

Introduction (Part 2)

Important Information

Prerequisite

This activity assumes successful completion of Part 1: Understand and Configure Enterprise Network with S-DC & L-DC (SWANSEA.ACCA).

Fundamental procedures—such as virtual machine installation and network adapter configuration—are not repeated here, as they were covered in Part 1.

Activity Sequence: Complete the tasks in the following order:

1. Installation of Check Point (GAiA) Appliances

Deploy the following components:

A-GUI (Management Interface), A-SMS (Security Management Server), A-GW (Security Gateway)

2. Configuration of Check Point (GAiA) Appliances

- a. Perform initial setup and policy configuration on all deployed appliances.

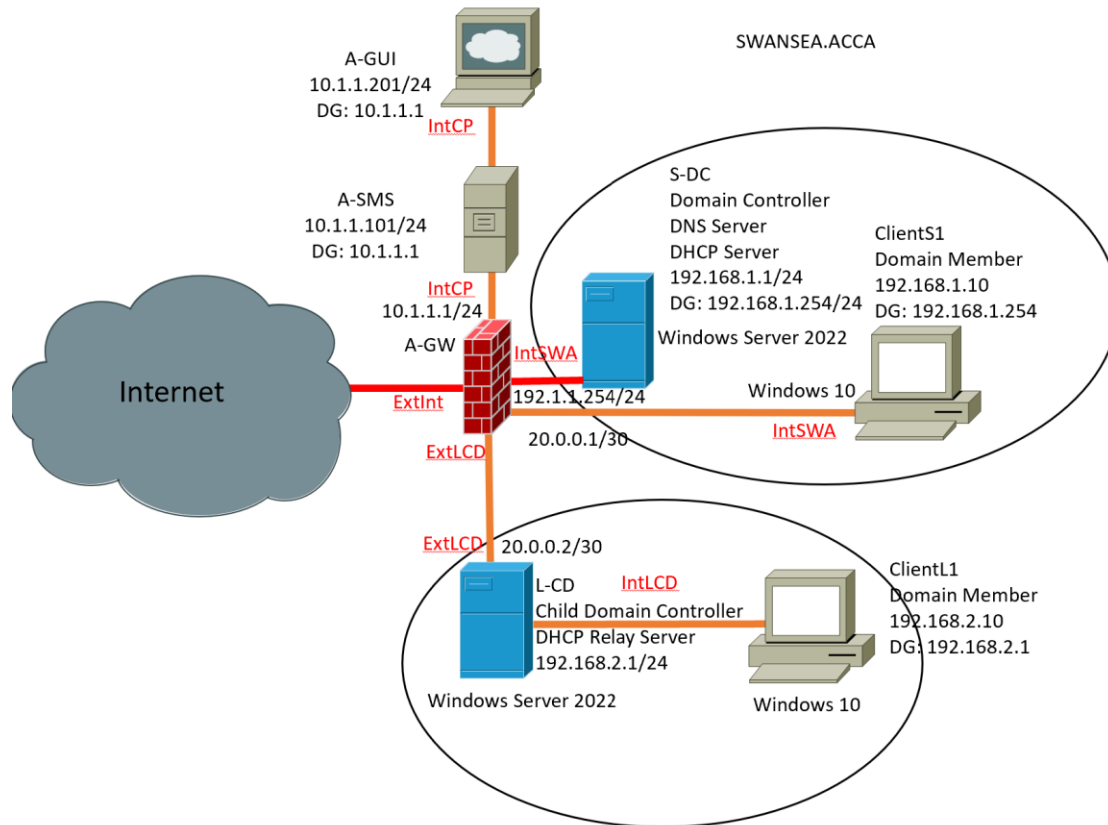
3. Interconnect S-DC and Check Point (GAiA) Networks

- a. Establish and verify connectivity between the S-DC network and the Check Point infrastructure.

