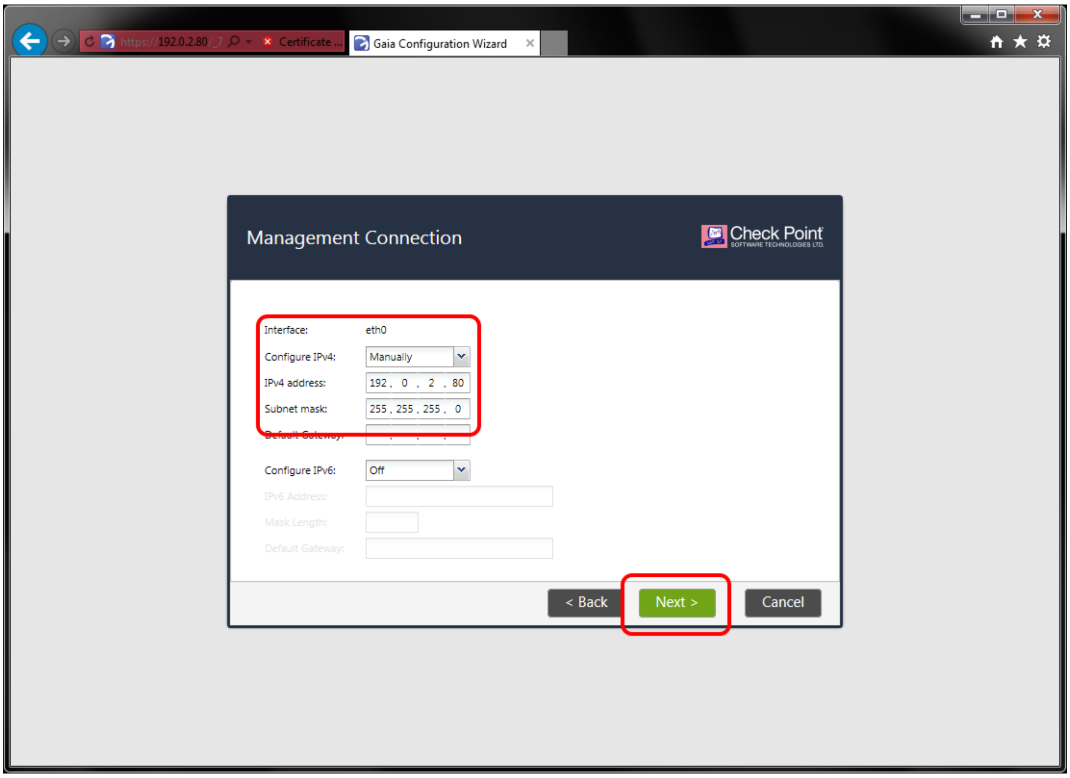
○ Install from USB device

Recovery

○ Import existing snapshot

Gaia Configuration Wizard
Certificate ...
Check Point SOFTWARE TECHNOLOGIES LTD.
< Back
Next >
Cancel

Leave the default IP address information and click **Next**.


https://192.0.2.80/
Certificate ...
Gaia Configuration Wizard
Check Point SOFTWARE TECHNOLOGIES LTD.
< Back
Next >
Cancel

Management Connection

Interface: eth0

Configure IPv4: Manually

IPv4 address: 192 . 0 . 2 . 80

Subnet mask: 255 . 255 . 255 . 0

Default Gateway: . . .

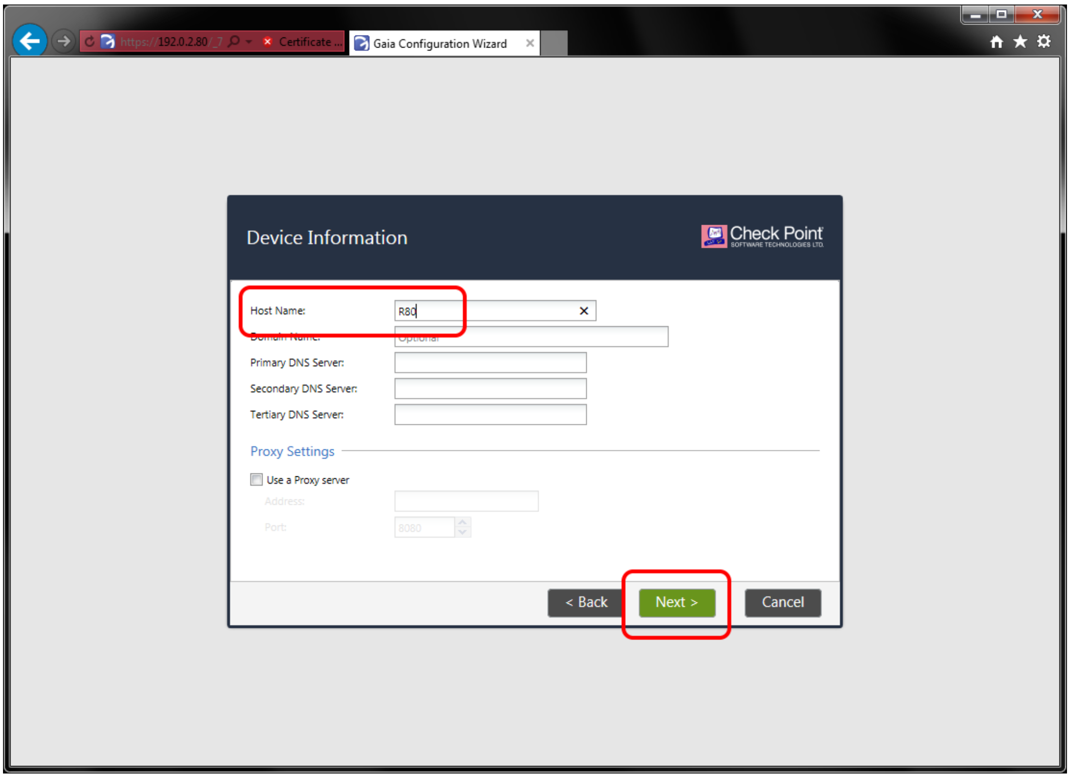
Configure IPv6: Off

IPv6 Address:

Mask Length:

Default Gateway:

Type in “R80” for the Hostname and click **Next**.


https://192.0.2.80/
Certificate ...
Gaia Configuration Wizard
Check Point SOFTWARE TECHNOLOGIES LTD.
< Back
Next >
Cancel

Device Information

Host Name: R80

Domain Name: Optional

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

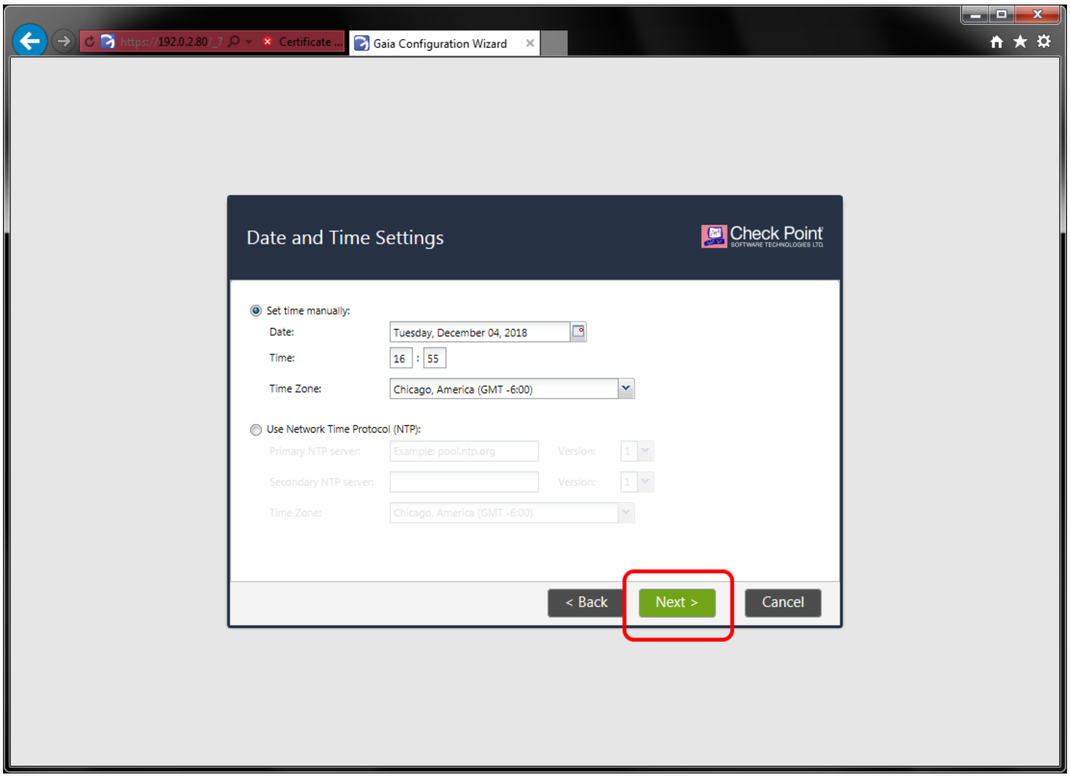
Proxy Settings

□ Use a Proxy server

Address:

Port: 8080

Leave the default Time and Date settings and click **Next**.



Date and Time Settings

● Set time manually:

Date: Tuesday, December 04, 2018

Time: 16 : 55

Time Zone: Chicago, America (GMT -6:00)

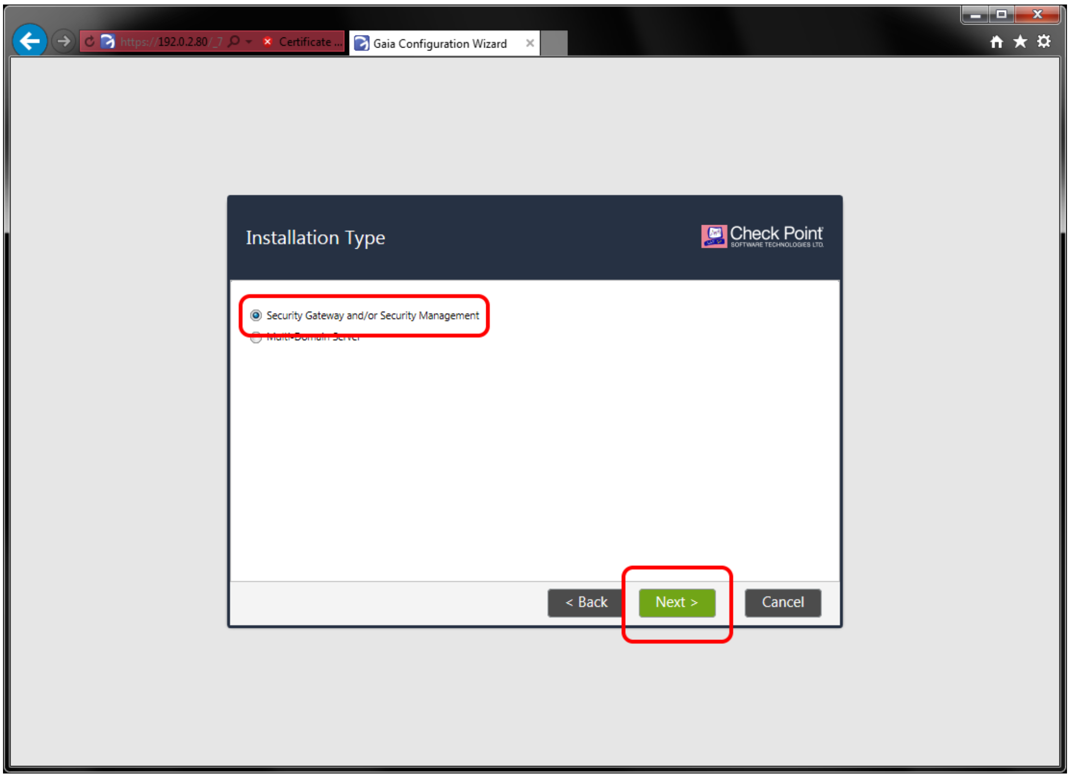
○ Use Network Time Protocol (NTP):

Primary NTP server: Example: pool.ntp.org Version: 1

Secondary NTP server: Version: 1

Time Zone: Chicago, America (GMT -6:00)

Make sure “Security Gateway and/or Security Management” is selected and click **Next**.

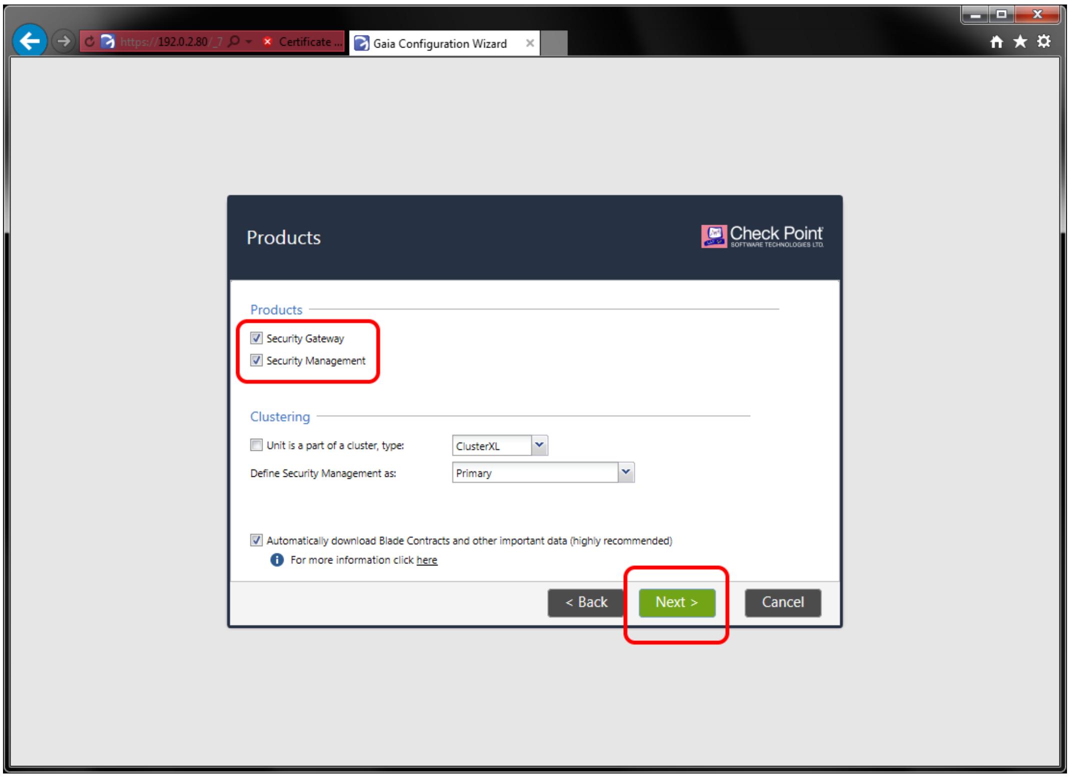


Installation Type

● Security Gateway and/or Security Management

○ Multi-Domain Server

Make sure both “Security Gateway” and “Security Management” are selected and click **Next**.



Products

Products

☑ Security Gateway

☑ Security Management

Clustering

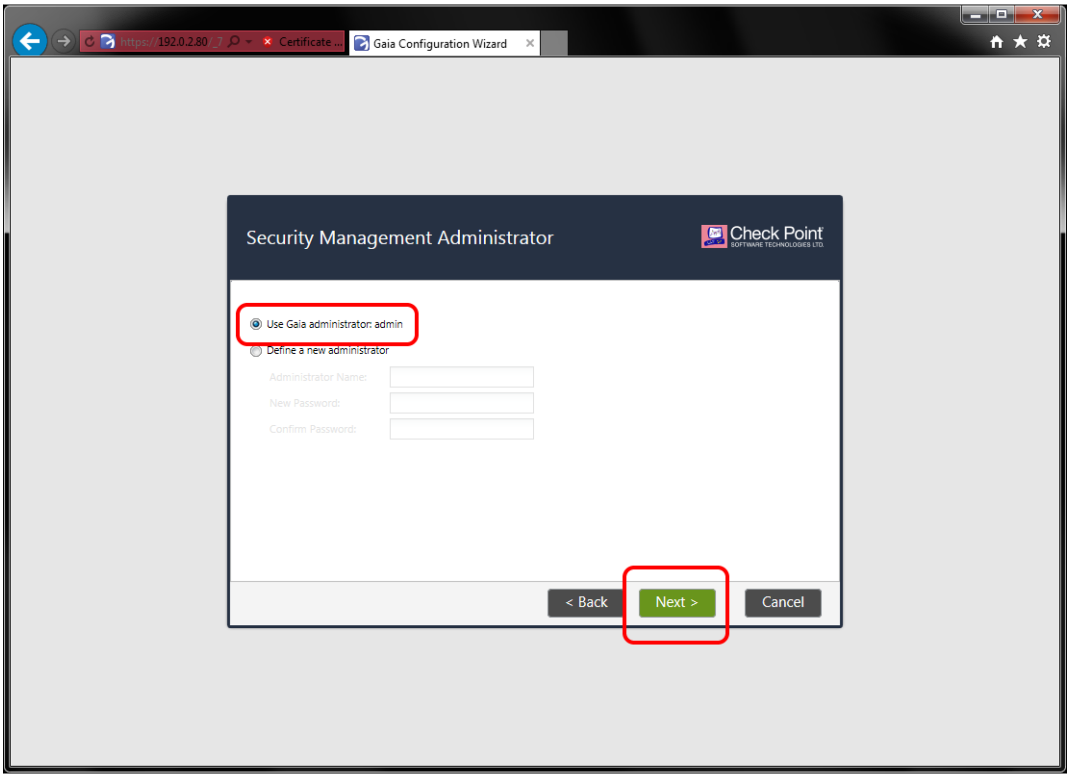
□ Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

☑ Automatically download Blade Contracts and other important data (highly recommended)

For more information click here

Leave “Use Gaia administrator” and click **Next**.



Security Management Administrator

● Use Gaia administrator: admin

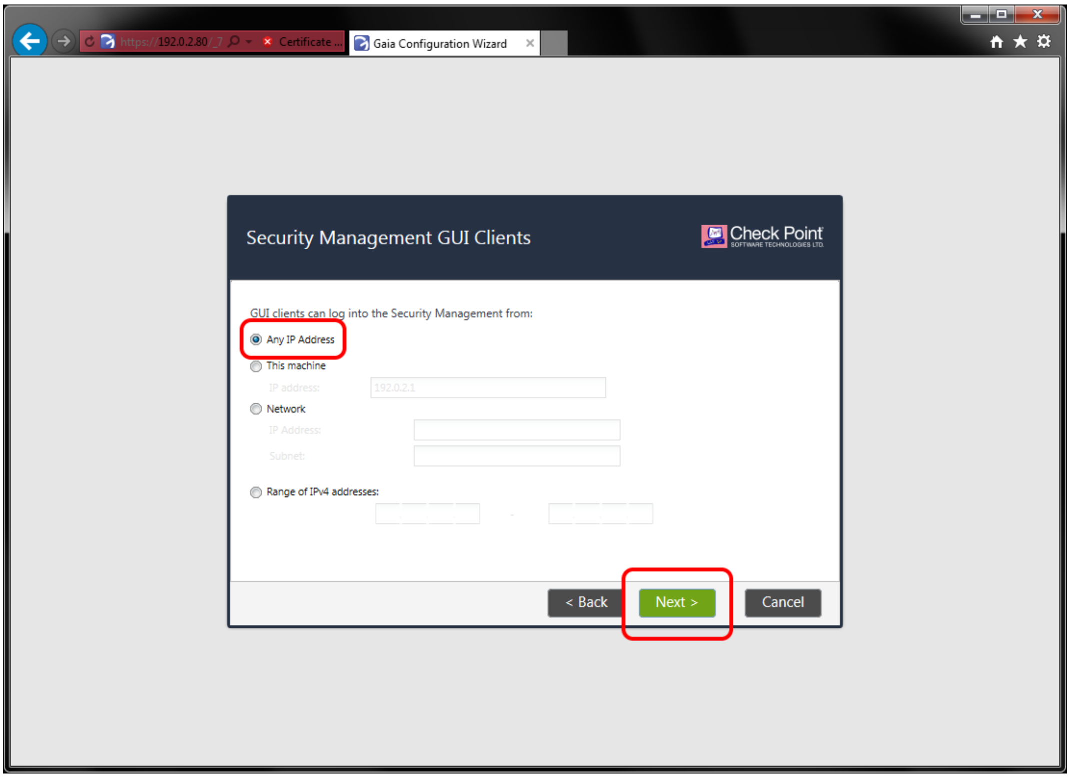
○ Define a new administrator

Administrator Name:

New Password:

Confirm Password:

Choose “Any IP Address” and click **Next**.



Security Management GUI Clients

GUI clients can log into the Security Management from:

● Any IP Address

○ This machine

IP address: 192.0.2.1

○ Network

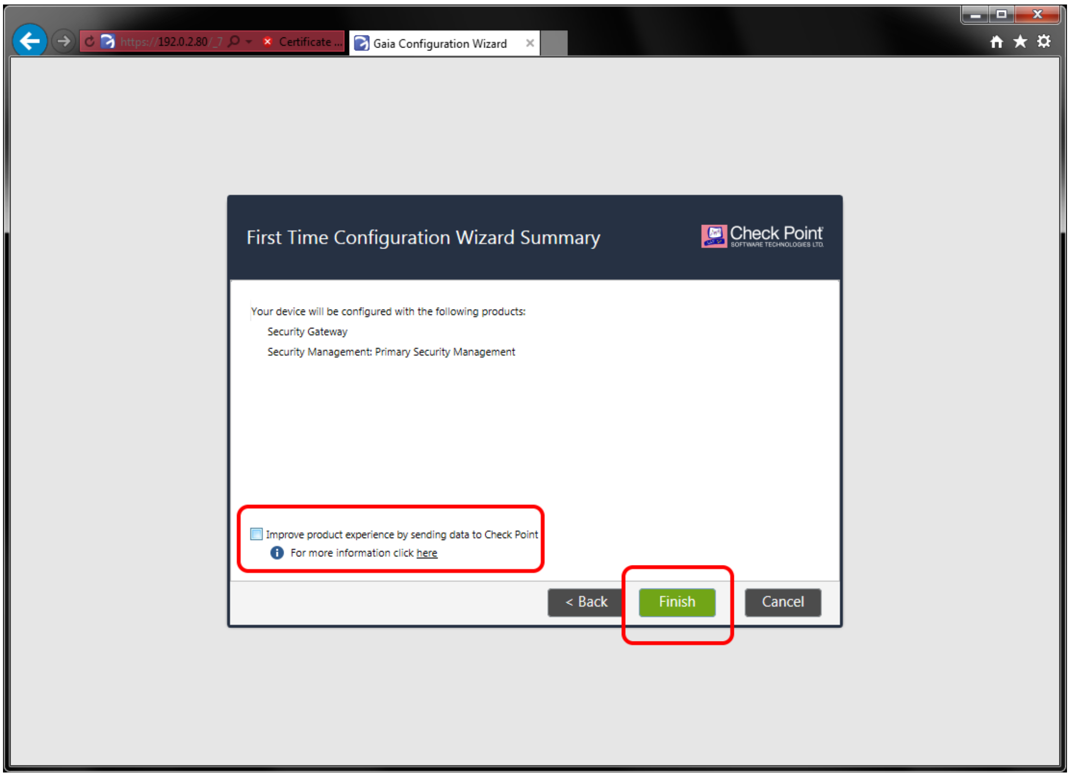
IP Address:

Subnet:

○ Range of IPv4 addresses:

< Back | Next > | Cancel

Un-check “Improve product experience by sending…” and click **Next**.