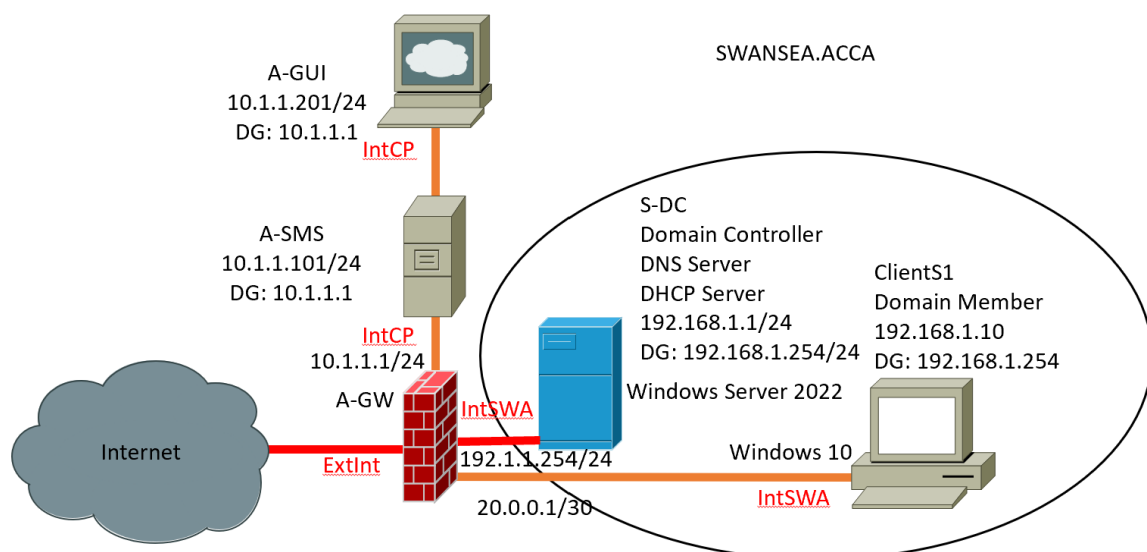
4. Enforce Security on the S-DC Network

- a. Implement and test security policies to protect the S-DC environment.

Demonstration Requirement: In addition to the core tasks, configure and enforce security policies for the L-DC network as part of your final demonstration.



Initial Focus to Setup the Appliances

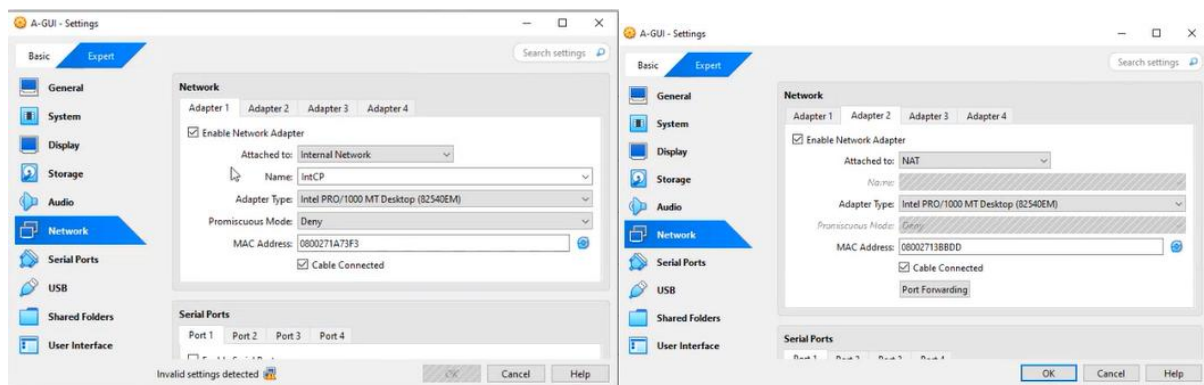


IP Addressing Summary

Component	Role	IP Address	Default Gateway	Configs
A-GUI	SmartConsole + GUI Access	10.1.1.201/24	10.1.1.1	Win 10 – 8 GB RAM 60 GB HDD
A-SMS	Security Management Server	10.1.1.101/24	10.1.1.1	CP R81.20 – 8 GB RAM – (60-80) GB HDD
A-GW	Security Gateway	10.1.1.1/24, 192.1.1.254/24, 20.0.0.1/30	-	CP R81.20 – 8 GB RAM – (60-80) GB HDD
S-DC	Primary Domain Controller (SWANSEA.ACCA)	192.168.1.1/24	192.168.1.254	Pre Configured
ClientS1	Windows 10 Domain Member	192.168.1.10/24	192.168.1.254	Pre Configured
L-CD	Child Domain Controller (LONDON.SWANSEA.ACCA)	192.168.2.1/24, 20.0.0.2/30	-	Pre Configured
ClientL1	Windows 10 Domain Member	192.168.2.10/24	192.168.2.1	Pre Configured

Make sure the adapter settings are correctly configured.

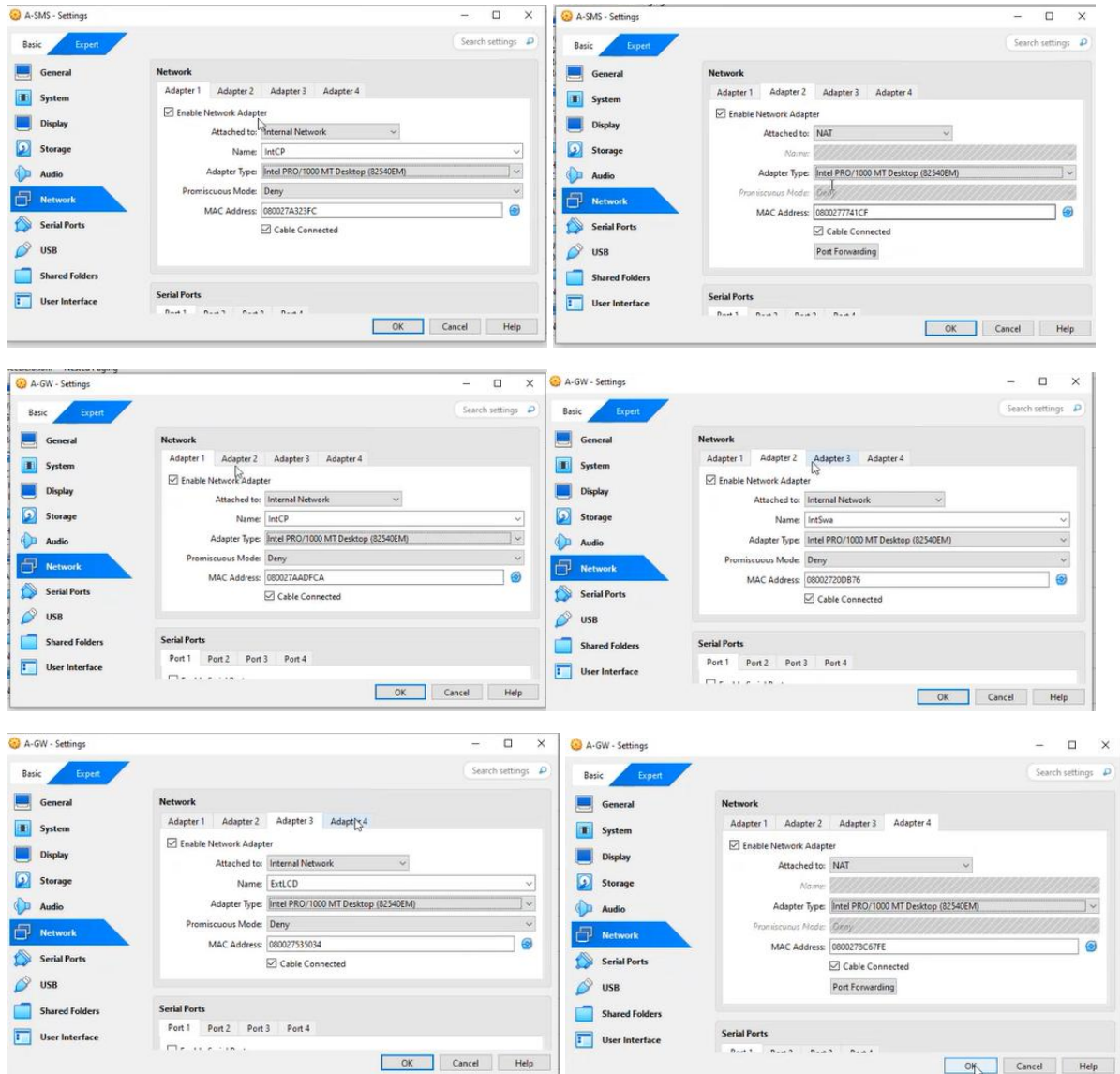
A_GUI



A_SMS

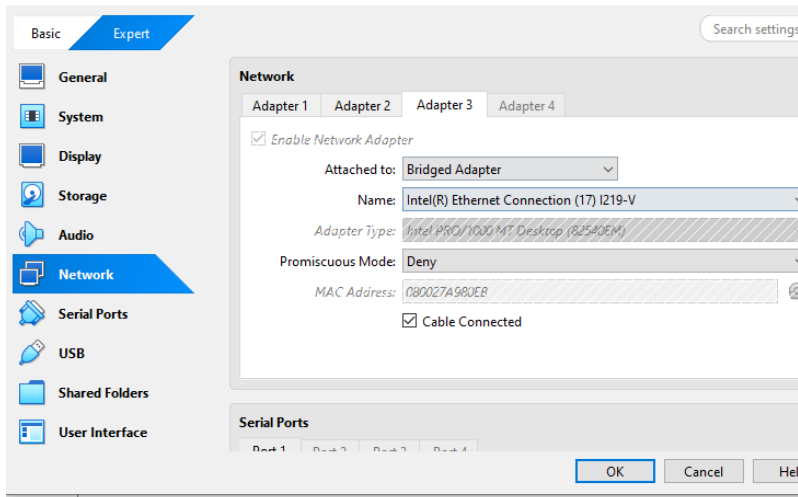
Checkpoint Appliances Installation Guide