First Time Configuration Wizard Summary

Your device will be configured with the following products:

Security Gateway

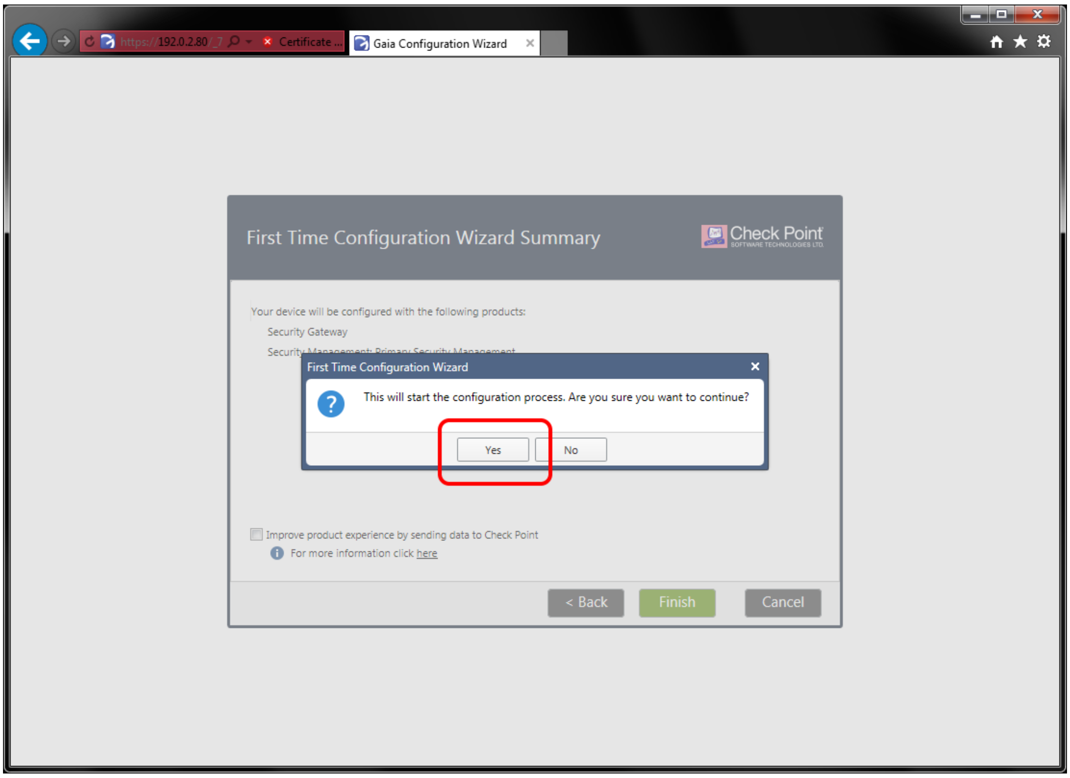
Security Management: Primary Security Management

□ Improve product experience by sending data to Check Point

For more information click here

< Back | Finish | Cancel

Click **Yes** to confirm configuration settings


Gaia Configuration Wizard
Check Point SOFTWARE TECHNOLOGIES LTD.
Yes
No
< Back
Finish
Cancel

First Time Configuration Wizard Summary

Your device will be configured with the following products:

Security Gateway

Security Management: Primary Security Management

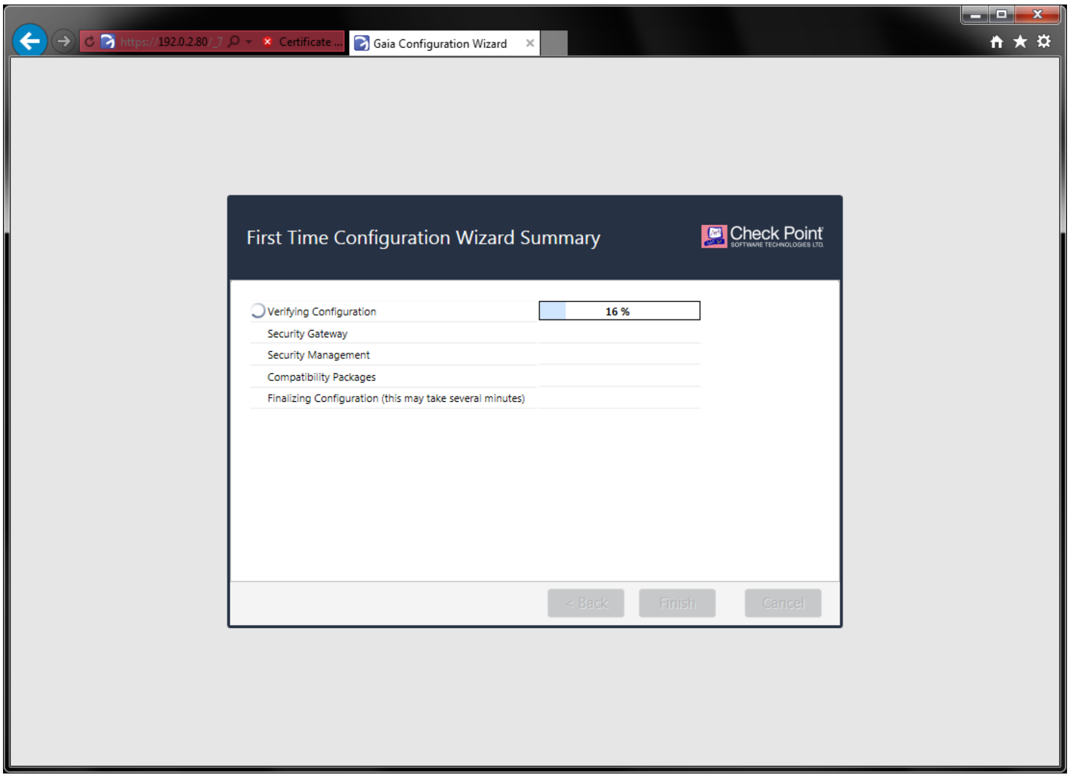
First Time Configuration Wizard

This will start the configuration process. Are you sure you want to continue?

□ Improve product experience by sending data to Check Point

For more information click here

You will see the status of the different steps progress…


Gaia Configuration Wizard
Check Point SOFTWARE TECHNOLOGIES LTD.
< Back
Finish
Cancel

First Time Configuration Wizard Summary

Verifying Configuration 16 %

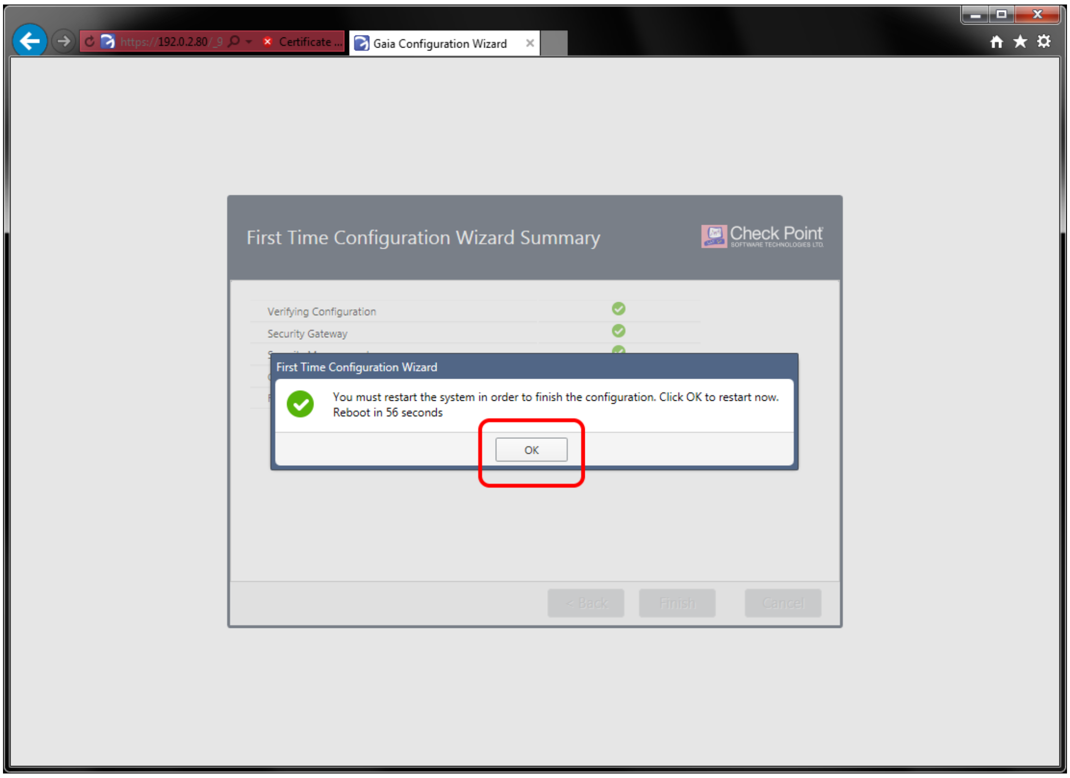
Security Gateway

Security Management

Compatibility Packages

Finalizing Configuration (this may take several minutes)

You will see a pop notification indicating that the wizard has completed. Click **OK** to reboot the system.



https://192.0.2.80/_9
Certificate ...
Gaia Configuration Wizard
Check Point SOFTWARE TECHNOLOGIES LTD.
< Back
Finish
Cancel

First Time Configuration Wizard Summary

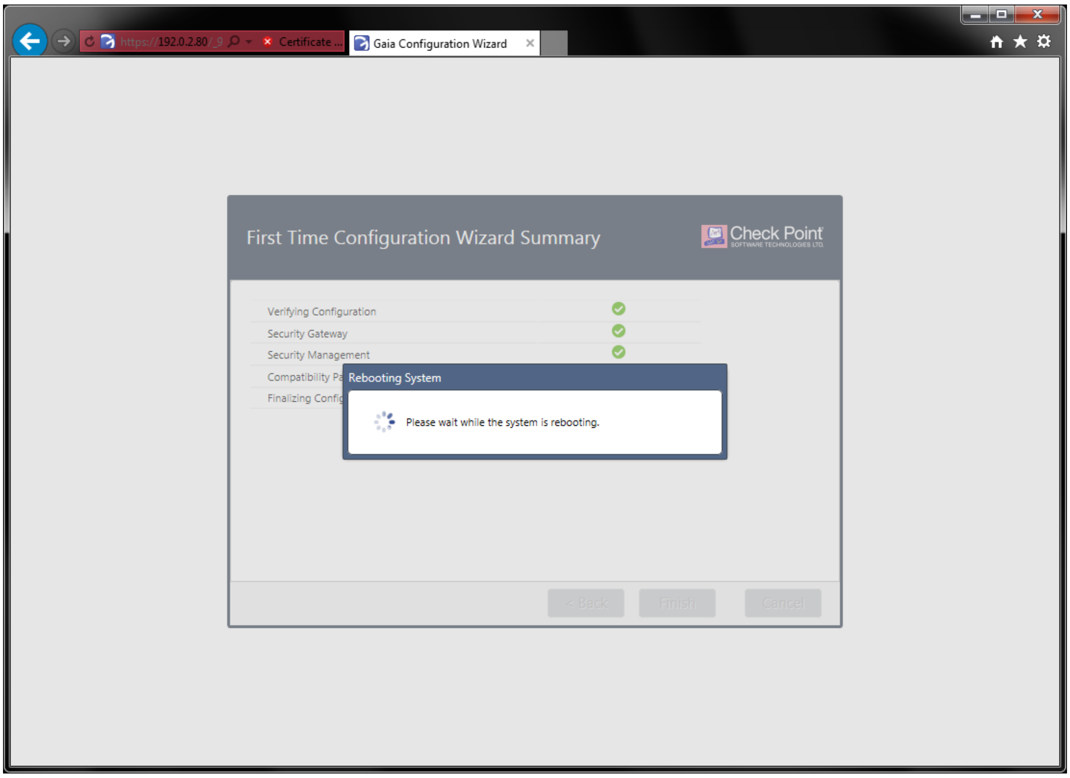
Verifying Configuration ✓
Security Gateway ✓

First Time Configuration Wizard

You must restart the system in order to finish the configuration. Click OK to restart now.
Reboot in 56 seconds

OK

Status of the reboot appears…



https://192.0.2.80/_9
Certificate ...
Gaia Configuration Wizard
Check Point SOFTWARE TECHNOLOGIES LTD.
< Back
Finish
Cancel

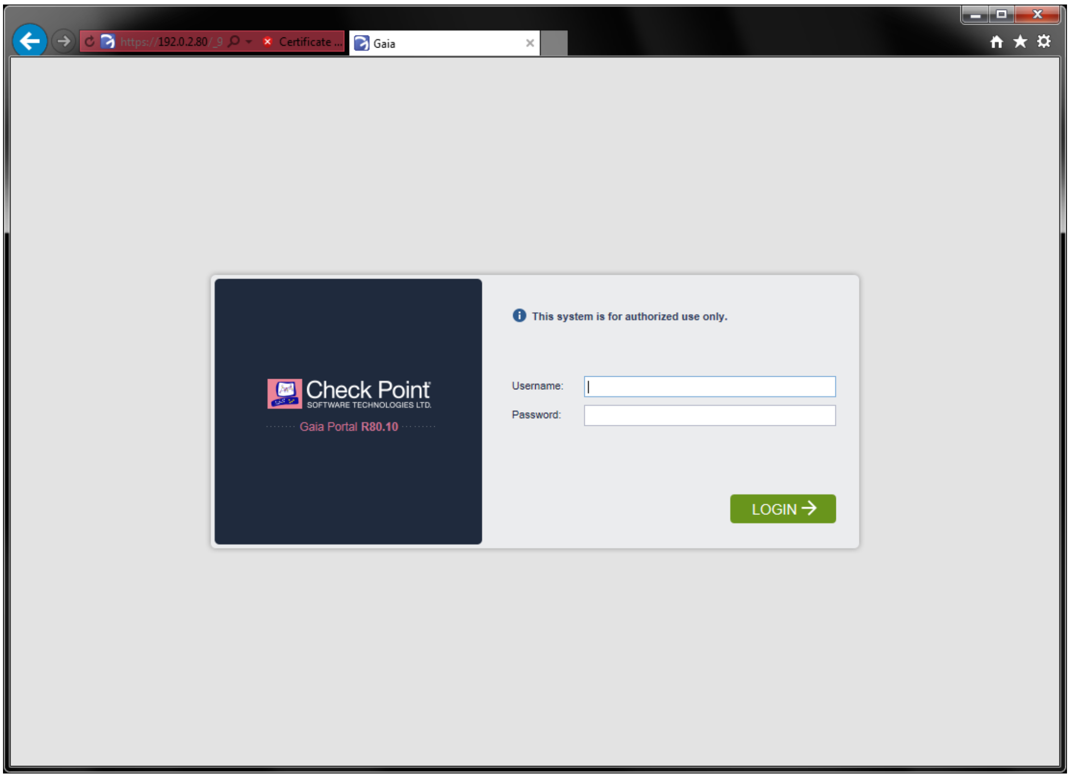
First Time Configuration Wizard Summary

Verifying Configuration ✓
Security Gateway ✓
Security Management ✓
Compatibility Pa
Finalizing Config

Rebooting System

Please wait while the system is rebooting.

When you see the login page load, your Check Point has rebooted.



This system is for authorized use only.

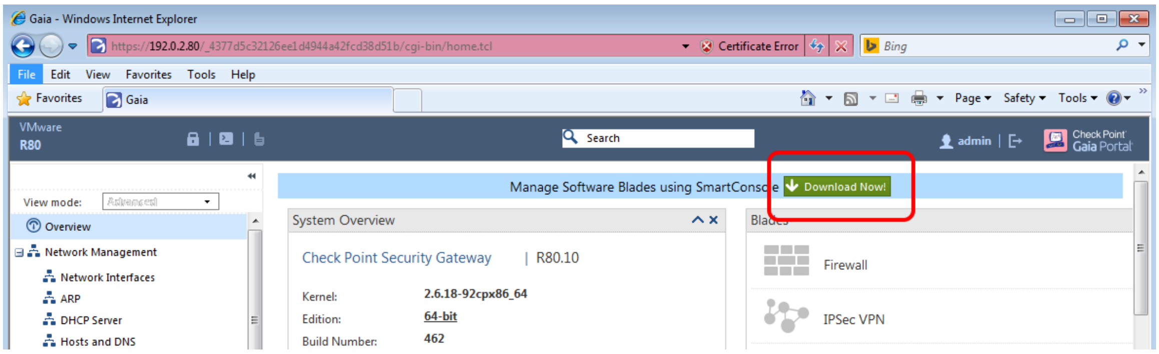
Username:

Password:

You can log into the WebUI again to look at the various configuration options. Remember, the settings are for the operating system only. The Security Policy configuration is only configured through SmartConsole.

R80.10 SmartConsole Installation

If you did not download SmartConsole from Support Center, you can download it directly from the WebUI. Go to the Overview section and look for the green **Download Now** link.



Manage Software Blades using SmartConsole Download Now!

System Overview

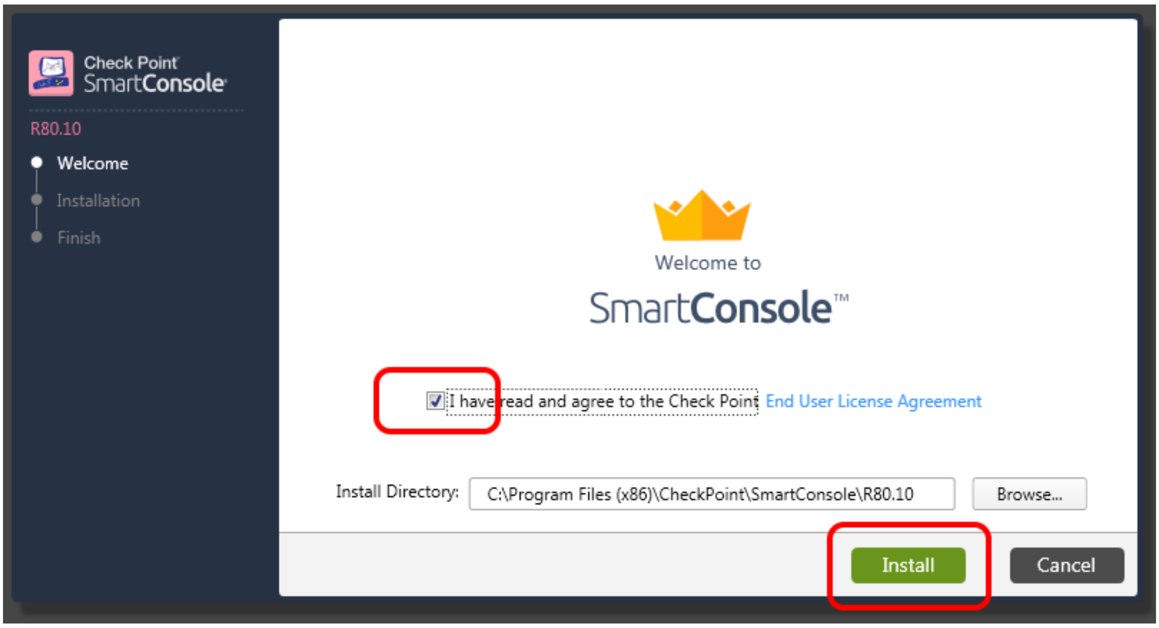
Check Point Security Gateway | R80.10

Kernel: 2.6.18-92cpx86_64

Edition: 64-bit

Build Number: 462

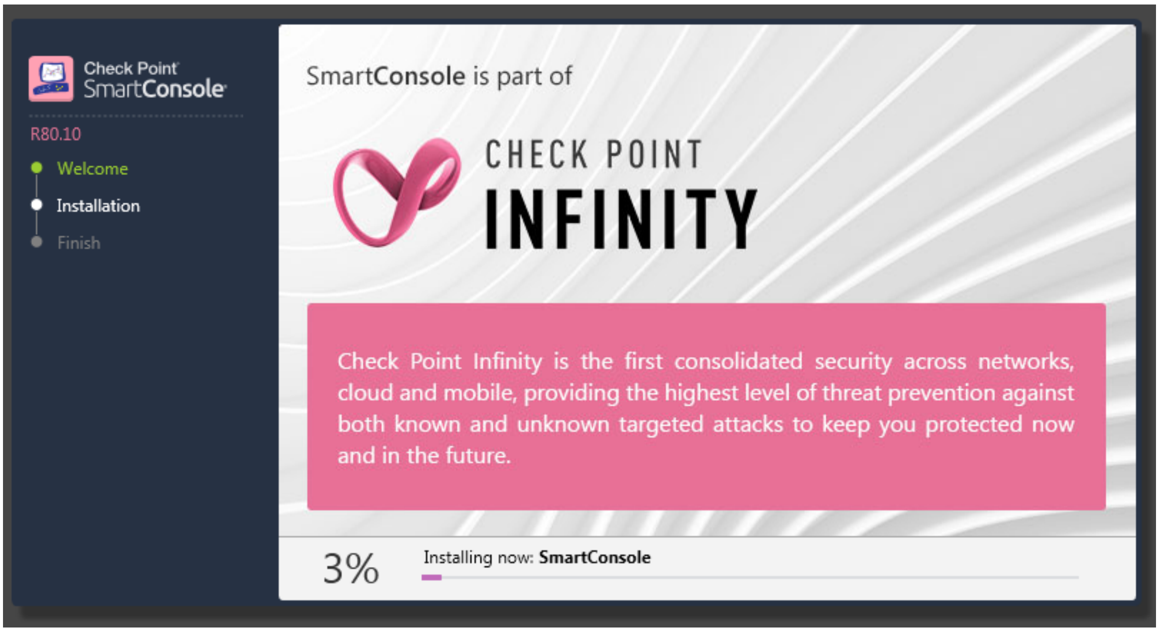
Double-click the installation package you downloaded. Check the box to indicate that you "…have read and agree to the Check Point…" EULA. Click **Install** to continue.



☑ I have read and agree to the Check Point End User License Agreement

Install Directory: C:\Program Files (x86)\CheckPoint\SmartConsole\R80.10

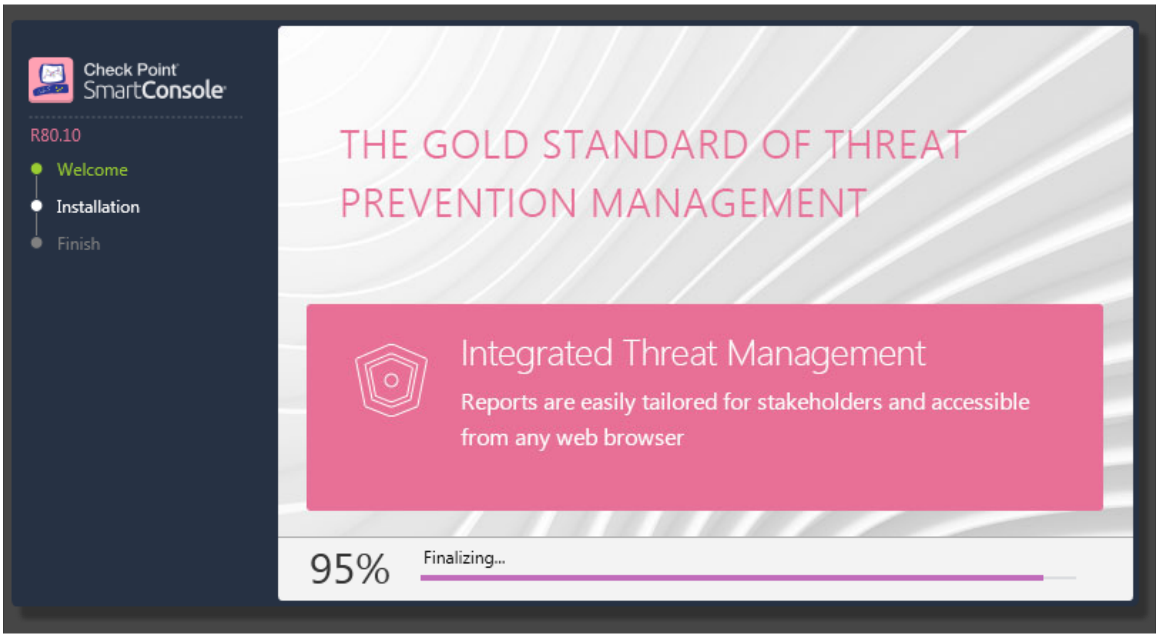
You will see the progress indicators as the software installs.



Check Point Infinity is the first consolidated security across networks, cloud and mobile, providing the highest level of threat prevention against both known and unknown targeted attacks to keep you protected now and in the future.