ACCA7032 Enterprise Network Security

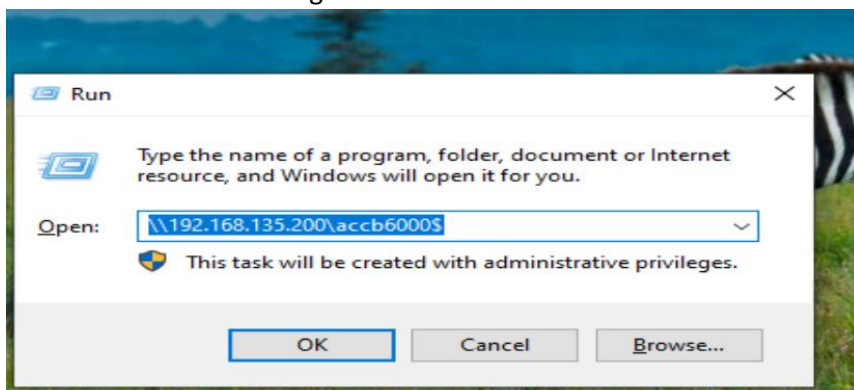


Installation of SmartConsole on A-GUI

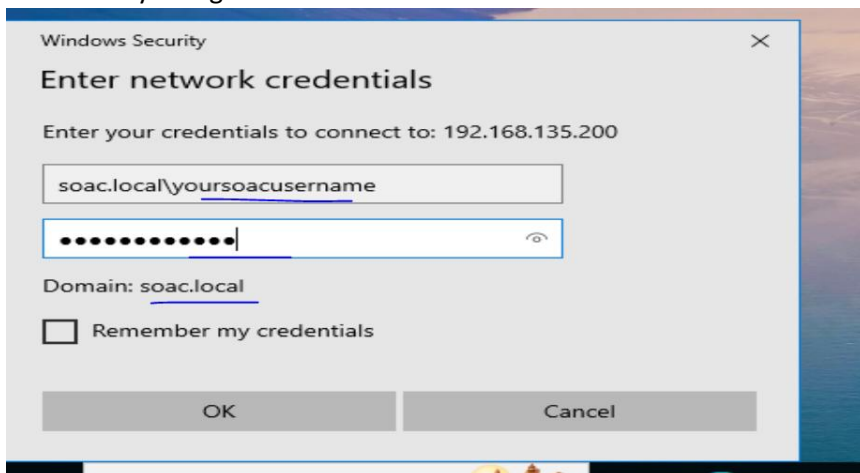
1. Download the ISO's from [\\192.168.135.200\accb6000\\$\\VM](\\192.168.135.200\accb6000$\\VM).
 2. Look for ENS Downloads (Only) Folder
 3. Install Win 10 OS (Refer to the Table above for Configurations).
 4. Start the A-GUI machine.
 5. To download the Licenses (you might need them later for your activities) and SMART Console, you need to connect to the Shared Folder.
- In order to do that, make sure you add a bridged adapter (later you might disable it)



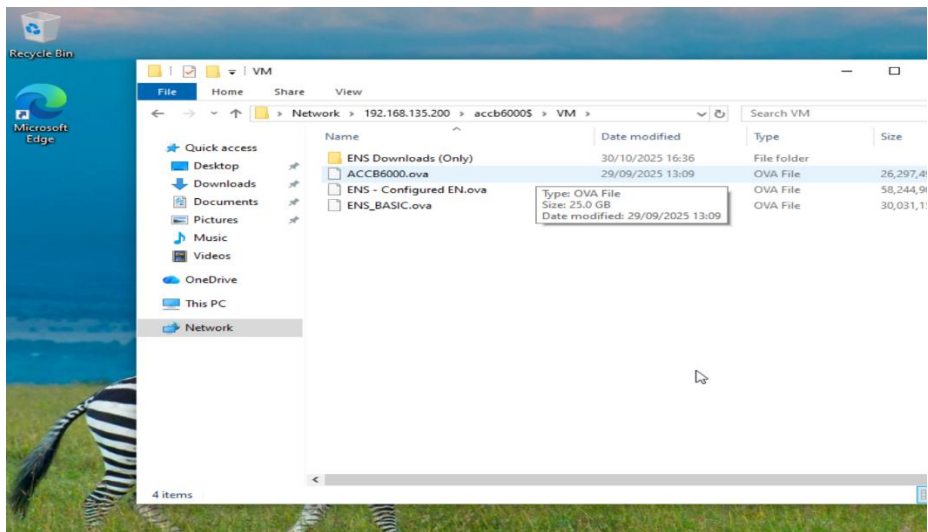
Use the run command to get into the Shared Folder



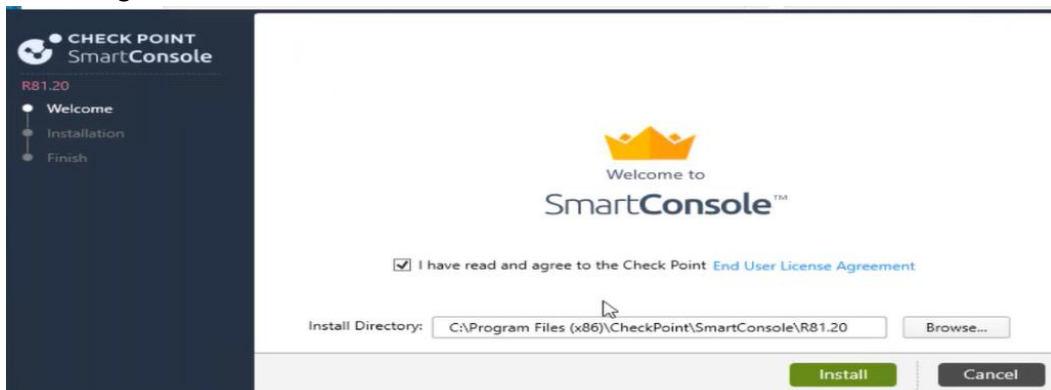
Make sure you login to SOAC.LOCAL



Open the ENS Downloads (Only) Folder and download the SMART CONSOLE and Licenses Folder