3% Installing now: SmartConsole

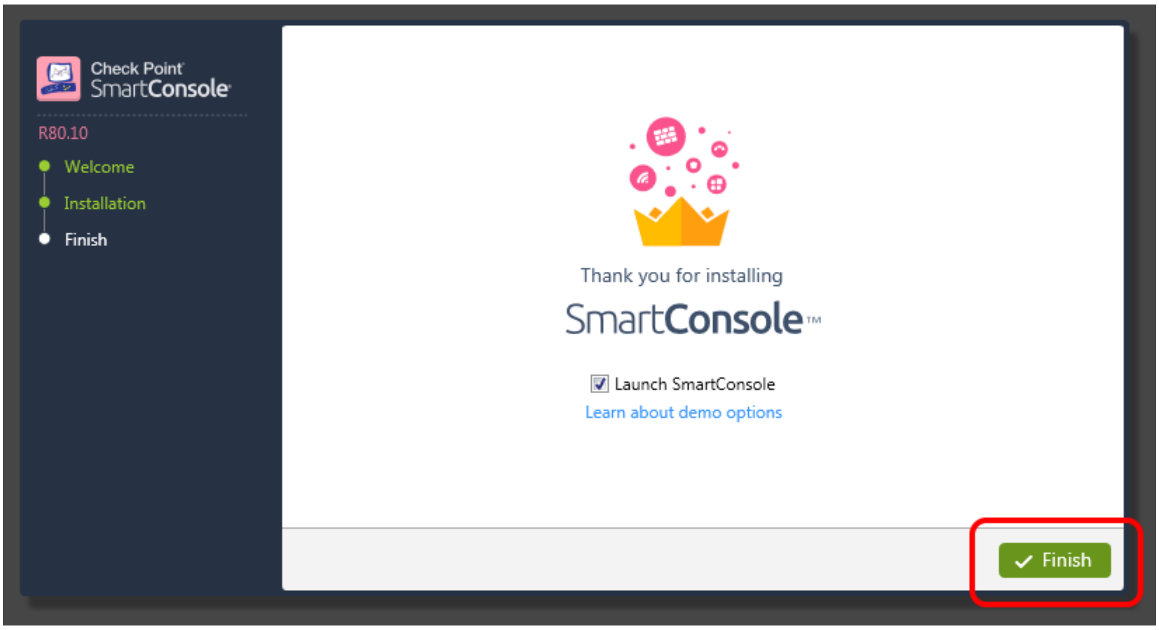
You will see the progress indicators as the software installs.


Check Point SmartConsole
R80.10
Welcome
Installation
Finish
THE GOLD STANDARD OF THREAT PREVENTION MANAGEMENT
Integrated Threat Management

Reports are easily tailored for stakeholders and accessible from any web browser

95% Finalizing...

When the installation completes, you have an option to “Launch SmartConsole” when you click **Finish**.



Thank you for installing

SmartConsole™

☑ Launch SmartConsole

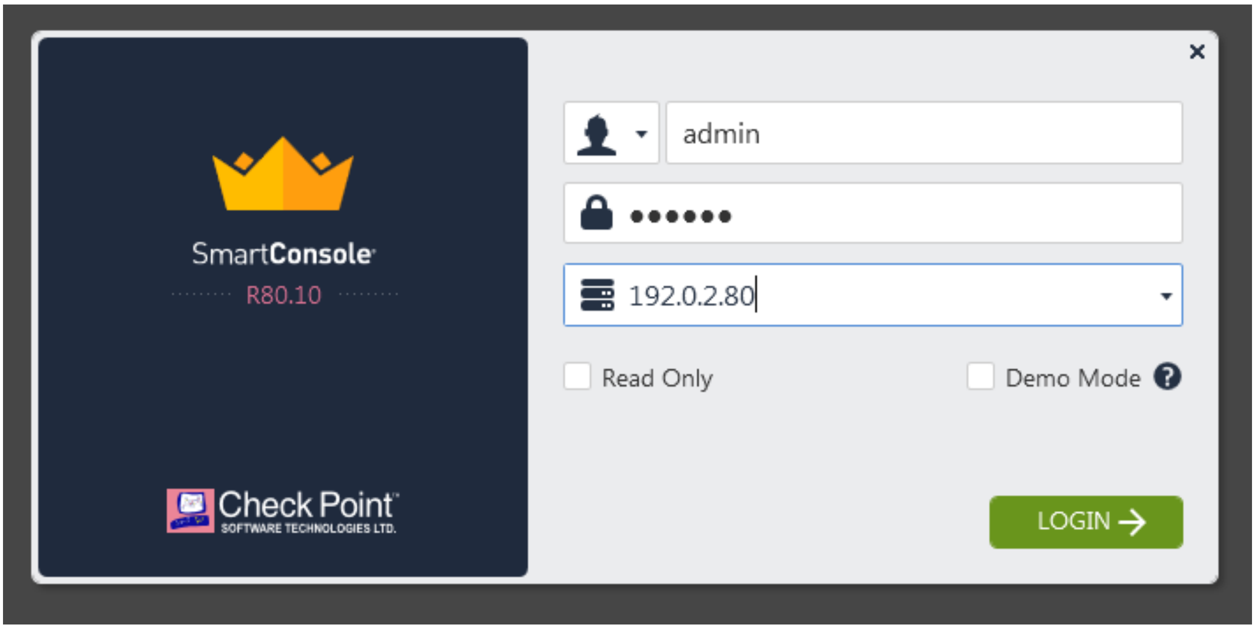
Learn about demo options

R80.10 Hands-on Demo

Launching SmartConsole

Double-Click the SmartConsole shortcut on the desktop (or in the Start menu > All Programs > Check Point SmartConsole R80.10 > Check Point SmartConsole R80.10).

Enter your credentials (admin/vpn123) can click **LOGIN**.



admin

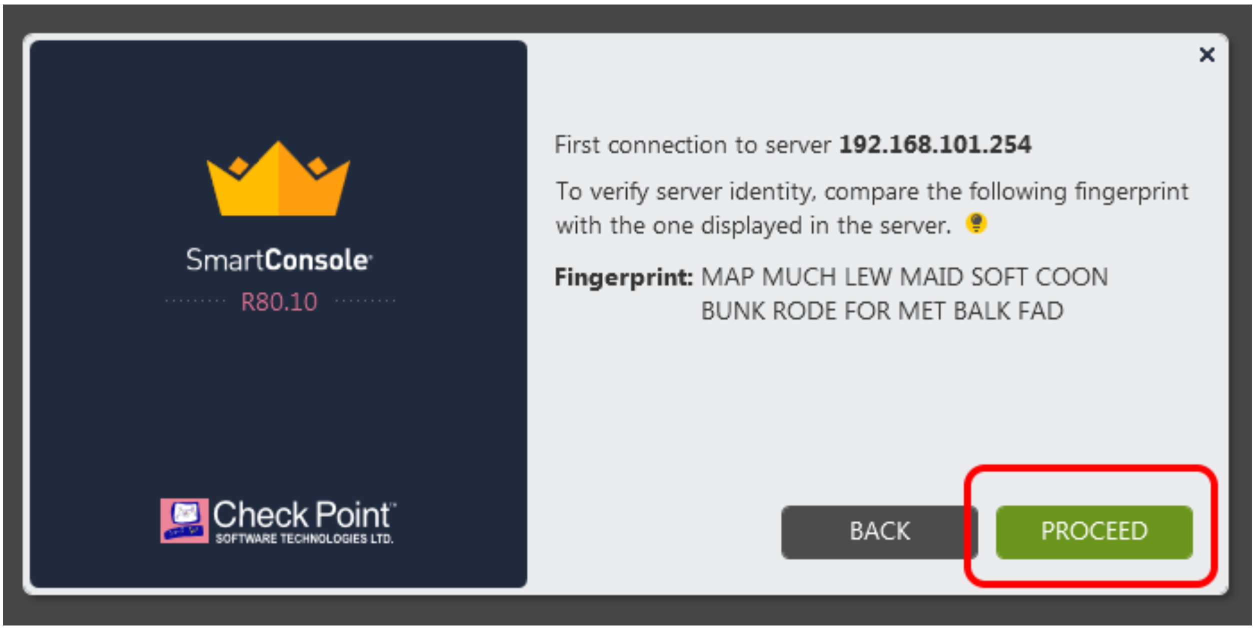
••••••

192.0.2.80

□ Read Only

□ Demo Mode

The first time you connect, you will see a pop with a Fingerprint verifying the identity of your Security Management Server. Click **Proceed**.



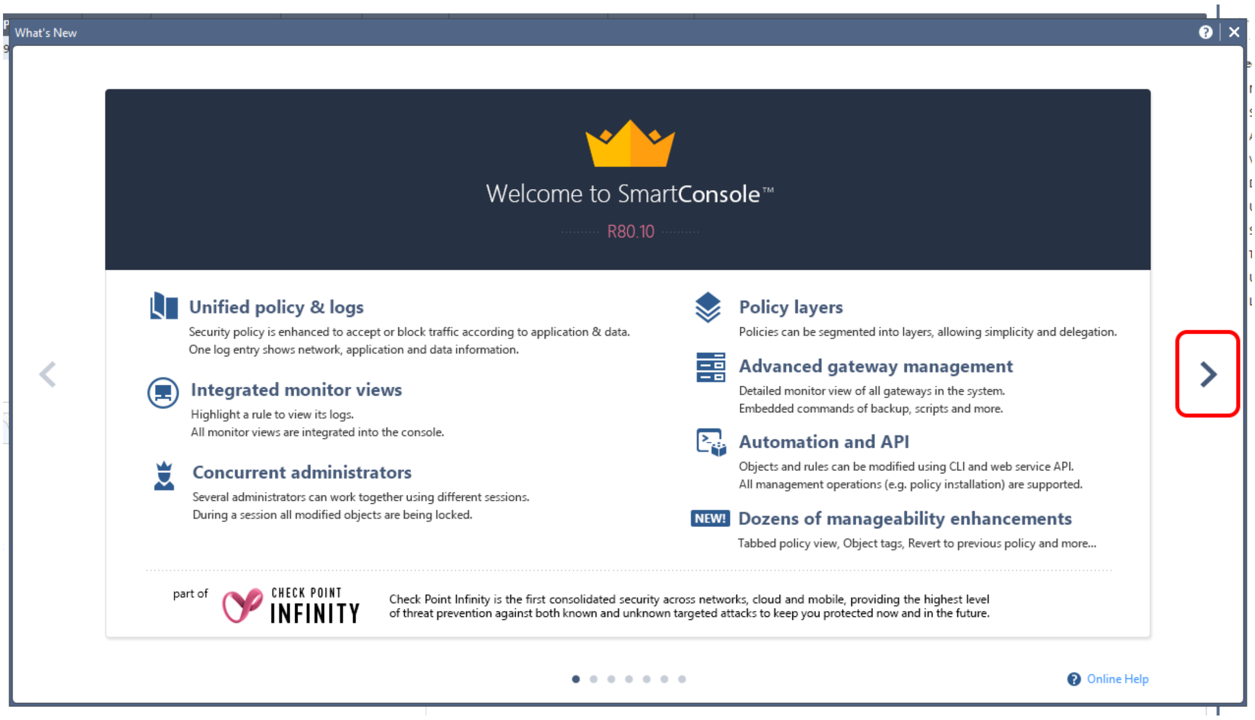
First connection to server **192.168.101.254**

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

Fingerprint: MAP MUCH LEW MAID SOFT COON BUNK RODE FOR MET BALK FAD

If this is the first time you have launched SmartConsole, the “Welcome to SmartConsole” screen will appear.

You can browse through the various pages to get a quick tour of the SmartConsole GUI’s layout using the arrows on the left and right of the pop-up screen. Close the pop-up to get into the main GUI when you are ready to continue.



Welcome to SmartConsole™

R80.10

Unified policy & logs
Security policy is enhanced to accept or block traffic according to application & data.
One log entry shows network, application and data information.

Integrated monitor views
Highlight a rule to view its logs.
All monitor views are integrated into the console.

Concurrent administrators
Several administrators can work together using different sessions.
During a session all modified objects are being locked.

Policy layers
Policies can be segmented into layers, allowing simplicity and delegation.

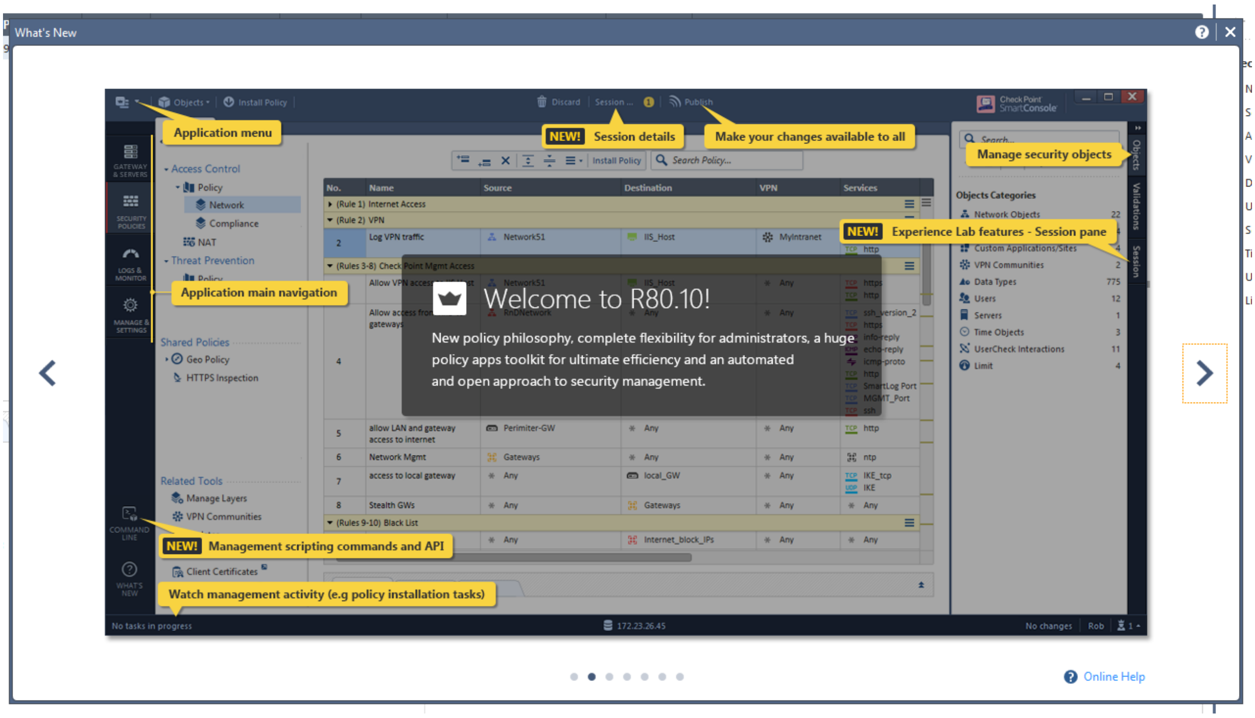
Advanced gateway management
Detailed monitor view of all gateways in the system.
Embedded commands of backup, scripts and more.

Automation and API
Objects and rules can be modified using CLI and web service API.
All management operations (e.g. policy installation) are supported.

NEW! **Dozens of manageability enhancements**
Tabbed policy view, Object tags, Revert to previous policy and more...

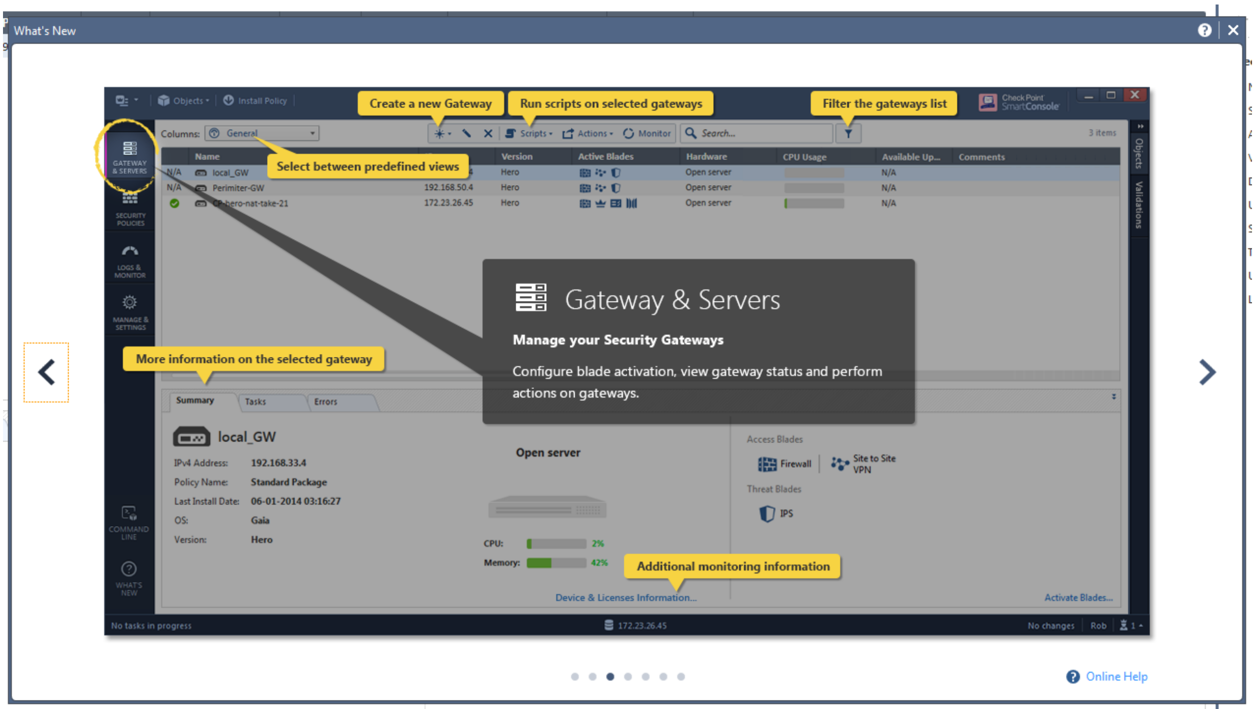
part of CHECK POINT INFINITY

Check Point Infinity is the first consolidated security across networks, cloud and mobile, providing the highest level of threat prevention against both known and unknown targeted attacks to keep you protected now and in the future.



Welcome to R80.10!

New policy philosophy, complete flexibility for administrators, a huge policy apps toolkit for ultimate efficiency and an automated and open approach to security management.



What's New

Create a new Gateway

Run scripts on selected gateways

Filter the gateways list

Select between predefined views

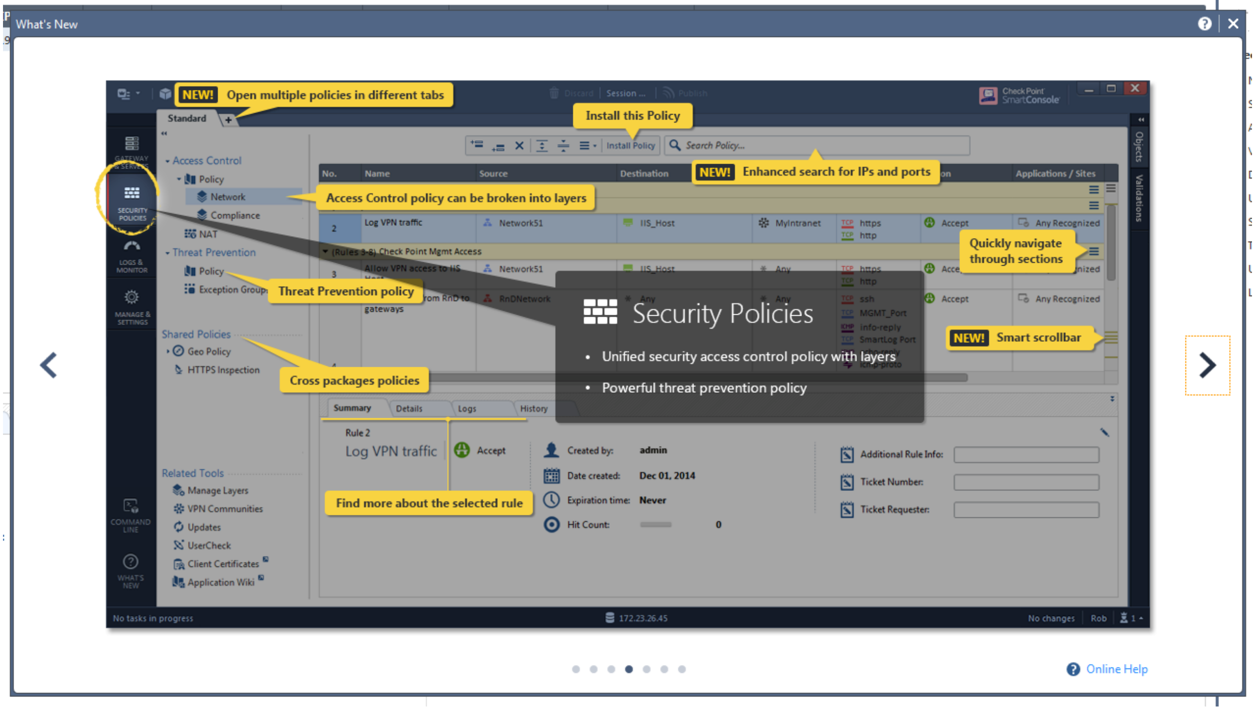
More information on the selected gateway

Additional monitoring information

Gateway & Servers

Manage your Security Gateways

Configure blade activation, view gateway status and perform actions on gateways.



What's New

NEW! Open multiple policies in different tabs

Install this Policy

NEW! Enhanced search for IPs and ports

Access Control policy can be broken into layers

Quickly navigate through sections

Threat Prevention policy

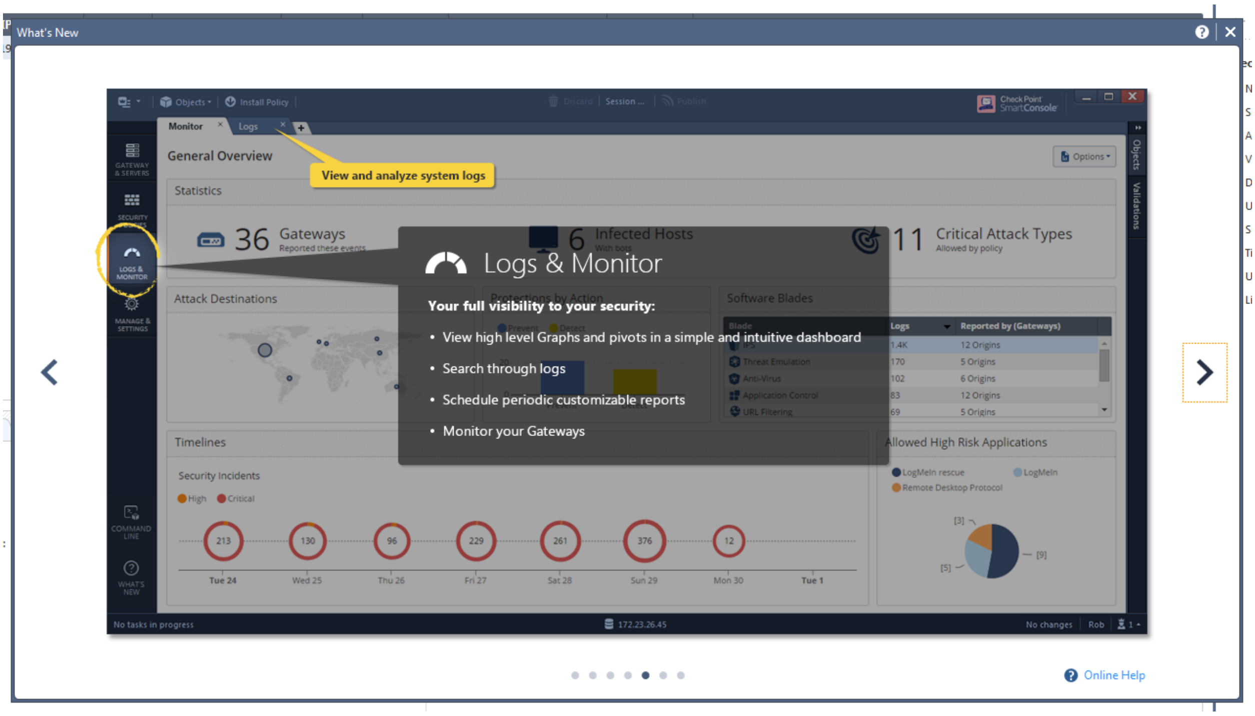
NEW! Smart scrollbar

Cross packages policies

Find more about the selected rule

Security Policies

- Unified security access control policy with layers
- Powerful threat prevention policy



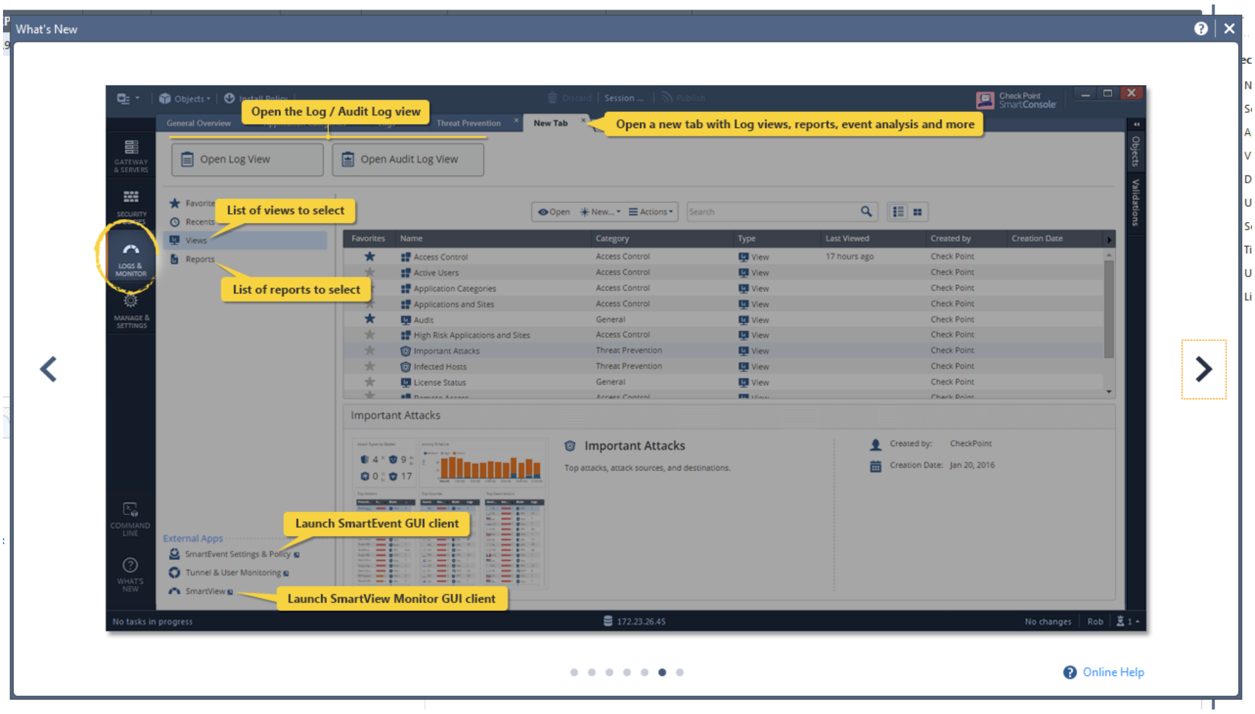
What's New

View and analyze system logs

Logs & Monitor

Your full visibility to your security:

- View high level Graphs and pivots in a simple and intuitive dashboard
- Search through logs
- Schedule periodic customizable reports
- Monitor your Gateways



What's New

Open the Log / Audit Log view

Open a new tab with Log views, reports, event analysis and more

List of views to select

List of reports to select

Favorites	Name	Category	Type	Last Viewed	Created by	Creation Date
★	Access Control	Access Control	View	17 hours ago	Check Point	
☆	Active Users	Access Control	View		Check Point	
☆	Application Categories	Access Control	View		Check Point	
☆	Applications and Sites	Access Control	View		Check Point	
★	Audit	General	View		Check Point	
☆	High Risk Applications and Sites	Access Control	View		Check Point	
☆	Important Attacks	Threat Prevention	View		Check Point	
☆	Infected Hosts	Threat Prevention	View		Check Point	
☆	License Status	General	View		Check Point	

Important Attacks

Important Attacks

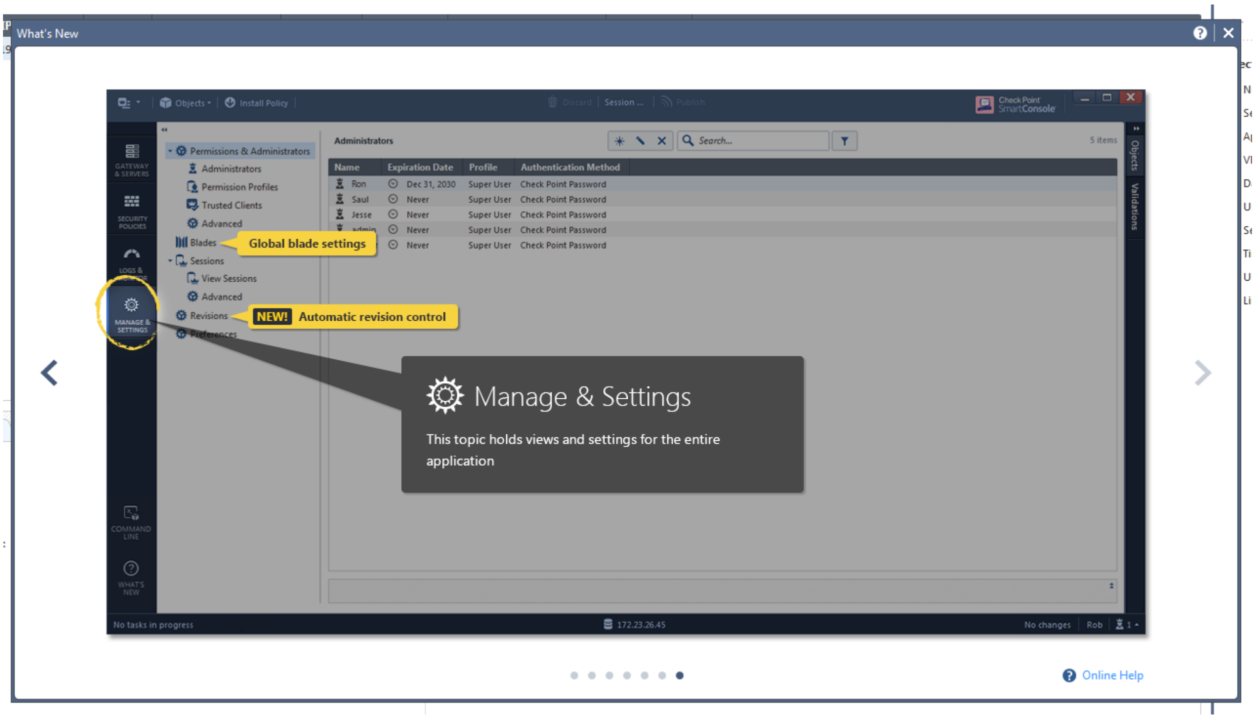
Top attacks, attack sources, and destinations.

Created by: CheckPoint

Creation Date: Jan 20, 2016

Launch SmartEvent GUI client

Launch SmartView Monitor GUI client



Administrators

Name	Expiration Date	Profile	Authentication Method
Ron	Dec 31, 2030	Super User	Check Point Password
Saul	Never	Super User	Check Point Password
Jesse	Never	Super User	Check Point Password
admin	Never	Super User	Check Point Password
	Never	Super User	Check Point Password

Global blade settings

NEW! Automatic revision control

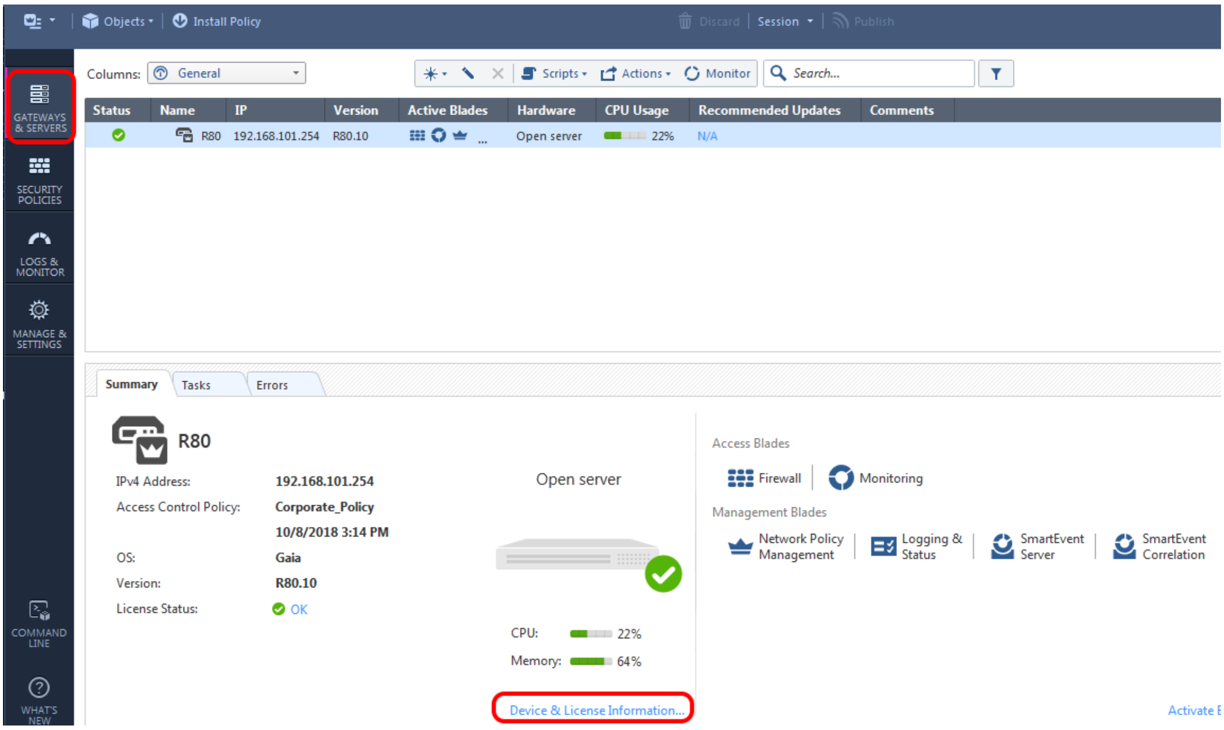
Manage & Settings

This topic holds views and settings for the entire application

No tasks in progress | 172.23.26.45 | No changes | Rob

Navigate the Four Main Tabs

The top tab is labeled “GATEWAYS & SERVERS”. You can view the status of your Check Point gateways and servers in this section.



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Comments
✓	R80	192.168.101.254	R80.10	...	Open server	22%	N/A	

R80

IPv4 Address: 192.168.101.254

Access Control Policy: Corporate_Policy
10/8/2018 3:14 PM

OS: Gaia

Version: R80.10

License Status: OK

Open server

CPU: 22%

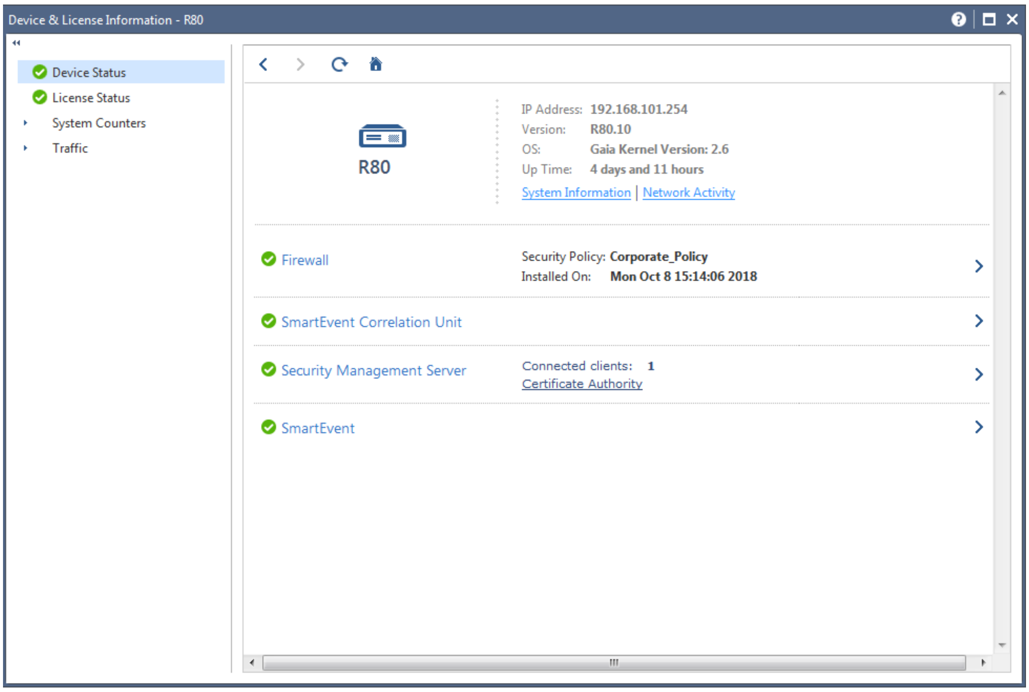
Memory: 64%

Device & License Information...

Access Blades: Firewall | Monitoring

Management Blades: Network Policy Management | Logging & Status | SmartEvent Server | SmartEvent Correlation

Click on the **Device & License Information** link near the bottom of the GUI. You can view information about Traffic, System Counters, License status, Hardware Health and more.



R80

IP Address: 192.168.101.254

Version: R80.10

OS: Gaia Kernel Version: 2.6

Up Time: 4 days and 11 hours

System Information | Network Activity

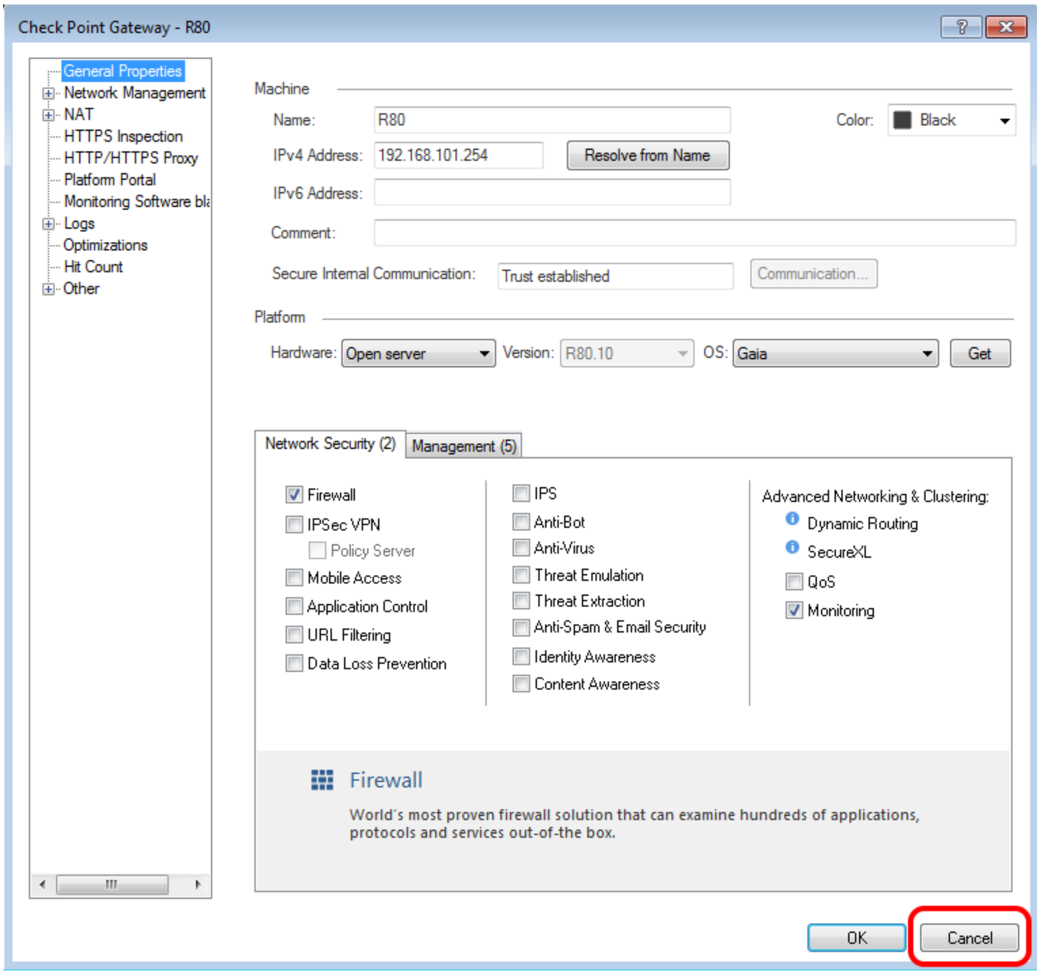
Firewall — Security Policy: Corporate_Policy; Installed On: Mon Oct 8 15:14:06 2018

SmartEvent Correlation Unit

Security Management Server — Connected clients: 1; Certificate Authority

SmartEvent

Double-click the Check Point entry in this list to see the Object Properties. Click **Cancel**.



Check Point Gateway - R80

- General Properties
- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- Monitoring Software bla
- Logs
- Optimizations
- Hit Count
- Other

Machine

Name: R80

Color: Black

IPv4 Address: 192.168.101.254

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server

Version: R80.10

OS: Gaia

Network Security (2) | Management (5)

☑ Firewall
□ IPSec VPN
□ Policy Server
□ Mobile Access
□ Application Control
□ URL Filtering
□ Data Loss Prevention

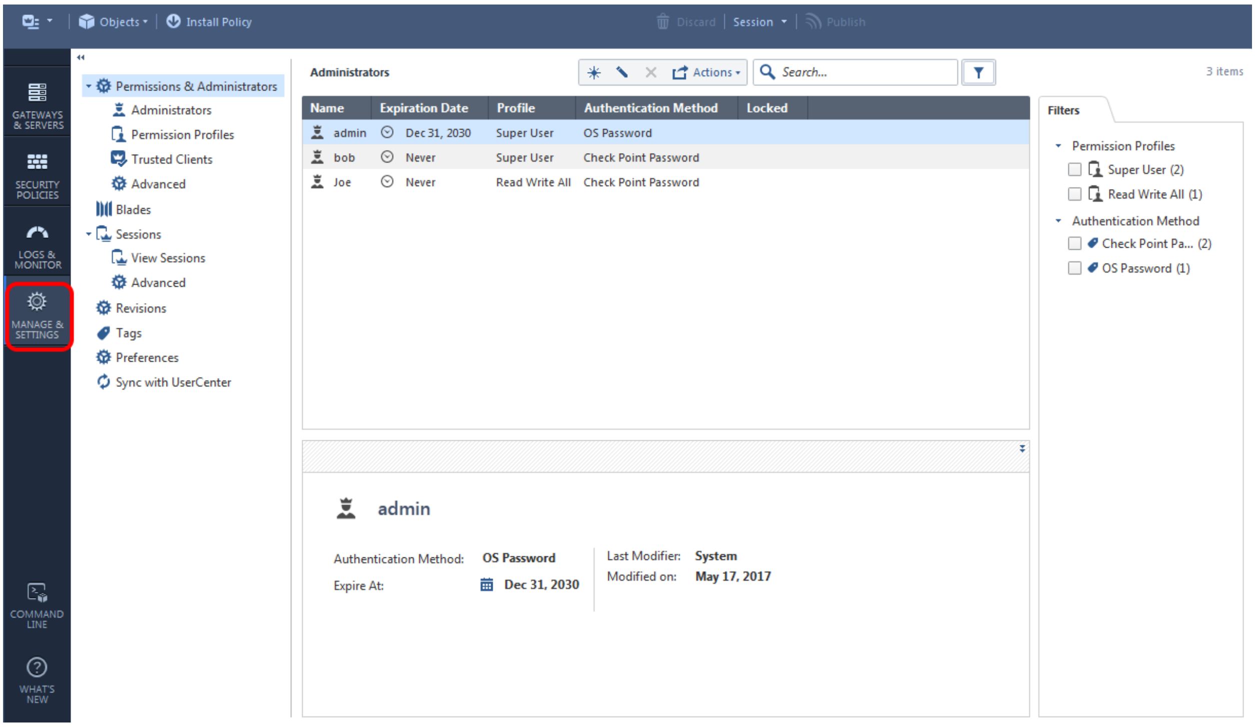
□ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
□ Identity Awareness
□ Content Awareness

Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
☑ Monitoring

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

Click on **MANAGE & SETTINGS** Tab. This is where you manage User Accounts, Sessions, Database Revisions, and more.



Name	Expiration Date	Profile	Authentication Method	Locked
admin	Dec 31, 2030	Super User	OS Password	
bob	Never	Super User	Check Point Password	
Joe	Never	Read Write All	Check Point Password	

admin

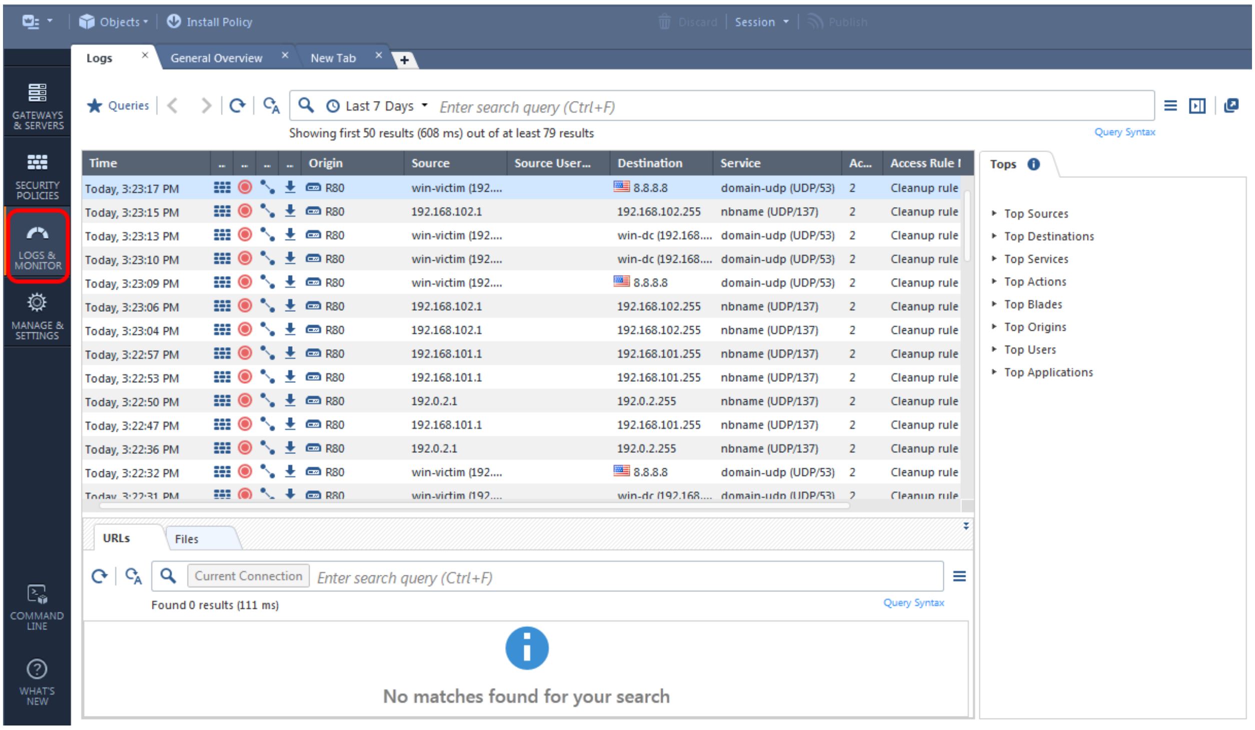
Authentication Method: OS Password

Expire At: Dec 31, 2030

Last Modifier: System

Modified on: May 17, 2017

Click on **LOGS & MONITOR** Tab. This is where you can view Logs and a General Overview Status of the environment. You can perform Boolean searches (e.g. AND OR NOT) for specific IP addresses, User or Machine names, actions, services, Gateway names, Blades, etc.