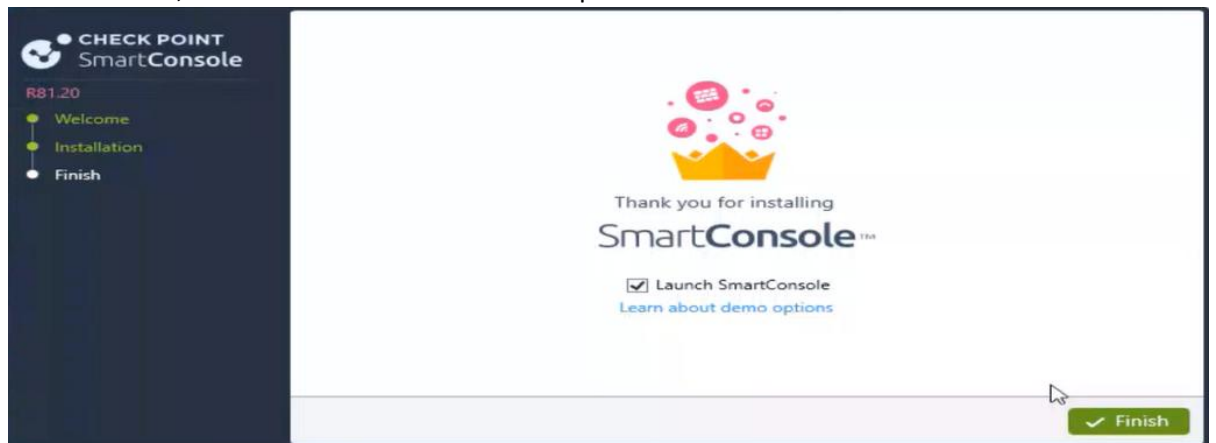
6. Install the Smart Console and Enable I have read and agree to the Check Point End User License Agreement and click install.



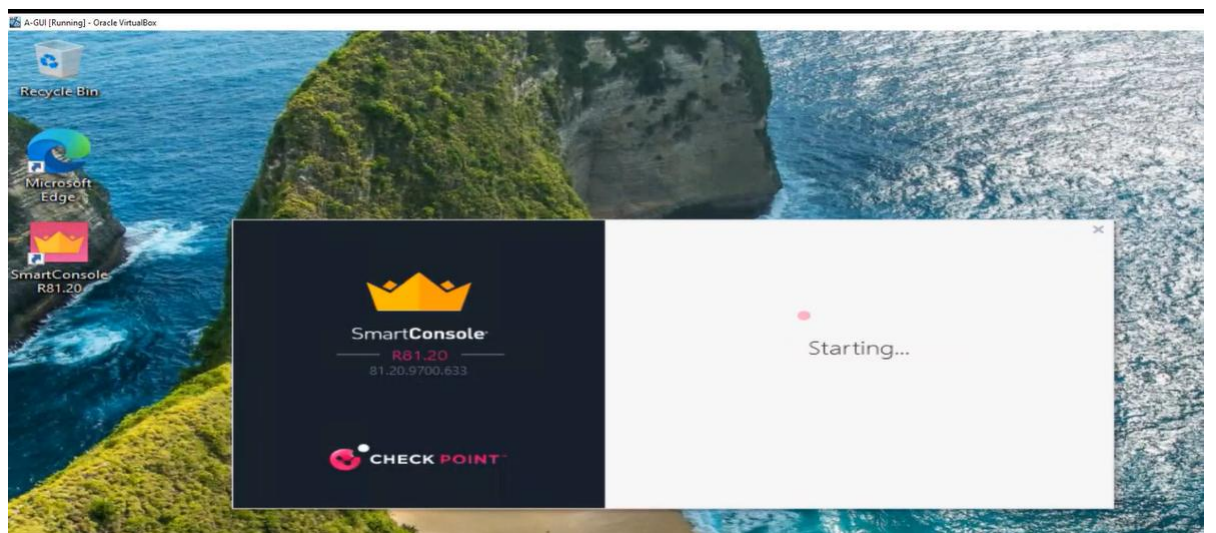
Smart Console will begin the installation.



7. Once installed, select the Finish button and complete the installation of Smart Console.



8. You could see Smart Console R81.20 in A-GUI desktop.

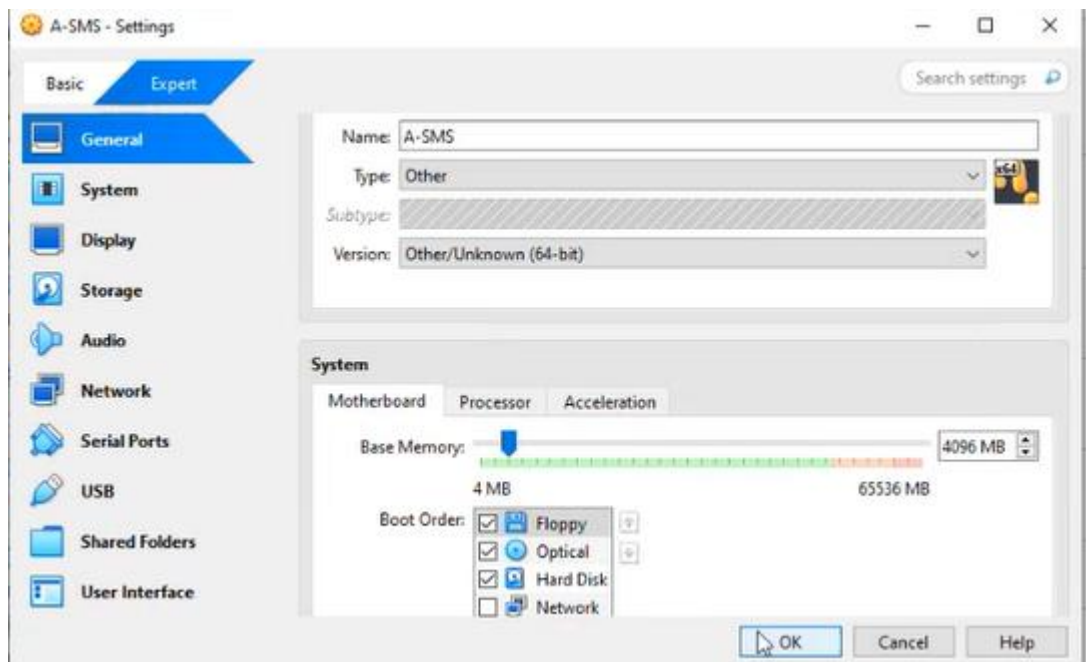


This is the end of the lab 1.

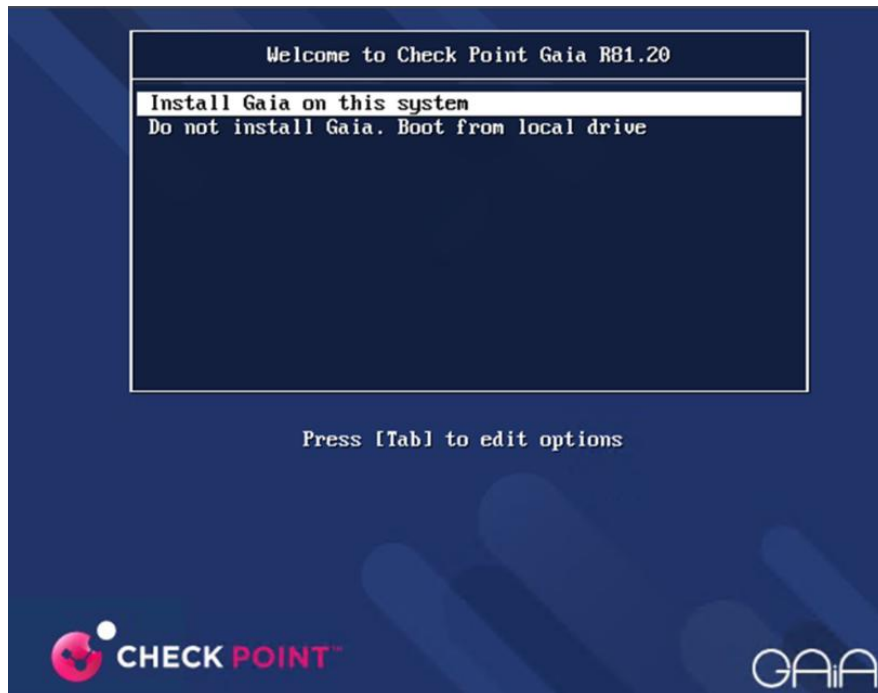
Chapter 2 : Installing the Primary Security Management Server (A-SMS)

In this lab, you will install the Gaia OS on A-SMS machine and configure the A-SMS as Security Management Server using First Time Wizard.