Showing first 50 results (608 ms) out of at least 79 results

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule I
Today, 3:23:17 PM					R80	win-victim (192....		8.8.8.8	domain-udp (UDP/53)	2	Cleanup rule
Today, 3:23:15 PM					R80	192.168.102.1		192.168.102.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:23:13 PM					R80	win-victim (192....		win-dc (192.168....	domain-udp (UDP/53)	2	Cleanup rule
Today, 3:23:10 PM					R80	win-victim (192....		win-dc (192.168....	domain-udp (UDP/53)	2	Cleanup rule
Today, 3:23:09 PM					R80	win-victim (192....		8.8.8.8	domain-udp (UDP/53)	2	Cleanup rule
Today, 3:23:06 PM					R80	192.168.102.1		192.168.102.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:23:04 PM					R80	192.168.102.1		192.168.102.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:22:57 PM					R80	192.168.101.1		192.168.101.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:22:53 PM					R80	192.168.101.1		192.168.101.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:22:50 PM					R80	192.0.2.1		192.0.2.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:22:47 PM					R80	192.168.101.1		192.168.101.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:22:36 PM					R80	192.0.2.1		192.0.2.255	nbname (UDP/137)	2	Cleanup rule
Today, 3:22:32 PM					R80	win-victim (192....		8.8.8.8	domain-udp (UDP/53)	2	Cleanup rule
Today, 3:22:31 PM					R80	win-victim (192....		win-dc (192.168....	domain-udp (UDP/53)	2	Cleanup rule

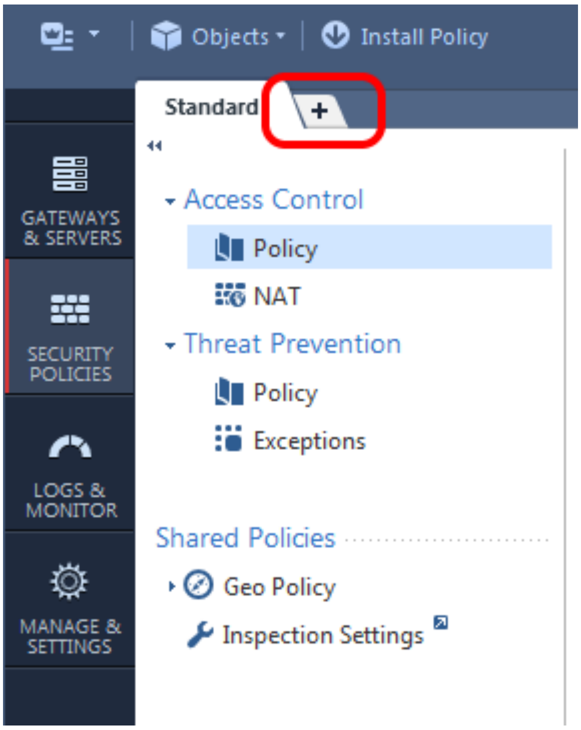
Found 0 results (111 ms)

No matches found for your search

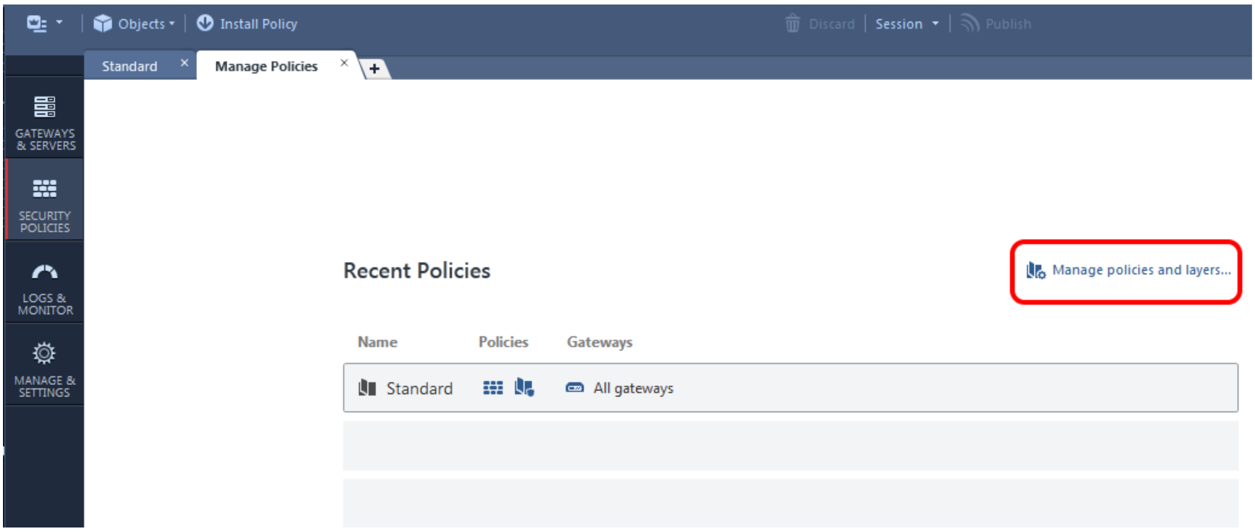
Create a Security Policy Package

Create a new Policy Package. Click on the **SECURITY POLICIES** Tab in the left-hand navigation

Click the **+** (Plus Sign) to open a New Tab. This shows the "Manage Policies" tab.



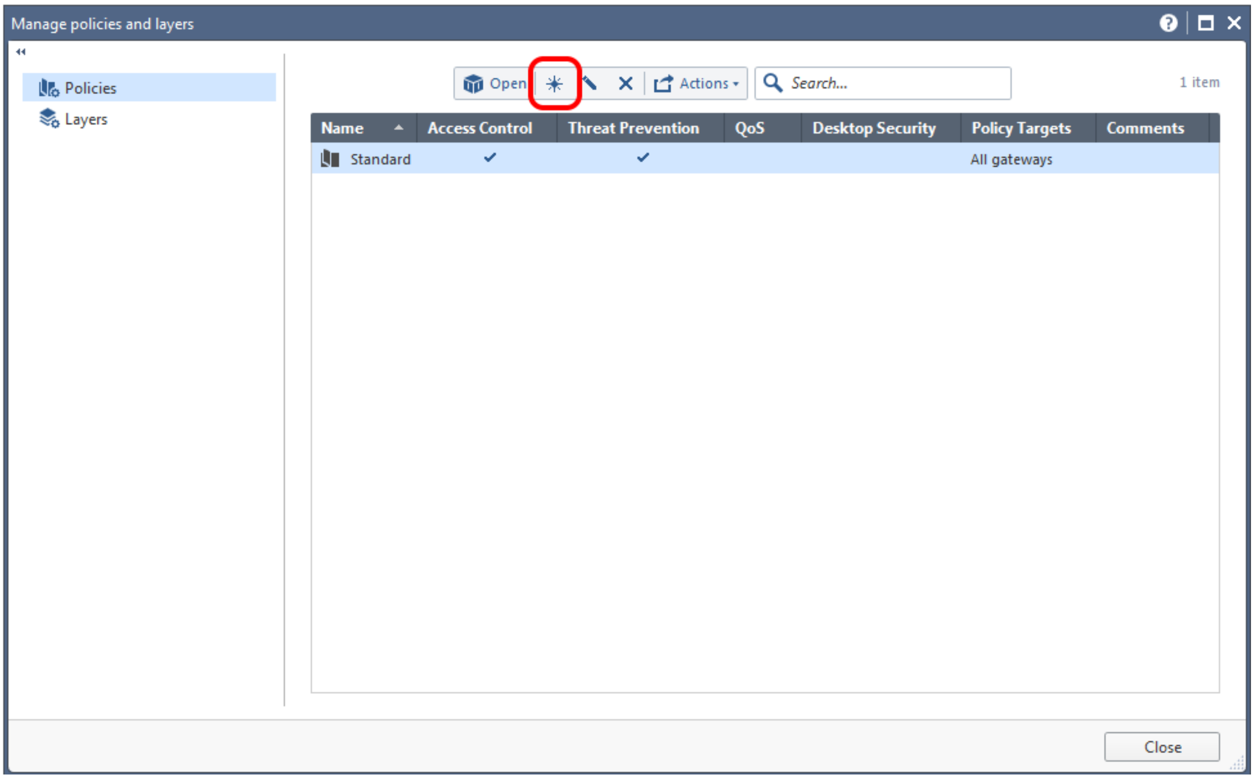
You can view and manage existing Security Policy packages. You can create a new Policy. Click the **Manage policies and layers…** link.



Recent Policies

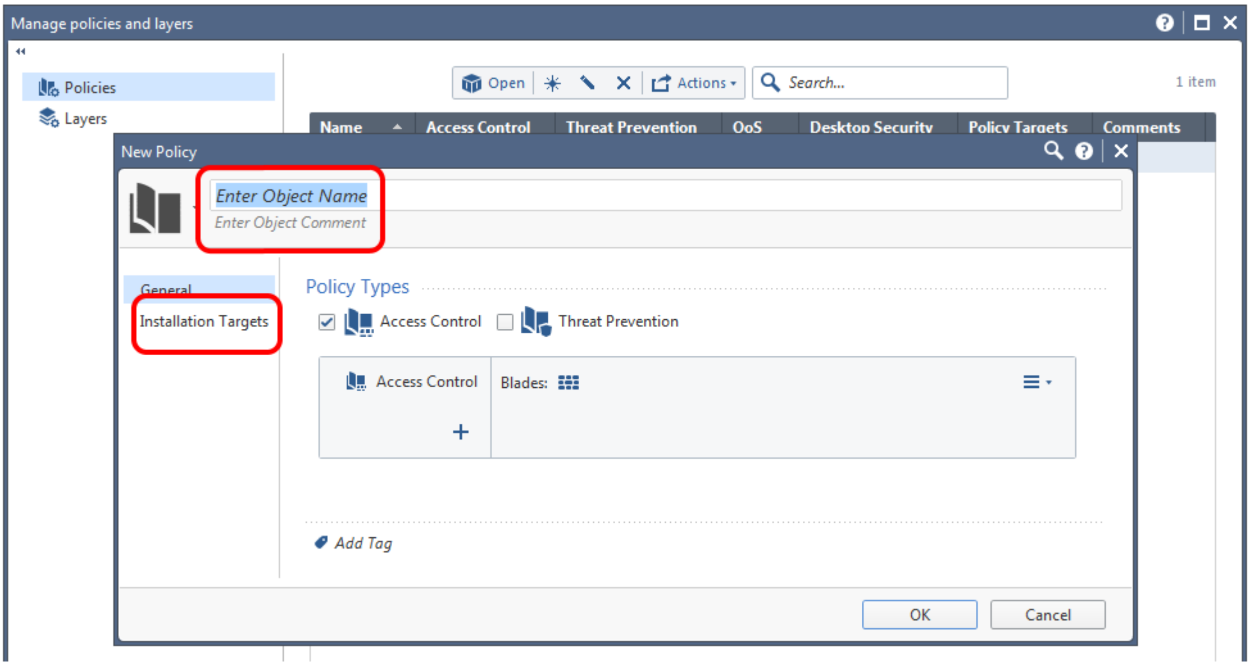
Name	Policies	Gateways
Standard		All gateways

This opens the “Manage Policies and layers” Dialog Box. Click the * (aka Star) button to create a new Policy. The “New Policy” dialog box appears.



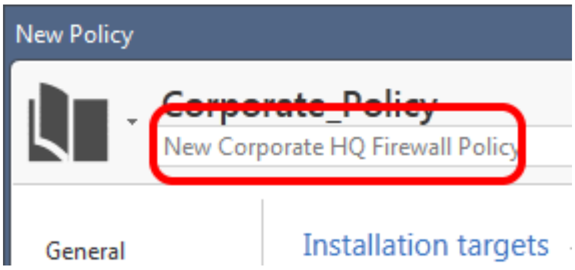
Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets	Comments
Standard	✓	✓			All gateways	

Type in a Name for the New Policy. No spaces are allowed in the Object Name field. The Object Name must being with a letter. Notice you can select to have Access Control and/or Threat Prevention in your Policy. Access Control is selected by default.



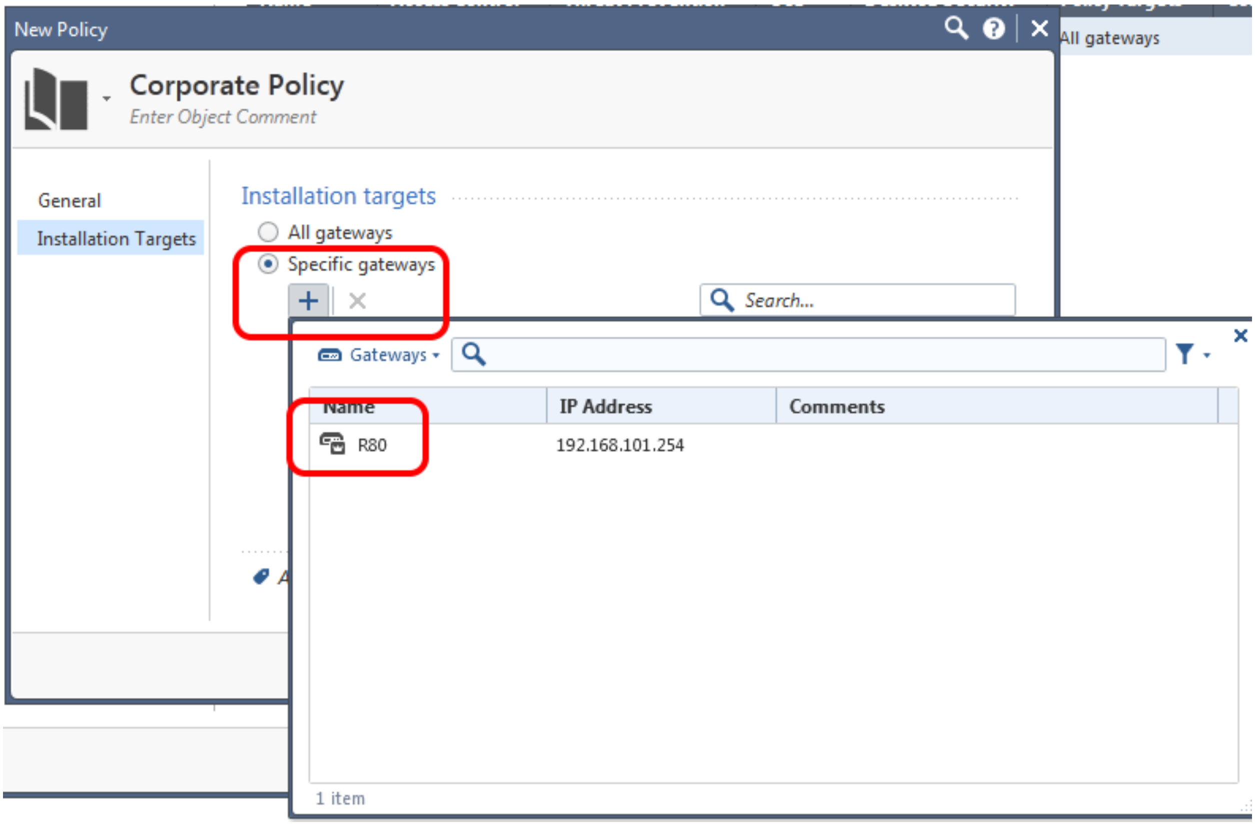
Policy Types ☑ Access Control ☐ Threat Prevention

Notice you can click on the GUI to enter a COMMENT or a TAG.



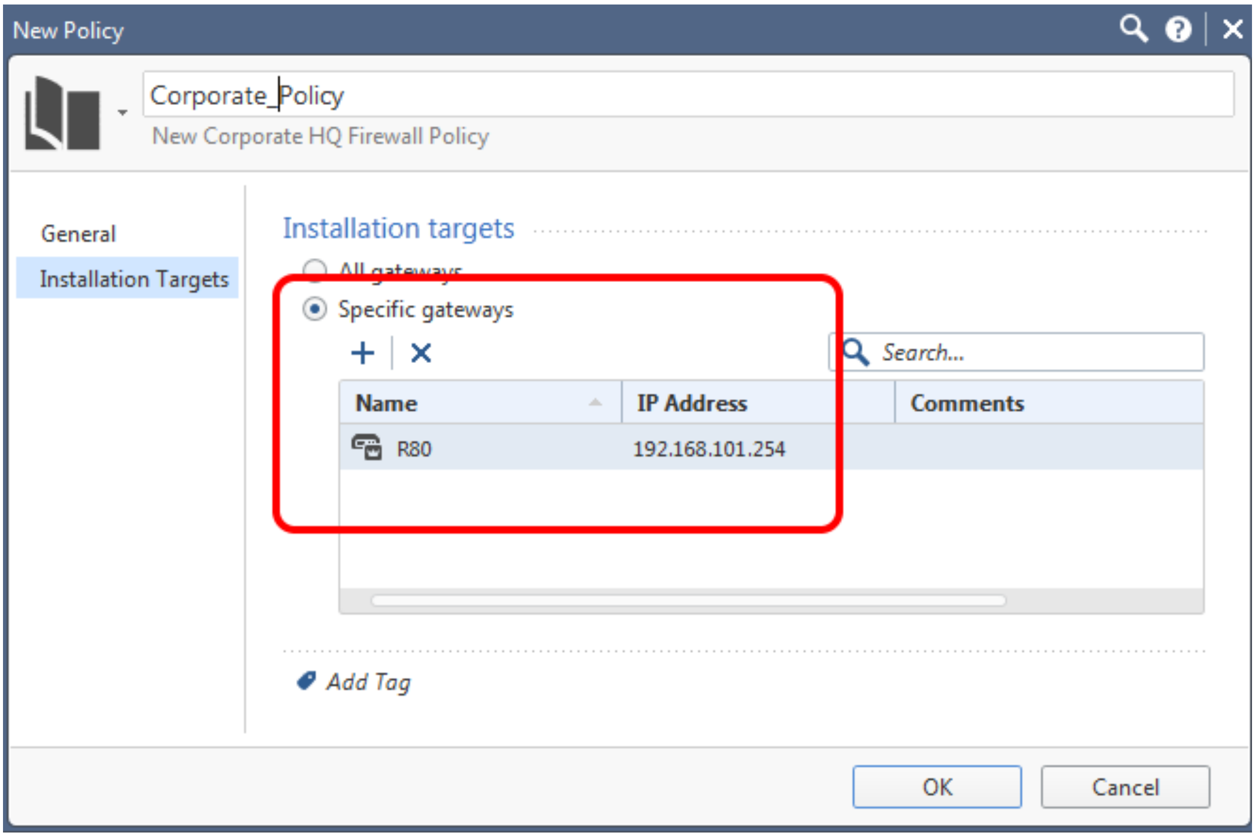
Click on the Installation Targets section. Here you can specify which Gateway(s) will available when you wish to Install the Policy later.

Click on Specific Gateways and click on the **+** **(**Plus Sign) to see available targets.



Name	IP Address	Comments
R80	192.168.101.254	

Select the Gateway you see (name may vary). Now you see the Gateway(s) for this Security Policy listed.



Corporate_Policy

New Corporate HQ Firewall Policy

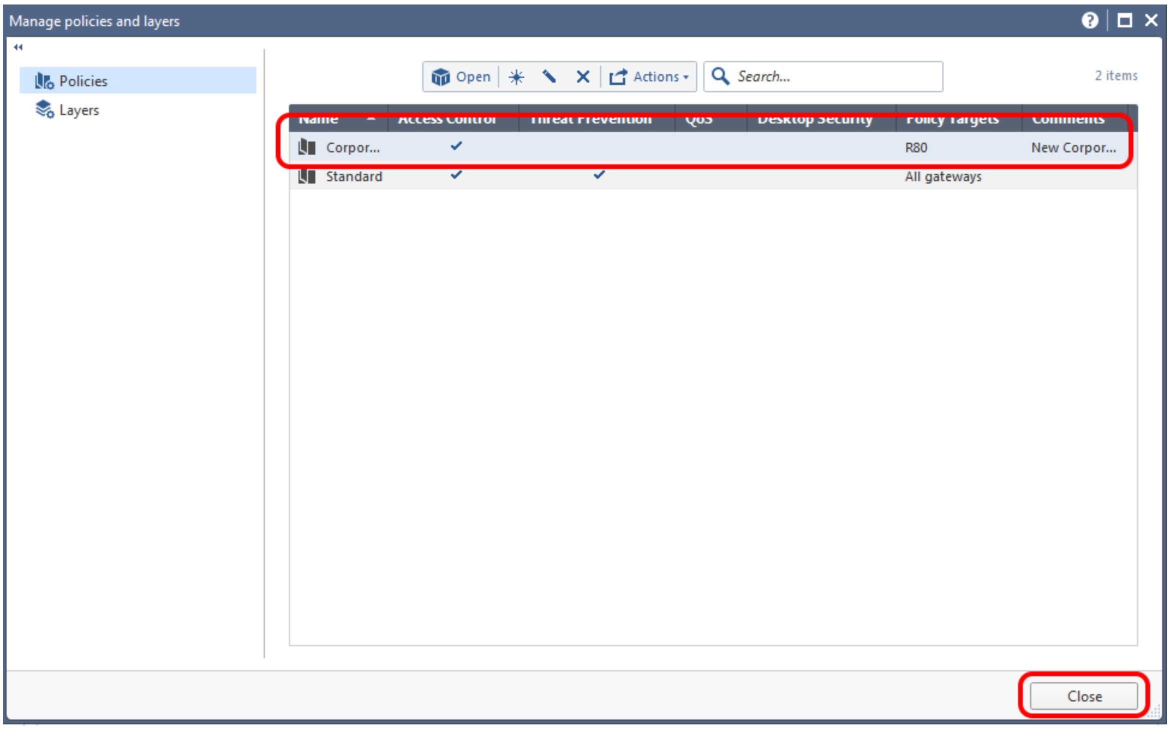
○ All gateways

● Specific gateways

Name	IP Address	Comments
R80	192.168.101.254	

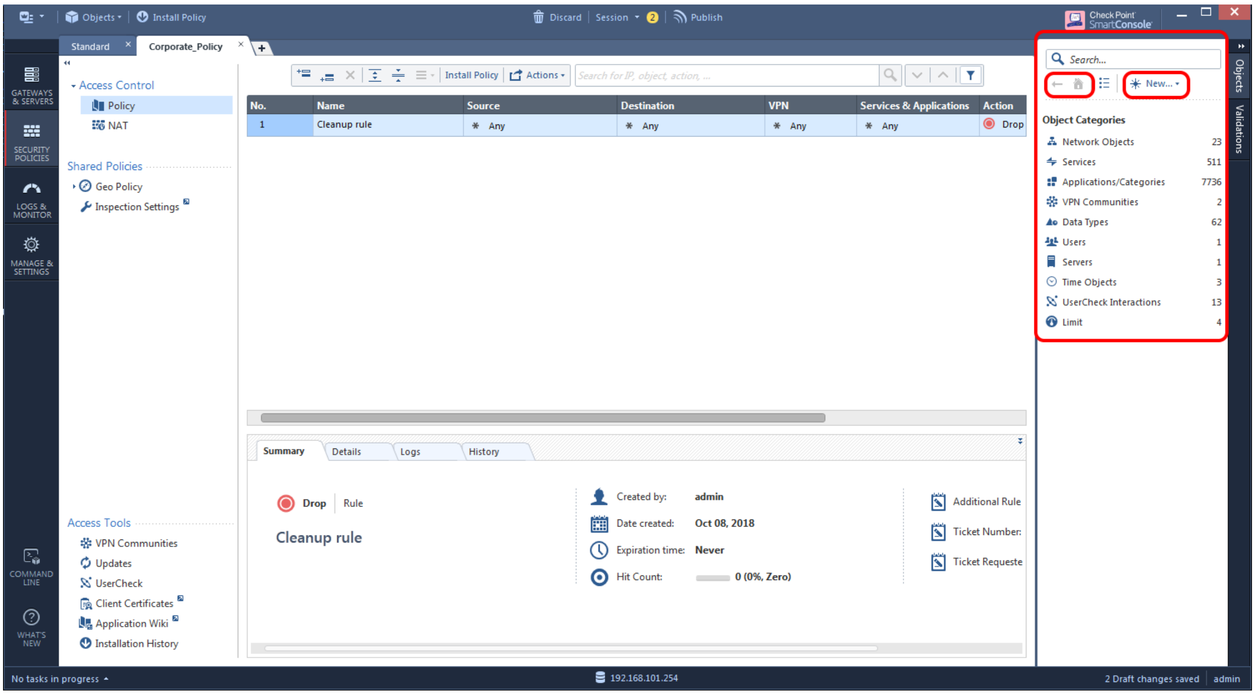
Click **OK**.

The new Policy appears in the Manage Policies list. Click the Close button.



Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets	Comments
Corpor...	✓				R80	New Corpor...
Standard	✓	✓			All gateways	

You now have a Policy that contains just 1 Rule, the Cleanup Rule.



No.	Name	Source	Destination	VPN	Services & Applications	Action
1	Cleanup rule	* Any	* Any	* Any	* Any	Drop

Drop | Rule

Cleanup rule

Created by: admin

Date created: Oct 08, 2018

Expiration time: Never

Hit Count: 0 (0%, Zero)

Object Categories

Network Objects	23
Services	511
Applications/Categories	7736
VPN Communities	2
Data Types	62
Users	1
Servers	1
Time Objects	3
UserCheck Interactions	13
Limit	4

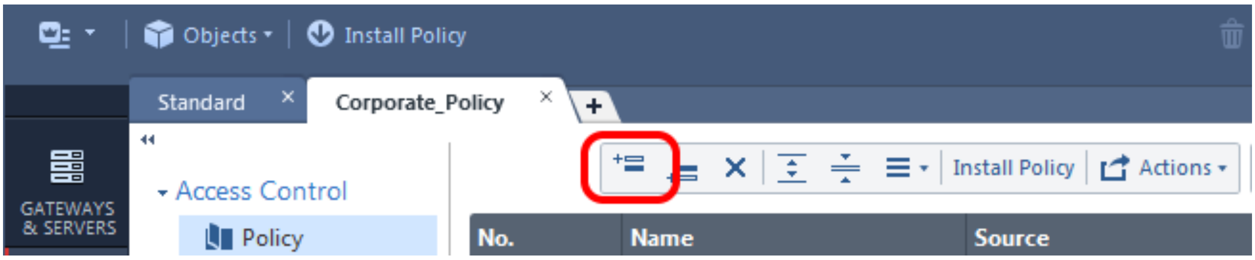
Notice that the Objects are now on the RIGHT HAND SIDE of the GUI.

You can click on each item in the list to "drill down" or use the search box. Click the **ARROW** button to return to the previous list of objects.

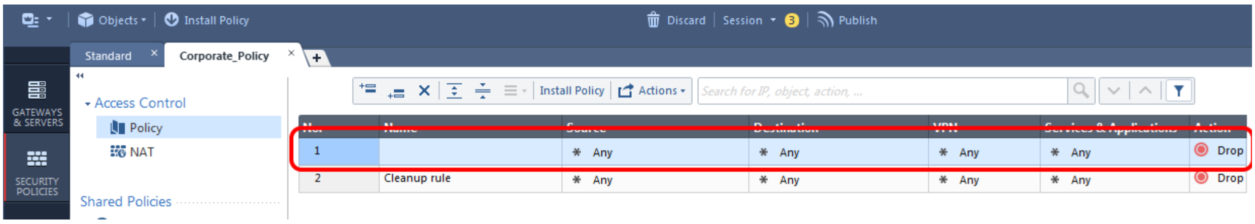
Click the **HOME** button (hint: looks like a house) to return to the top list again. The **STAR** button can be used to create new Objects.

Create a New Rule

Use the button in the middle toolbar to create a new Rule at the TOP of the Rulebase. Hover over the other buttons to see what they do.

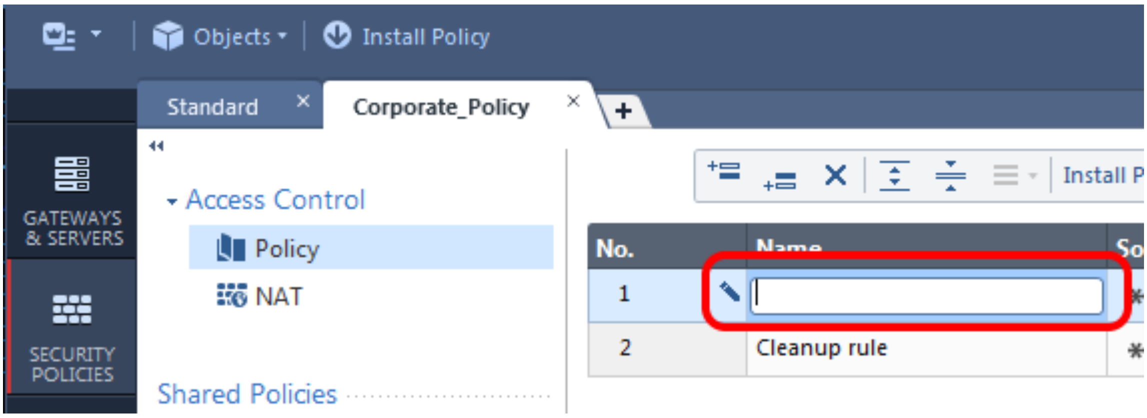


A new blank rule appears.



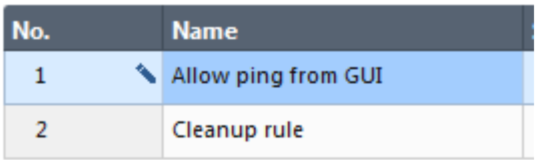
No.	Name	Source	Destination	VPN	Services & Applications	Action
1		Any	Any	Any	Any	Drop
2	Cleanup rule	Any	Any	Any	Any	Drop

Double-Click the Name field to edit the Name of the Rule



No.	Name
1	
2	Cleanup rule

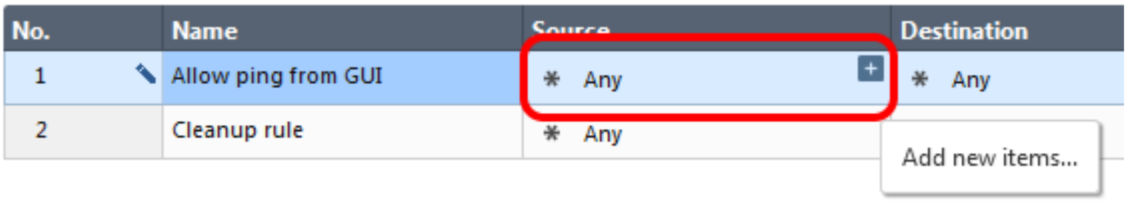
Type a new for the new rule and hit ENTER



No.	Name
1	Allow ping from GUI
2	Cleanup rule

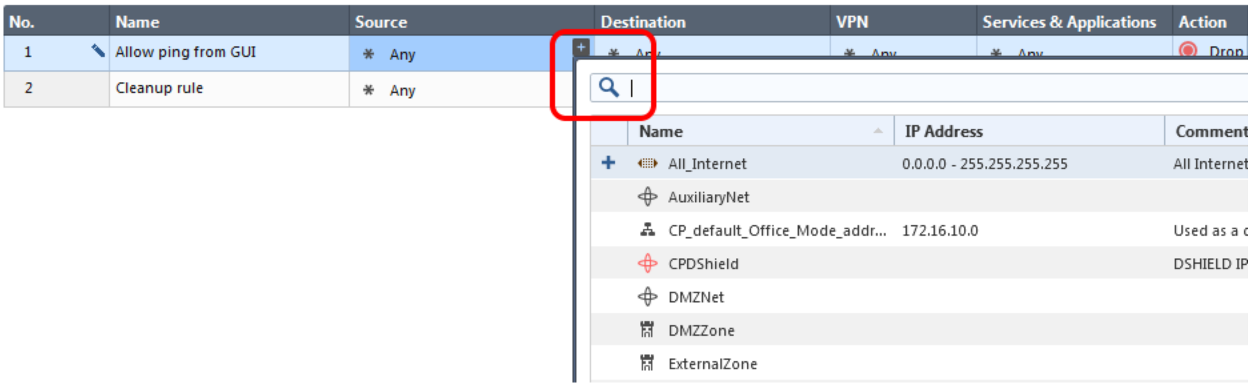
Create a Host Object and add it to a Rule

Add an object to the Source Column. Hover your mouse pointer in the Cell until the "Plus Sign" appears.



No.	Name	Source	Destination
1	Allow ping from GUI	✱ Any	✱ Any
2	Cleanup rule	✱ Any	

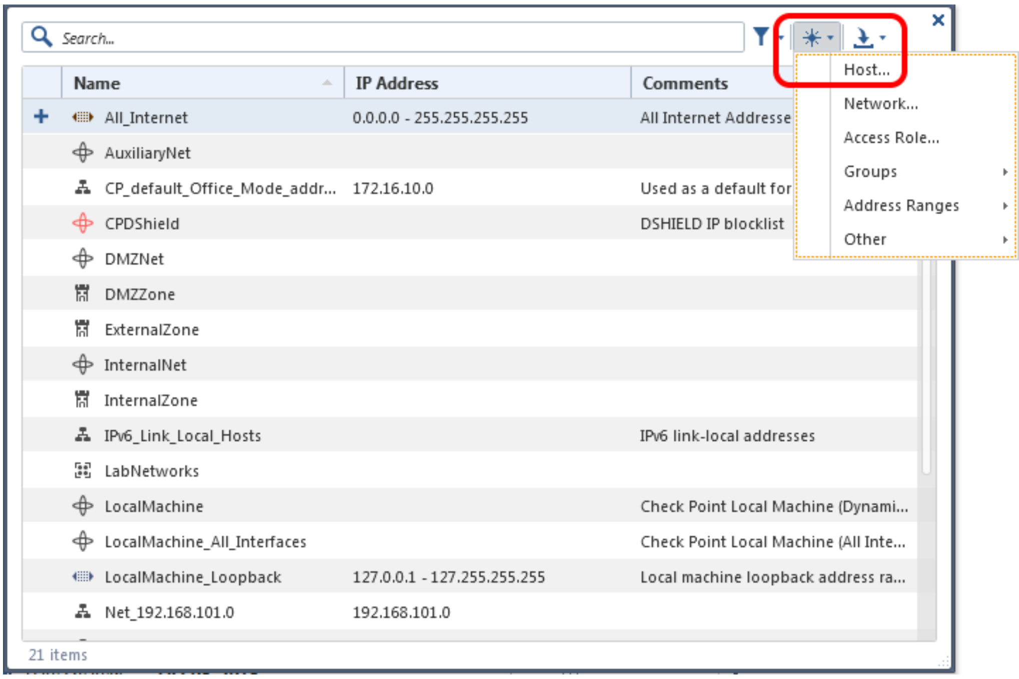
Click the **+** (Plus Sign) to select Objects from a list.



No.	Name	Source	Destination	VPN	Services & Applications	Action
1	Allow ping from GUI	✱ Any	✱ Any	✱ Any	✱ Any	Drop
2	Cleanup rule	✱ Any				

Name	IP Address	Comment
All_Internet	0.0.0.0 - 255.255.255.255	All Internet
AuxiliaryNet		
CP_default_Office_Mode_addr...	172.16.10.0	Used as a c
CPDShield		DSHIELD IP
DMZNet		
DMZZone		
ExternalZone		

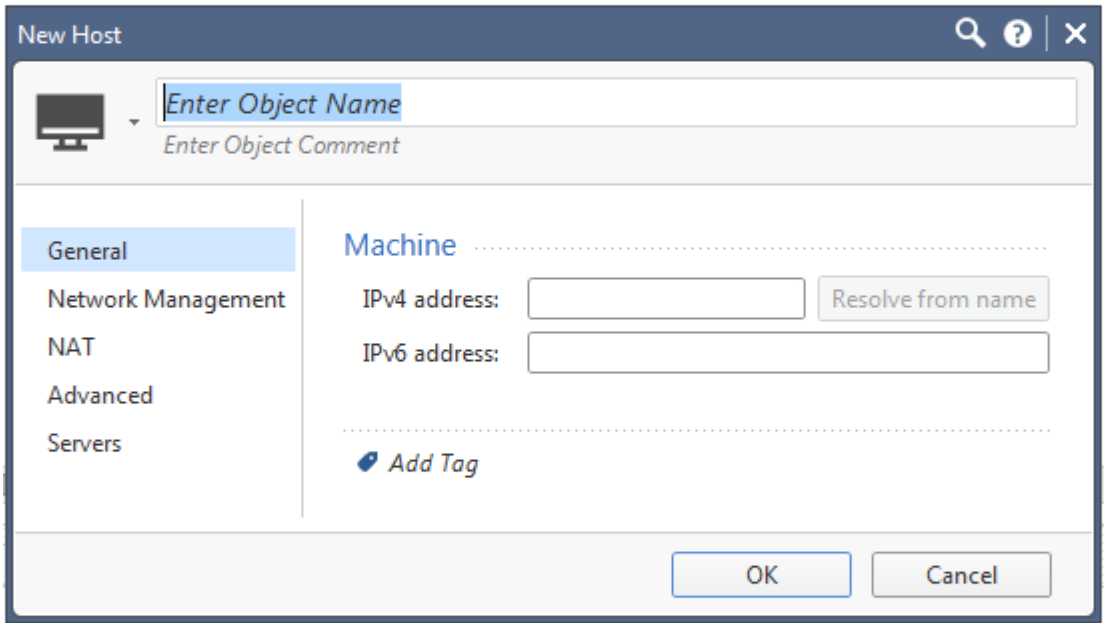
The Dialog appears to add an Object to the Source of the rule. Click on the **+** (STAR) button, and then choose **Host** from the Menu that appears to create a new Object.



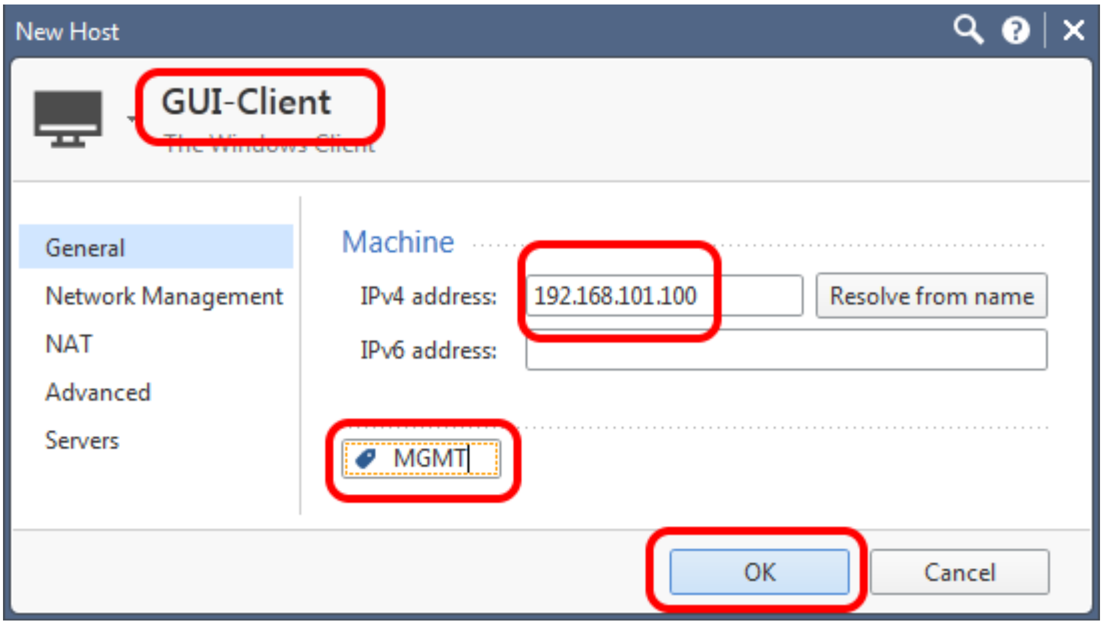
Name	IP Address	Comments
All_Internet	0.0.0.0 - 255.255.255.255	All Internet Addresse
AuxiliaryNet		
CP_default_Office_Mode_addr...	172.16.10.0	Used as a default for
CPDShield		DSHIELD IP blocklist
DMZNet		
DMZZone		
ExternalZone		
InternalNet		
InternalZone		
IPv6_Link_Local_Hosts		IPv6 link-local addresses
LabNetworks		
LocalMachine		Check Point Local Machine (Dynami...
LocalMachine_All_Interfaces		Check Point Local Machine (All Inte...
LocalMachine_Loopback	127.0.0.1 - 127.255.255.255	Local machine loopback address ra...
Net_192.168.101.0	192.168.101.0	

21 items

The "New Host" dialog box will appear.



Fill in the Object Name, IPv4 address. Enter a Comment and a Tag if you prefer. Click **OK**.



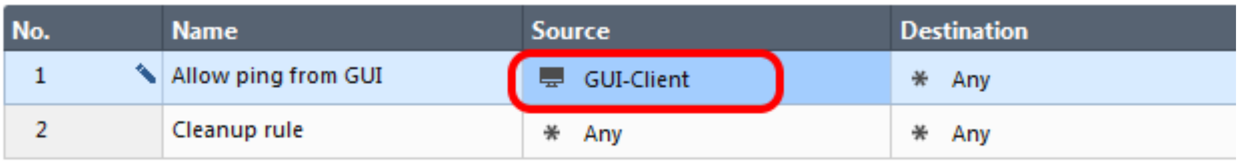
GUI-Client

The Windows Client

IPv4 address: 192.168.101.100

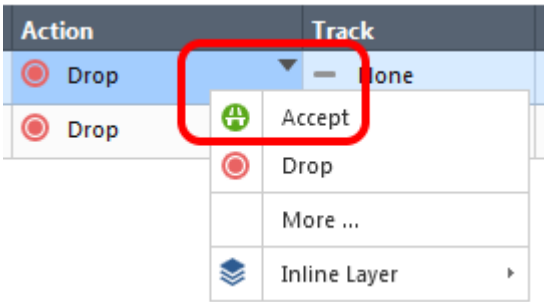
MGMT

Now the new Object is shown in the Source field of the Rule.

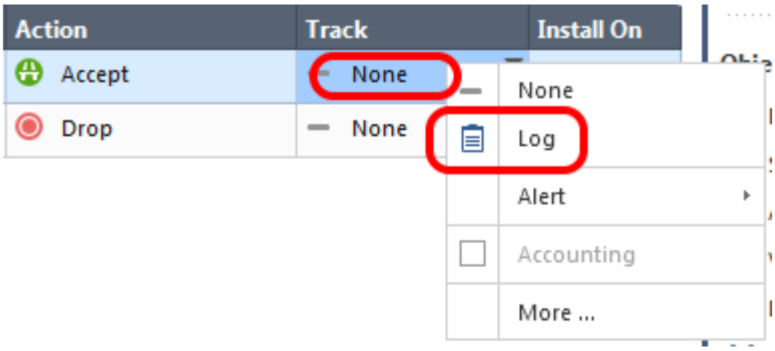


No.	Name	Source	Destination
1	Allow ping from GUI	GUI-Client	✱ Any
2	Cleanup rule	✱ Any	✱ Any

Change the Action field from Drop to Accept. Click in the Action field to see the menu of choices. Click on **Accept**.

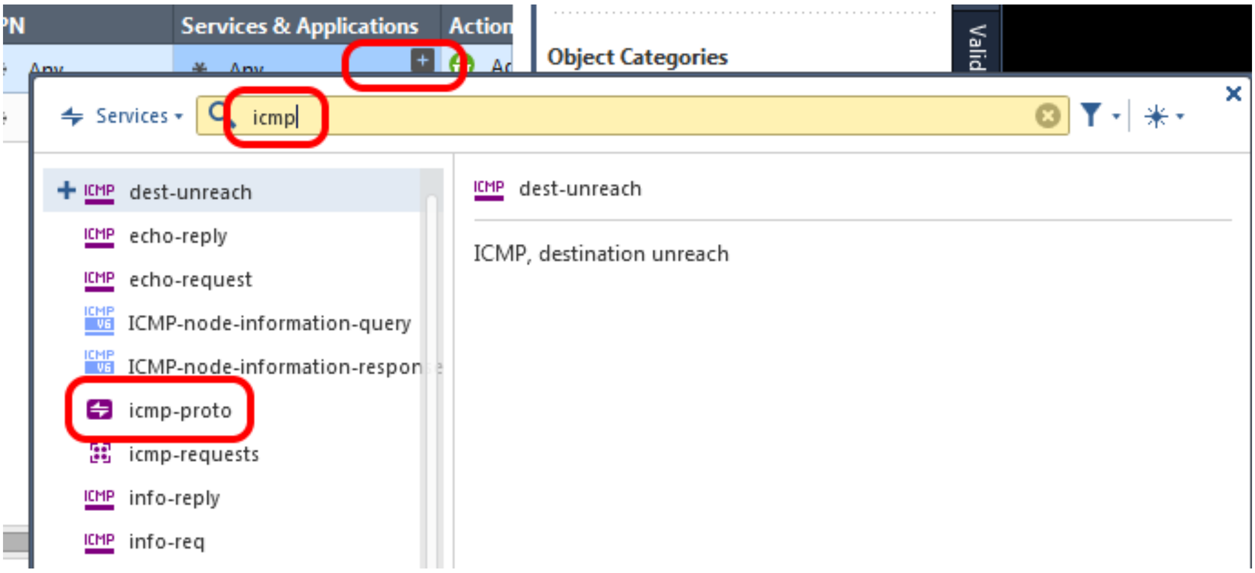


Now click in the Track field and Select **Log** from the menu that appears.



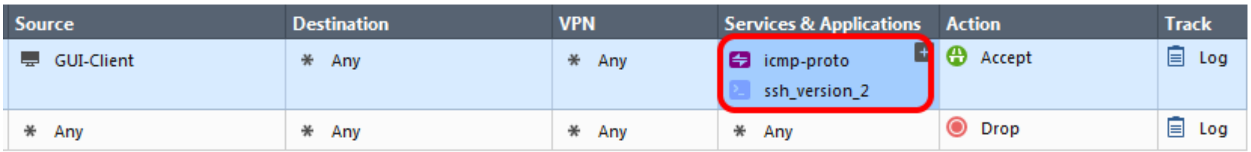
Search for Services and add them to a Rule

Add “icmp” and “ssh” to the Services & Applications field of Rule 1. Click on the **+** (Plus Sign) in the field to see the search list. Type "icmp" into the search field to narrow the results (or scroll to see your choices). Select icmp-proto to add it to the rule.



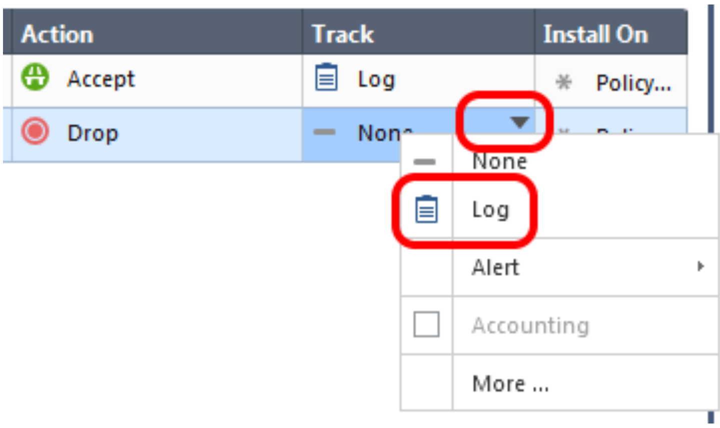
ICMP, destination unreach

If you click the "Plus Sign" that appears next to icmp-proto, you can type in another search for ssh. Select ssh-version-2. Both services appear in the Services & Applications field.



Source	Destination	VPN	Services & Applications	Action	Track
GUI-Client	Any	Any	icmp-proto ssh_version_2	Accept	Log
Any	Any	Any	Any	Drop	Log

Enable Logging for the Cleanup Rule

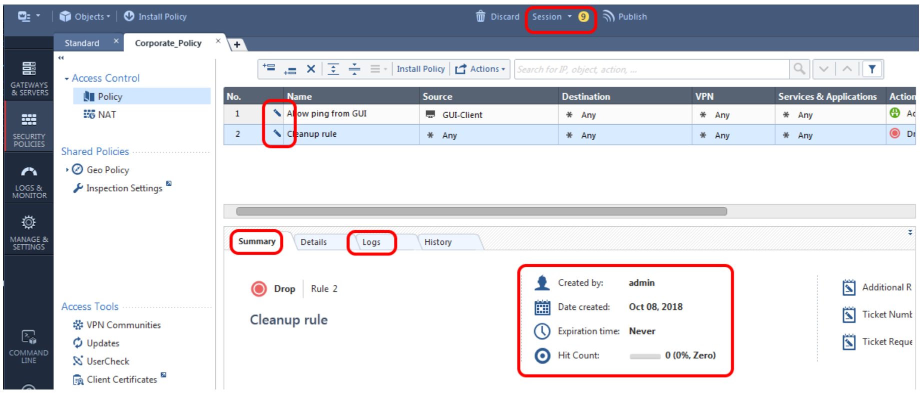


Action	Track	Install On
Accept	Log	Policy...
Drop	None	Poli

Sessions, changes, and Publishing

Notice the small “Pencil” Icons next to each rule we have modified in the Policy. This signifies edits you have made to the policy. Notice the Summary Tab below the policy with the details of who created the Rule, when the rule was created, Hit Count and more. There are fields for entering details for the change being made (work orders, authorization codes, ticket requests, etc.). These fields can be customized to your liking. Click on each rule to see the available information. Also notice the in the top of the SmartConsole, there is a Yellow circle with a number it in. This is the number of Changes we have made to the Policy in our current Session. Before we can install the new Security Policy on the Gateway, we must Publish the changes to the database.

Note: The number of changes may vary in your lab



No.	Name	Source	Destination	VPN	Services & Applications	Action
1	Allow ping from GUI	GUI-Client	Any	Any	Any	Ac
2	Cleanup rule	Any	Any	Any	Any	Dr

Drop | Rule 2

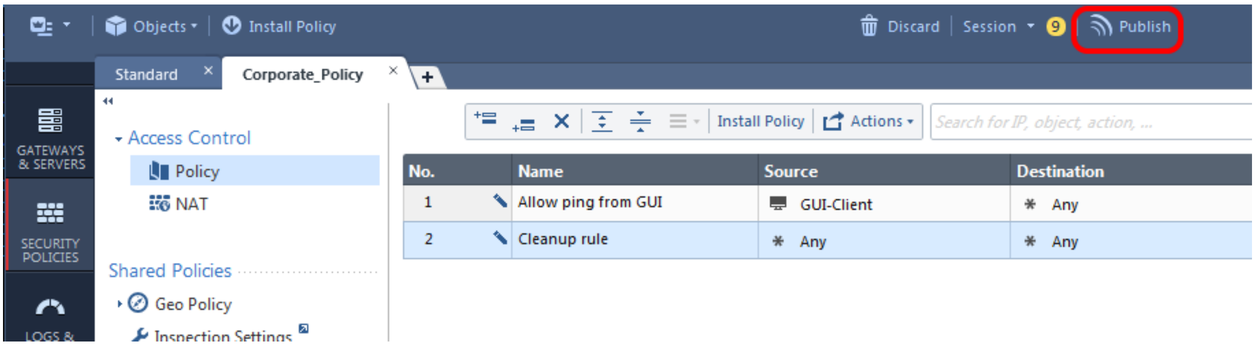
Cleanup rule

Created by: admin
Date created: Oct 08, 2018
Expiration time: Never
Hit Count: 0 (0%, Zero)

You will see a tab called "Logs" next to the Summary tab. We don't have any traffic yet, so we probably won't see any logs yet.

Publish Changes to the Security Policy

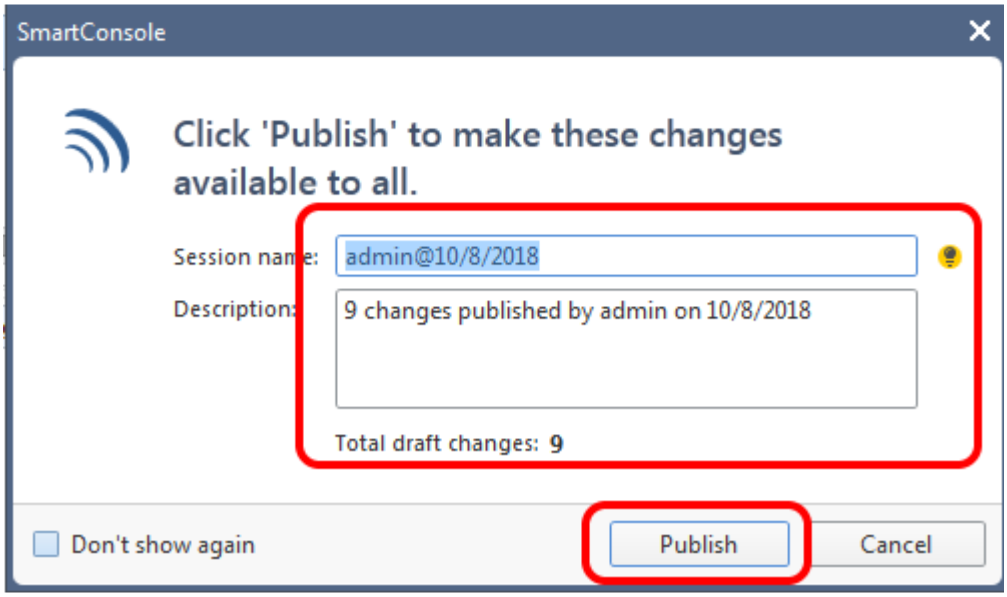
Click the **Publish** button.



No.	Name	Source	Destination
1	Allow ping from GUI	GUI-Client	Any
2	Cleanup rule	Any	Any

Enter the relevant details (or make no changes) and click the **Publish** button. You will see a progress indicator briefly while the changes are written to the database.

Once that completes, you will notice the little pencil icons and the Yellow Circle are gone.



Click 'Publish' to make these changes available to all.

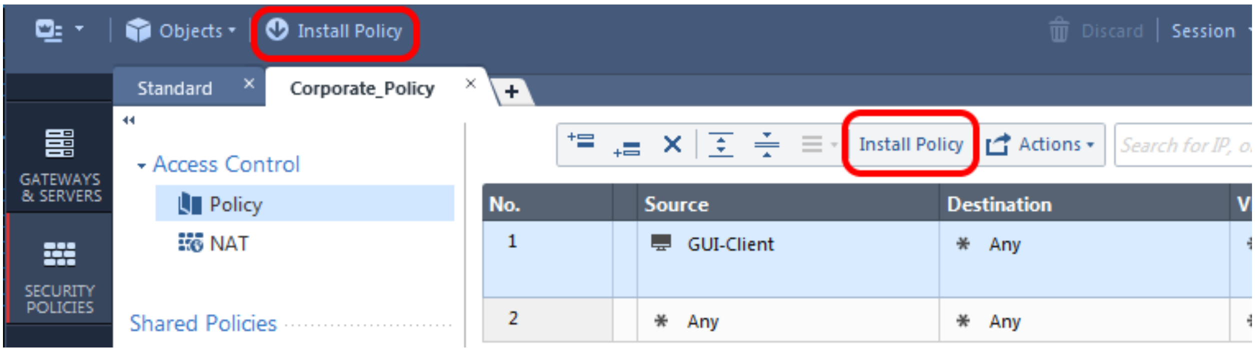
Session name: admin@10/8/2018

Description: 9 changes published by admin on 10/8/2018

Total draft changes: 9

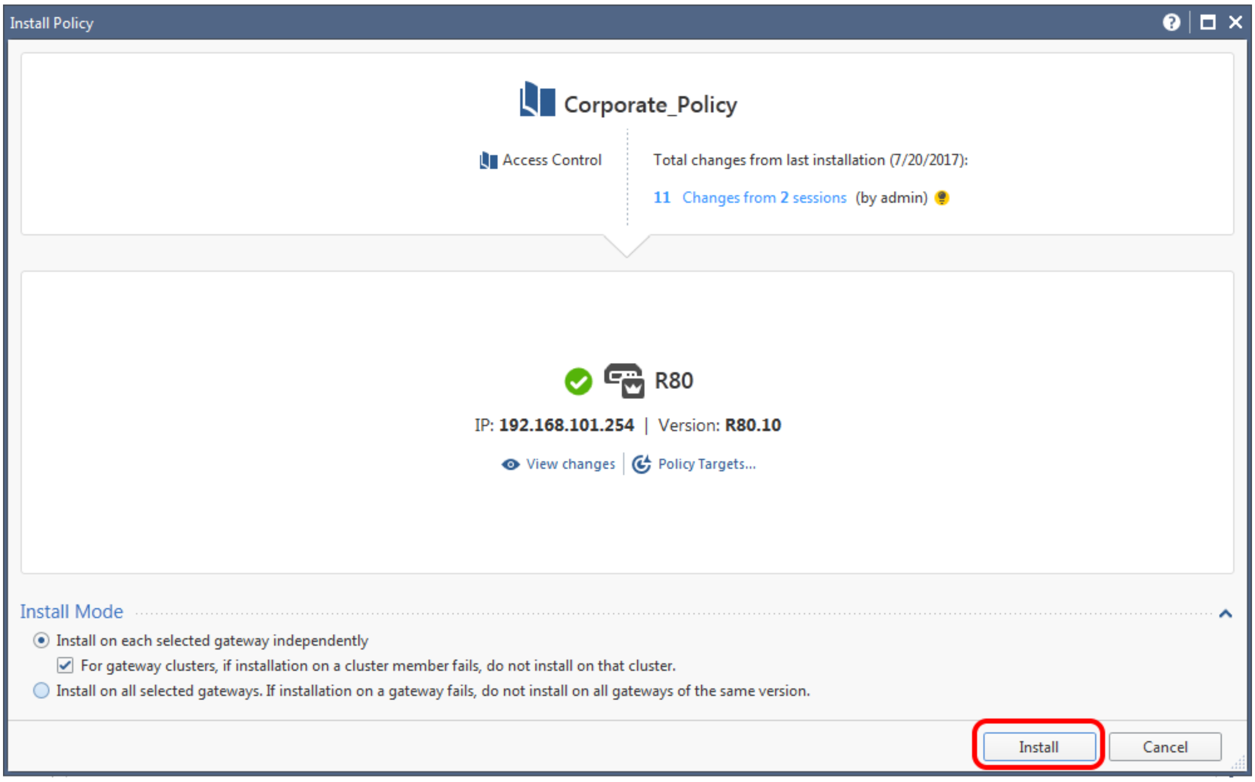
Install the Security Policy

Click the **Install Policy** button. There are 2 **Install Policy** buttons in the GUI. One is in the middle tool ribbon, and the other in the upper left ribbon of buttons.



No.	Source	Destination	V
1	GUI-Client	Any	
2	Any	Any	

The "Install Policy" dialog appears. Click the **Install** button.


Install Policy

Corporate_Policy

Access Control

Total changes from last installation (7/20/2017):

11 Changes from 2 sessions (by admin)

R80

IP: **192.168.101.254** | Version: **R80.10**

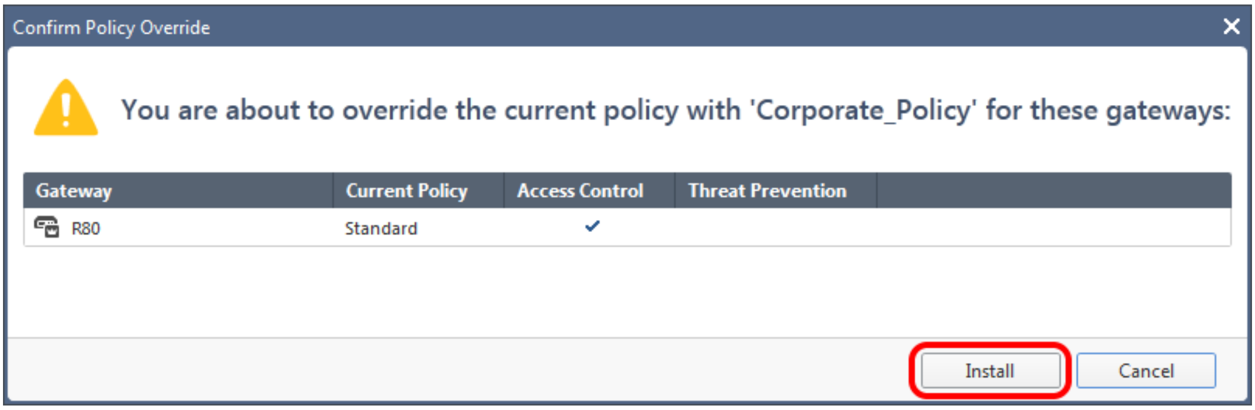
Install Mode

● Install on each selected gateway independently

☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

You will be asked to confirm that you wish to over-write the current Policy with the newly created “Corporate Policy". Click **Install** to continue.

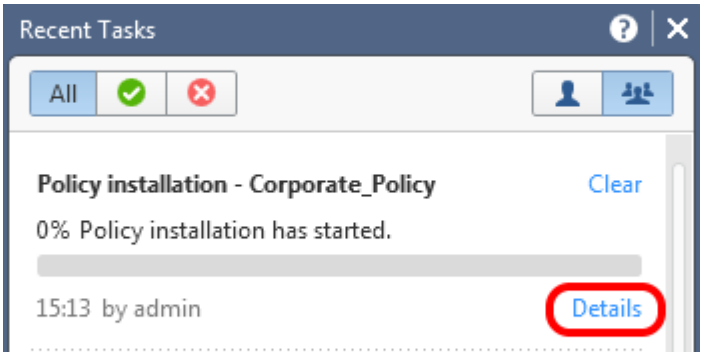


Confirm Policy Override

You are about to override the current policy with 'Corporate_Policy' for these gateways:

Gateway	Current Policy	Access Control	Threat Prevention
R80	Standard	✓	

The "Recent Tasks" dialog will appear, showing status for the Policy validation, compilation and installation. You can click the **Details** link for more information.



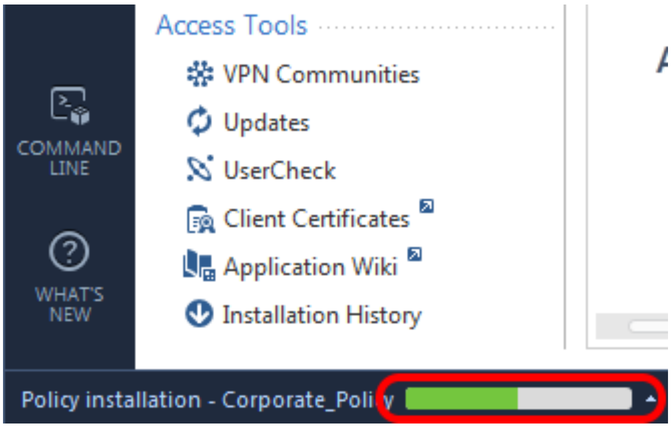
Recent Tasks

Policy installation - Corporate_Policy

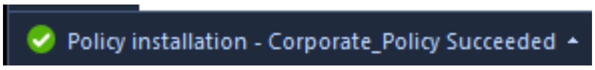
0% Policy installation has started.

15:13 by admin

After a short time, it will minimize itself to the bottom left notification area. You can click the **green progress bar** if your wish to view the larger version again.



Policy Installation will complete with a notification.

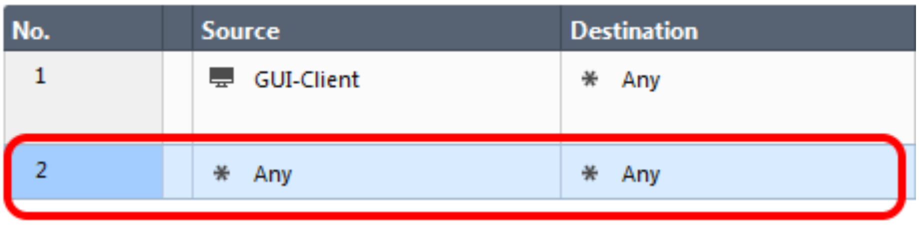


Policy installation - Corporate_Policy Succeeded

Add Section Titles to the Policy

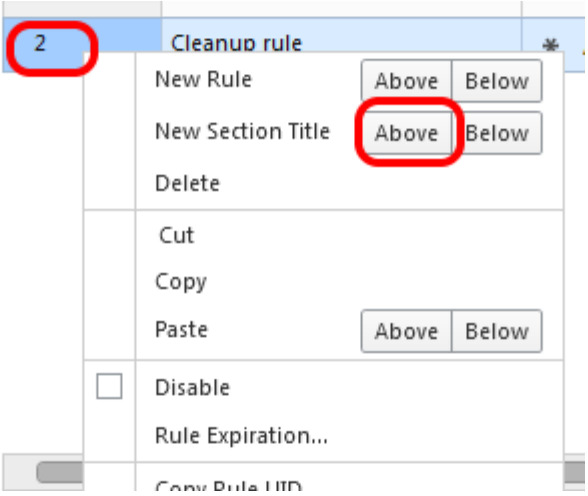
Create a New Section Title to help keep your Policy organized.

Click on Rule 2 to highlight it.



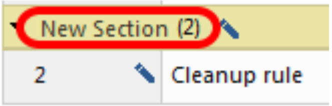
No.	Source	Destination
1	GUI-Client	✱ Any
2	✱ Any	✱ Any

Right-click on Rule 2, and click **ABOVE** "New Section Title".



2 Cleanup rule

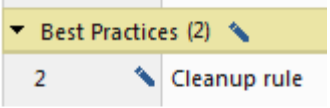
A new section title appears



New Section (2)

2 Cleanup rule

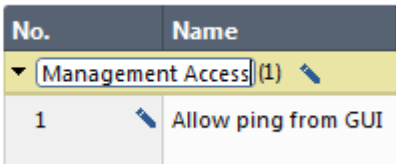
Double click "New Section" to edit and type in "Best Practices".



Best Practices (2)

2 Cleanup rule

Now add a Section Title above Rule 1 and name it "Management Access".

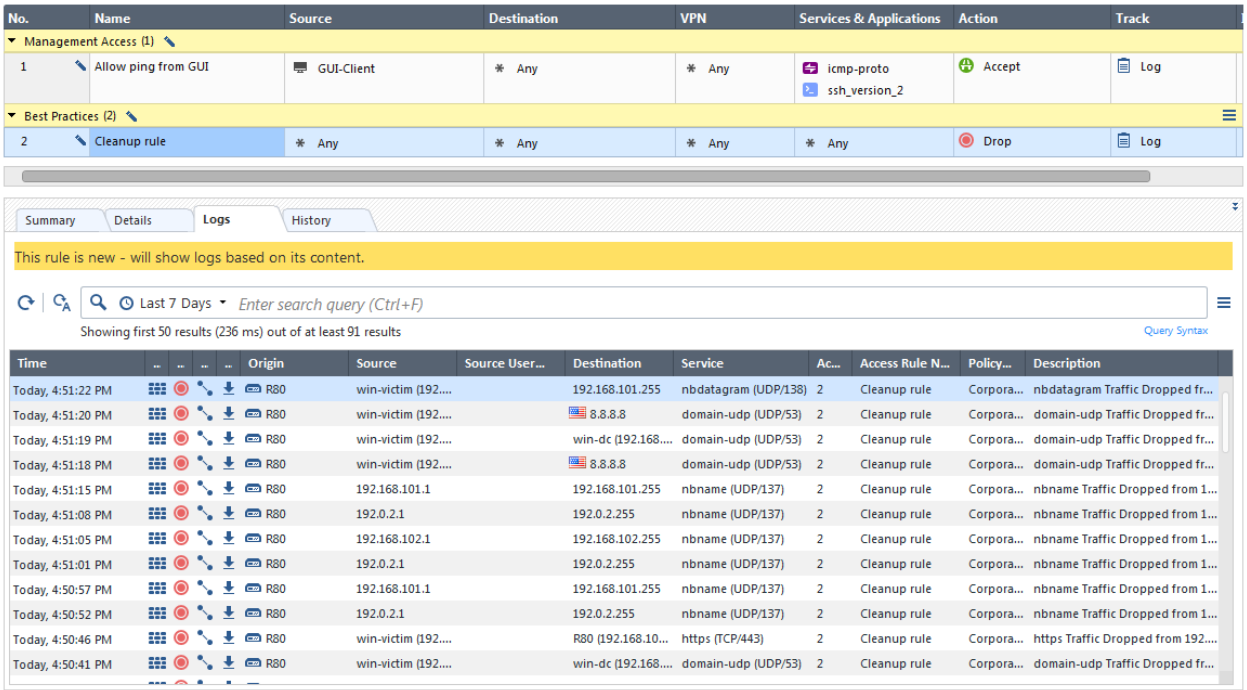


No.	Name
Management Access (1)	
1	Allow ping from GUI

Publish the changes and Install the Policy.

View the logs for a specific Rule without switching to the **LOGS & MONITOR** Tab. Highlight Rule 2 (aka The Cleanup Rule) in the Policy.

You will see the most recent logs for the selected rule appear below the security policy.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
Management Access (1)							
1	Allow ping from GUI	GUI-Client	* Any	* Any	icmp-proto ssh_version_2	Accept	Log
Best Practices (2)							
2	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log

Summary | Details | Logs | History

This rule is new - will show logs based on its content.

Last 7 Days ▾ Enter search query (Ctrl+F)

Showing first 50 results (236 ms) out of at least 91 results

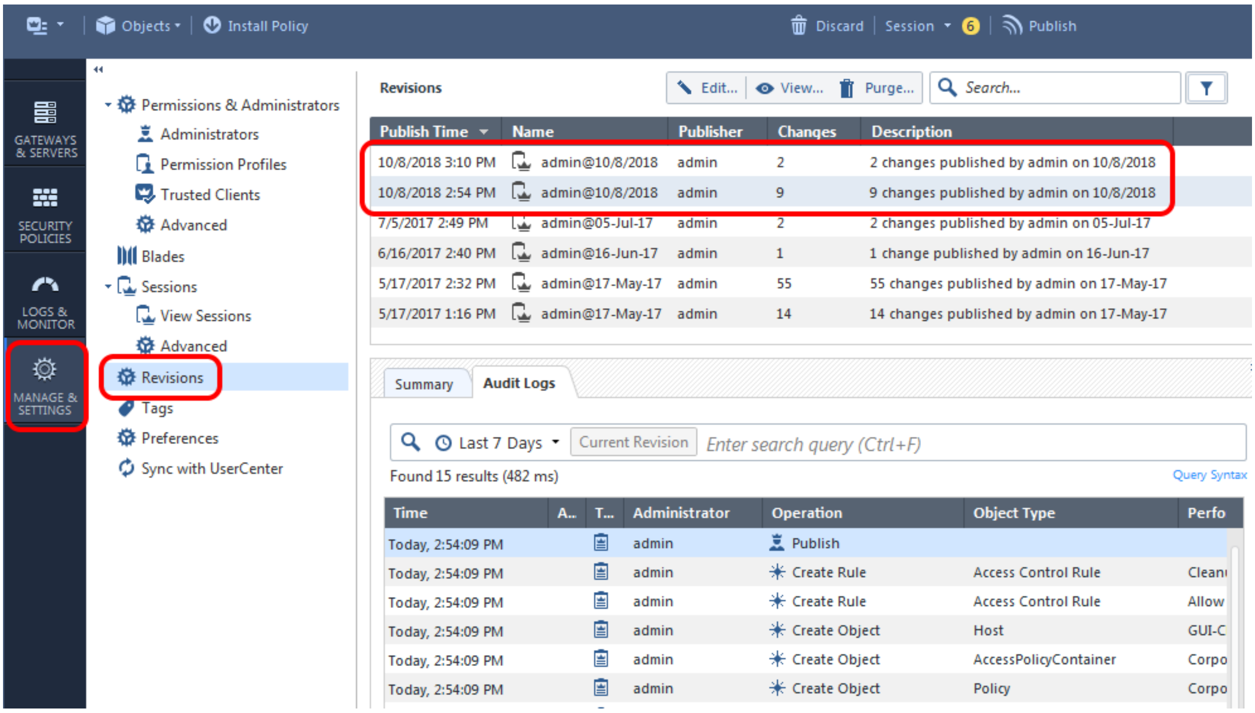
Query Syntax

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 4:51:22 PM					R80	win-victim (192....		192.168.101.255	nbdatagram (UDP/138)	2	Cleanup rule	Corpora...	nbdatagram Traffic Dropped fr...
Today, 4:51:20 PM					R80	win-victim (192....		8.8.8.8	domain-udp (UDP/53)	2	Cleanup rule	Corpora...	domain-udp Traffic Dropped fr...
Today, 4:51:19 PM					R80	win-victim (192....		win-dc (192.168....	domain-udp (UDP/53)	2	Cleanup rule	Corpora...	domain-udp Traffic Dropped fr...
Today, 4:51:18 PM					R80	win-victim (192....		8.8.8.8	domain-udp (UDP/53)	2	Cleanup rule	Corpora...	domain-udp Traffic Dropped fr...
Today, 4:51:15 PM					R80	192.168.101.1		192.168.101.255	nbname (UDP/137)	2	Cleanup rule	Corpora...	nbname Traffic Dropped from 1...
Today, 4:51:08 PM					R80	192.0.2.1		192.0.2.255	nbname (UDP/137)	2	Cleanup rule	Corpora...	nbname Traffic Dropped from 1...
Today, 4:51:05 PM					R80	192.168.102.1		192.168.102.255	nbname (UDP/137)	2	Cleanup rule	Corpora...	nbname Traffic Dropped from 1...
Today, 4:51:01 PM					R80	192.0.2.1		192.0.2.255	nbname (UDP/137)	2	Cleanup rule	Corpora...	nbname Traffic Dropped from 1...
Today, 4:50:57 PM					R80	192.168.101.1		192.168.101.255	nbname (UDP/137)	2	Cleanup rule	Corpora...	nbname Traffic Dropped from 1...
Today, 4:50:52 PM					R80	192.0.2.1		192.0.2.255	nbname (UDP/137)	2	Cleanup rule	Corpora...	nbname Traffic Dropped from 1...
Today, 4:50:46 PM					R80	win-victim (192....		R80 (192.168.10...	https (TCP/443)	2	Cleanup rule	Corpora...	https Traffic Dropped from 192....
Today, 4:50:41 PM					R80	win-victim (192....		win-dc (192.168....	domain-udp (UDP/53)	2	Cleanup rule	Corpora...	domain-udp Traffic Dropped fr...

Revisions and Sessions

It is possible to view the Policy Changes made by an Administrator during a session.

Click on the **MANAGE & SETTINGS** Tab. Click on **Revisions**. Click on one of the available Sessions. Click on the **Audit Logs** Tab.

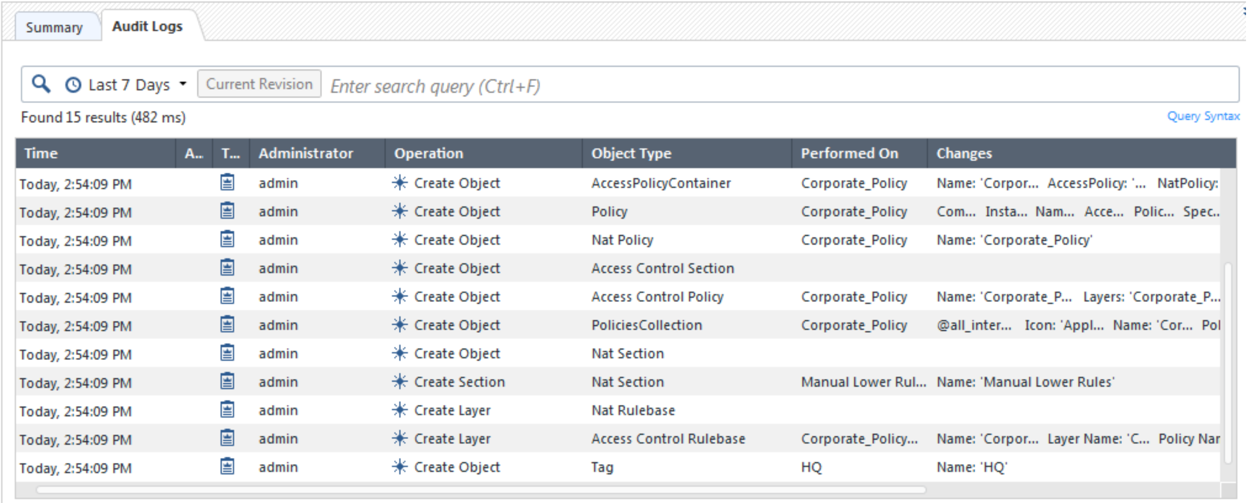


Publish Time	Name	Publisher	Changes	Description
10/8/2018 3:10 PM	admin@10/8/2018	admin	2	2 changes published by admin on 10/8/2018
10/8/2018 2:54 PM	admin@10/8/2018	admin	9	9 changes published by admin on 10/8/2018
7/5/2017 2:49 PM	admin@05-Jul-17	admin	2	2 changes published by admin on 05-Jul-17
6/16/2017 2:40 PM	admin@16-Jun-17	admin	1	1 change published by admin on 16-Jun-17
5/17/2017 2:32 PM	admin@17-May-17	admin	55	55 changes published by admin on 17-May-17
5/17/2017 1:16 PM	admin@17-May-17	admin	14	14 changes published by admin on 17-May-17

Found 15 results (482 ms)

Time	A...	T...	Administrator	Operation	Object Type	Perfo
Today, 2:54:09 PM			admin	Publish		
Today, 2:54:09 PM			admin	Create Rule	Access Control Rule	Clean
Today, 2:54:09 PM			admin	Create Rule	Access Control Rule	Allow
Today, 2:54:09 PM			admin	Create Object	Host	GUI-C
Today, 2:54:09 PM			admin	Create Object	AccessPolicyContainer	Corpo
Today, 2:54:09 PM			admin	Create Object	Policy	Corpo

You can see the changes made, the time stamps of the changes, and the details.



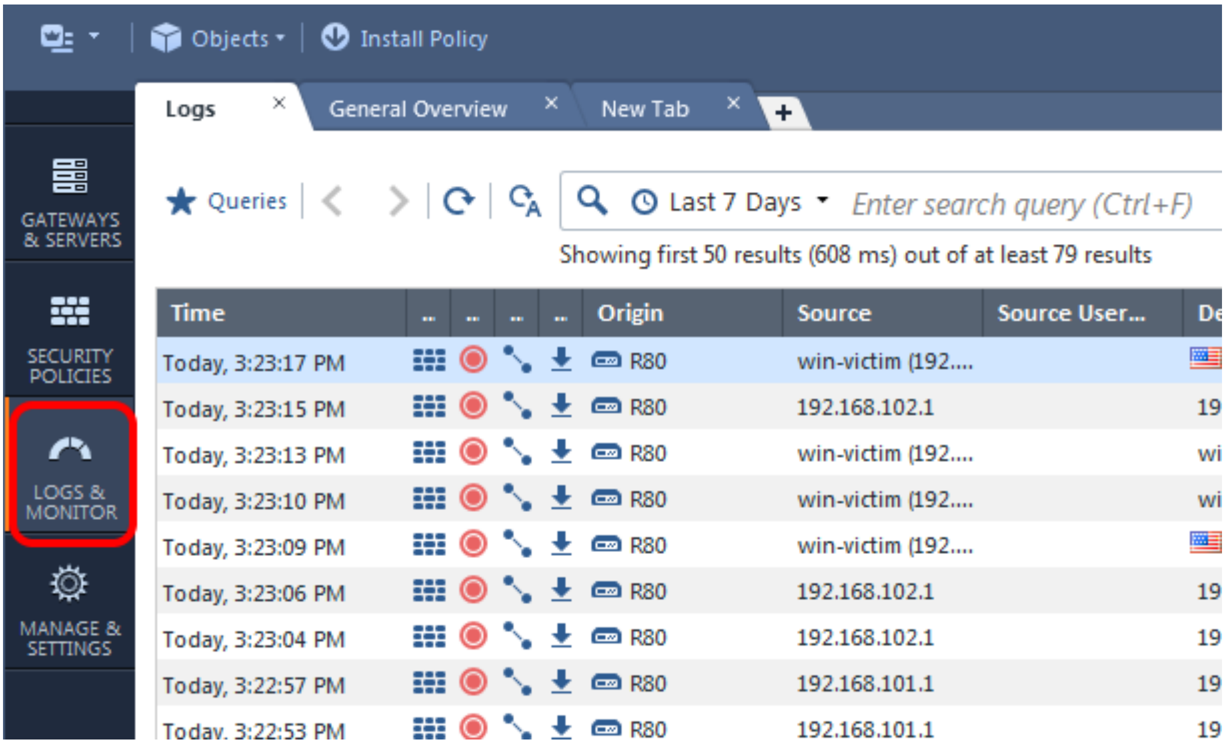
Found 15 results (482 ms)

Time	A...	T...	Administrator	Operation	Object Type	Performed On	Changes
Today, 2:54:09 PM			admin	Create Object	AccessPolicyContainer	Corporate_Policy	Name: 'Corpor... AccessPolicy: '... NatPolicy:
Today, 2:54:09 PM			admin	Create Object	Policy	Corporate_Policy	Com... Insta... Nam... Acce... Polic... Spec..
Today, 2:54:09 PM			admin	Create Object	Nat Policy	Corporate_Policy	Name: 'Corporate_Policy'
Today, 2:54:09 PM			admin	Create Object	Access Control Section		
Today, 2:54:09 PM			admin	Create Object	Access Control Policy	Corporate_Policy	Name: 'Corporate_P... Layers: 'Corporate_P...
Today, 2:54:09 PM			admin	Create Object	PoliciesCollection	Corporate_Policy	@all_inter... Icon: 'Appl... Name: 'Cor... Pol
Today, 2:54:09 PM			admin	Create Object	Nat Section		
Today, 2:54:09 PM			admin	Create Section	Nat Section	Manual Lower Rul...	Name: 'Manual Lower Rules'
Today, 2:54:09 PM			admin	Create Layer	Nat Rulebase		
Today, 2:54:09 PM			admin	Create Layer	Access Control Rulebase	Corporate_Policy...	Name: 'Corpor... Layer Name: 'C... Policy Nar
Today, 2:54:09 PM			admin	Create Object	Tag	HQ	Name: 'HQ'

You can use the Query box to search for specific changes. Search for "Cleanup". Do you see a result? Did you have multiple Sessions? Was naming the Cleanup rule part of this Revision?

Looking at Logs

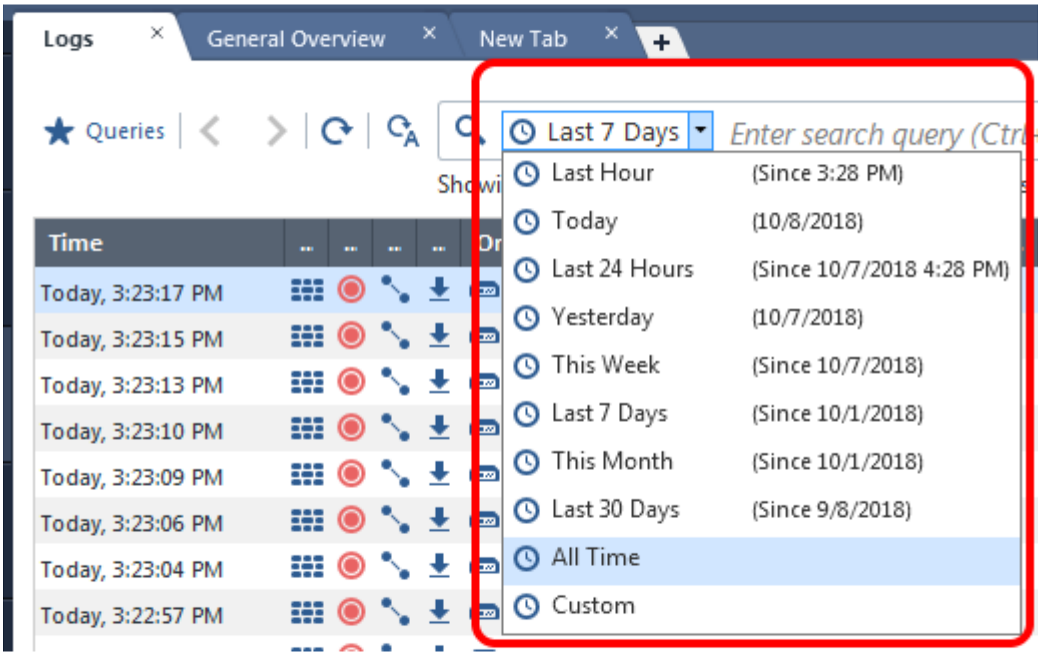
Browse to the **LOGS & MONITOR** Tab. Since we are not passing traffic through the gateway, we are probably just Dropping some traffic from the local network.



Showing first 50 results (608 ms) out of at least 79 results

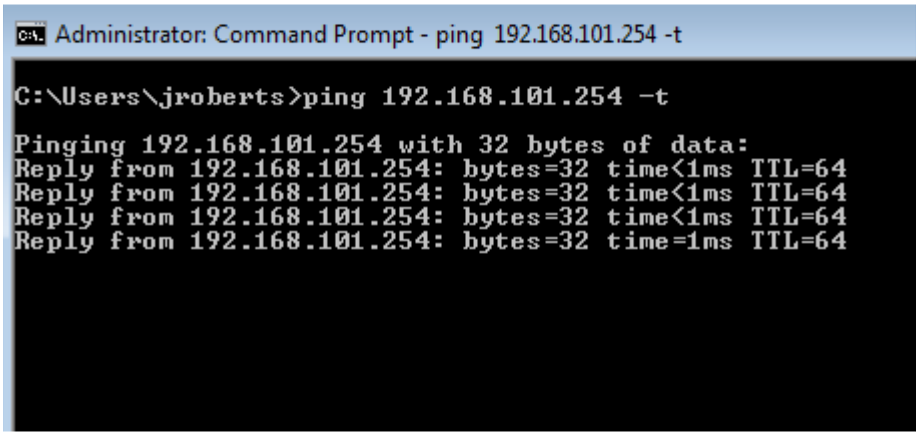
Time	...	...	...	...	Origin	Source	Source User...	De
Today, 3:23:17 PM					R80	win-victim (192....		
Today, 3:23:15 PM					R80	192.168.102.1		19
Today, 3:23:13 PM					R80	win-victim (192....		wi
Today, 3:23:10 PM					R80	win-victim (192....		wi
Today, 3:23:09 PM					R80	win-victim (192....		
Today, 3:23:06 PM					R80	192.168.102.1		19
Today, 3:23:04 PM					R80	192.168.102.1		19
Today, 3:22:57 PM					R80	192.168.101.1		19
Today, 3:22:53 PM					R80	192.168.101.1		19

The default search timeframe is 7 Days, but you can search for other options. Click **Last 7 Days** to see the options.



Last Hour	(Since 3:28 PM)
Today	(10/8/2018)
Last 24 Hours	(Since 10/7/2018 4:28 PM)
Yesterday	(10/7/2018)
This Week	(Since 10/7/2018)
Last 7 Days	(Since 10/1/2018)
This Month	(Since 10/1/2018)
Last 30 Days	(Since 9/8/2018)
All Time	
Custom	

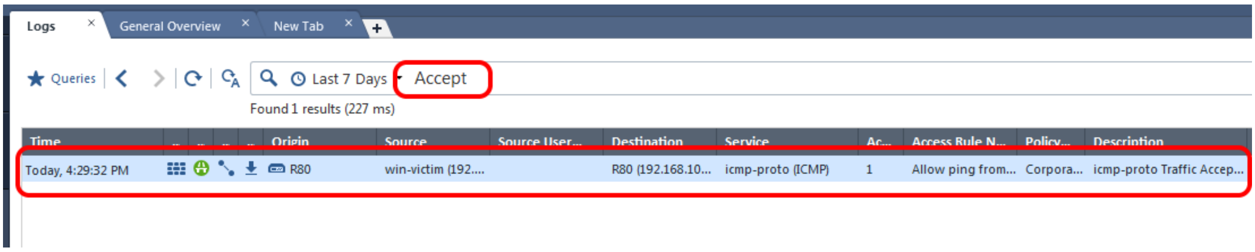
Open cmd.exe on the Windows GUI and ping the IP address of your Check Point Gateway



Administrator: Command Prompt - ping 192.168.101.254 -t

```
C:\Users\jroberts>ping 192.168.101.254 -t

Pinging 192.168.101.254 with 32 bytes of data:
Reply from 192.168.101.254: bytes=32 time<1ms TTL=64
Reply from 192.168.101.254: bytes=32 time<1ms TTL=64
Reply from 192.168.101.254: bytes=32 time<1ms TTL=64
Reply from 192.168.101.254: bytes=32 time=1ms TTL=64
```

Now Search for "Accept" in Logs.

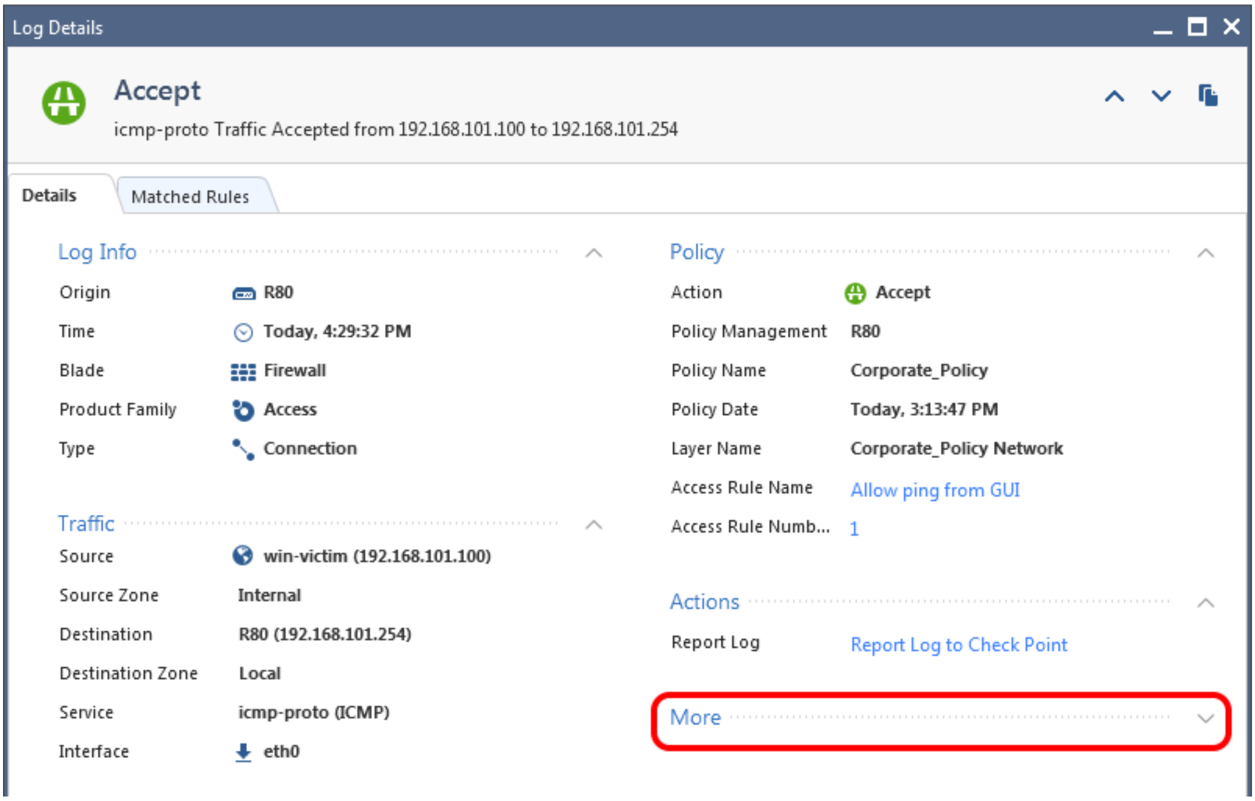


Accept

Found 1 results (227 ms)

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 4:29:32 PM					R80	win-victim (192....		R80 (192.168.10...	icmp-proto (ICMP)	1	Allow ping from...	Corpora...	icmp-proto Traffic Accep...

Double-click the log entry to view the details.



Accept

icmp-proto Traffic Accepted from 192.168.101.100 to 192.168.101.254

Log Info

Origin	R80
Time	Today, 4:29:32 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	win-victim (192.168.101.100)
Source Zone	Internal
Destination	R80 (192.168.101.254)
Destination Zone	Local
Service	icmp-proto (ICMP)
Interface	eth0

Policy

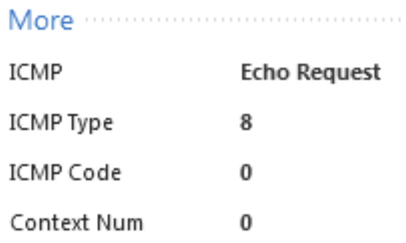
Action	Accept
Policy Management	R80
Policy Name	Corporate_Policy
Policy Date	Today, 3:13:47 PM
Layer Name	Corporate_Policy Network
Access Rule Name	Allow ping from GUI
Access Rule Numb...	1

Actions

Report Log	Report Log to Check Point

More

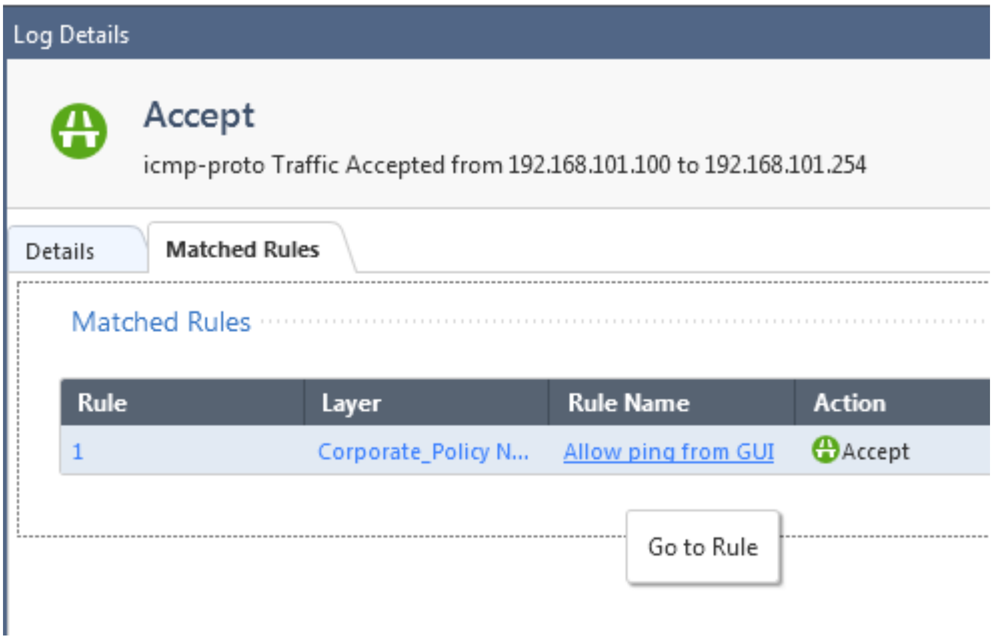
Click on "More" to see more details about the Protocol/Service in use. In this case, we see ICMP Type 8 (aka Echo request)



More

ICMP	Echo Request
ICMP Type	8
ICMP Code	0
Context Num	0

Click on the **Matched Rules** tab. You can go to the Rule in the Policy by clicking the links shown on this Tab.



Log Details

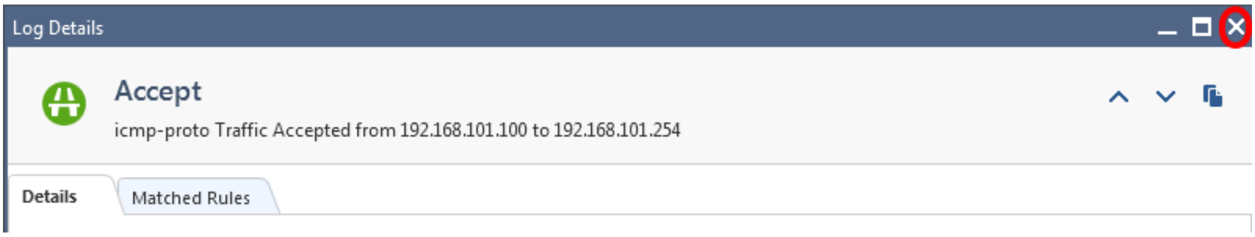
Accept

icmp-proto Traffic Accepted from 192.168.101.100 to 192.168.101.254

Matched Rules

Rule	Layer	Rule Name	Action
1	Corporate_Policy N...	Allow ping from GUI	Accept

Click the red **X** in the upper right to close the Log Details.



Log Details

Accept

icmp-proto Traffic Accepted from 192.168.101.100 to 192.168.101.254