1. Download the GAIA ISO (R81.20) from [\\192.168.135.200\accb6000\\$\\VM](https://192.168.135.200/accb6000$\\VM).
2. Look for ENS Downloads (Only) Folder
3. Install GAIA OS (Refer to the Table above for Configurations).
4. Make sure you select Ubuntu in the OS.
5. Before power on A-SMS, go to the settings of A-SMS machine. Under General properties, make sure version refers to other/Unknown(64-bit)

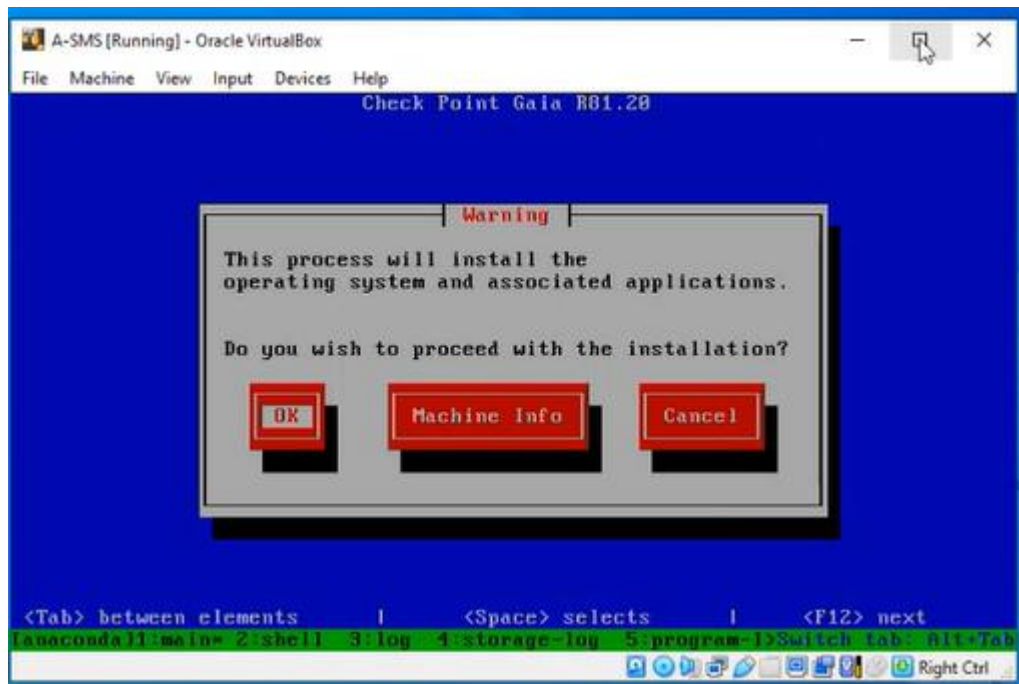


6. Mount to GaiaOS.iso and start the machine. When the system is started, the following screen appears:



7. Click on install Gaia on this system

A warning message will appear, select OK to continue the installation and press Enter



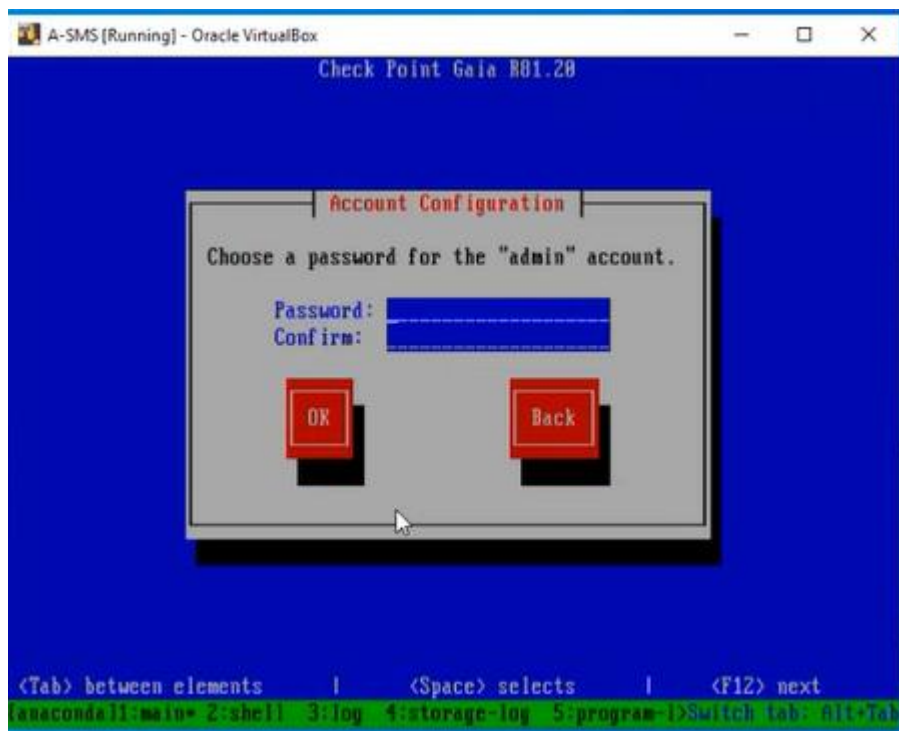
8. Select a keyboard language. US is the default, select Great Britain version:



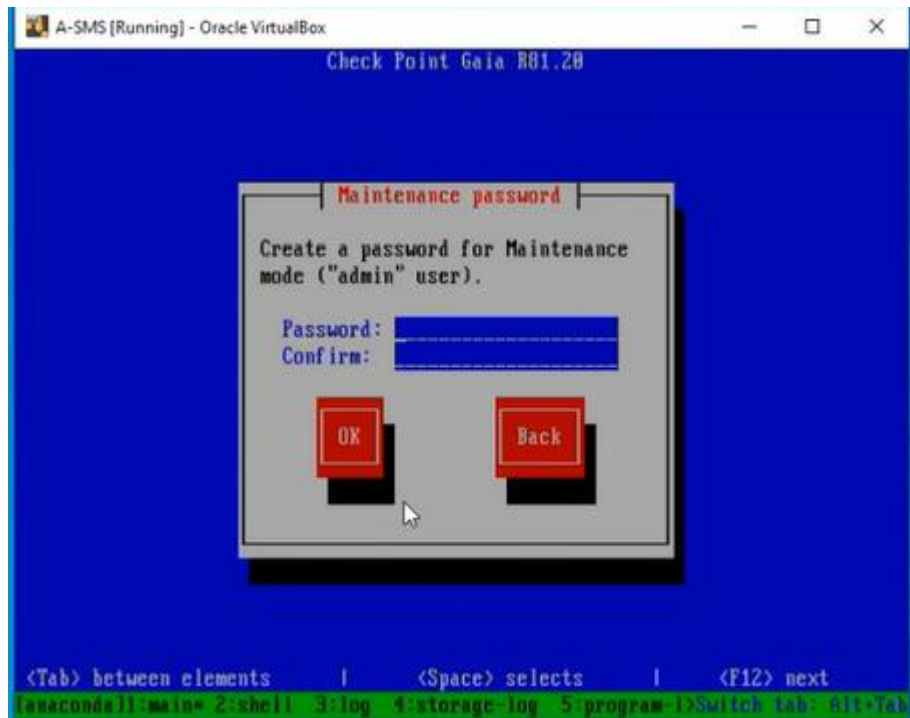
9. Check the partition configuration. The disk space depends on your system configuration. So, don't change it. Press TAB key to select the OK button and press Enter.



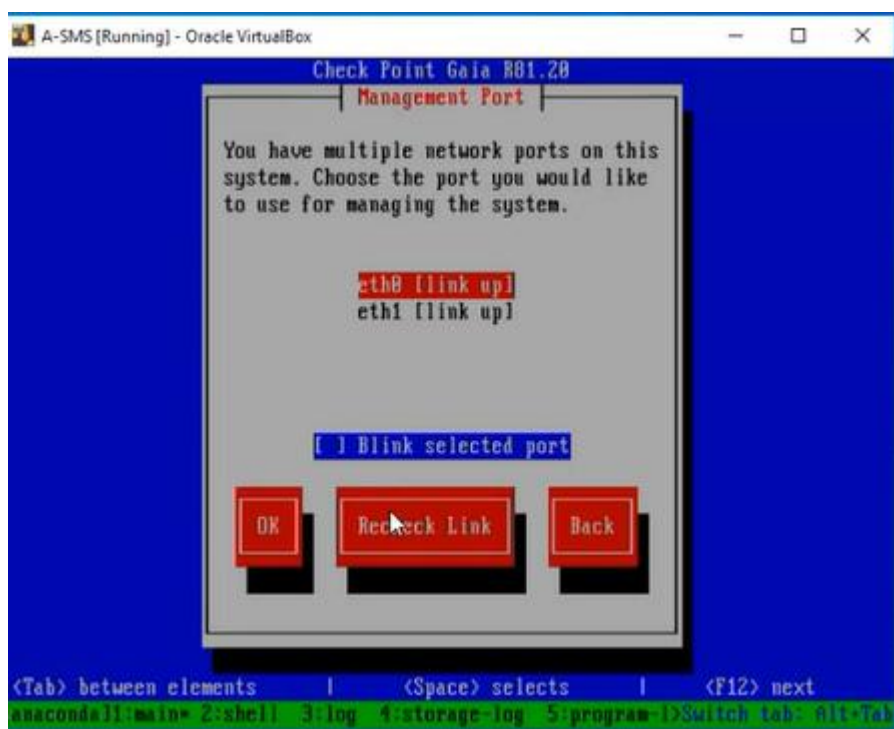
10. Enter the password for the admin account and confirm it. You can use any password. For this document, Chkp1234 is used as password.



11. Enter the password for Maintenance admin password. For this documentation, Chkpl234 has been used as a password. You can choose any password of your choice. Make sure you remember it.
12. Click OK to continue.



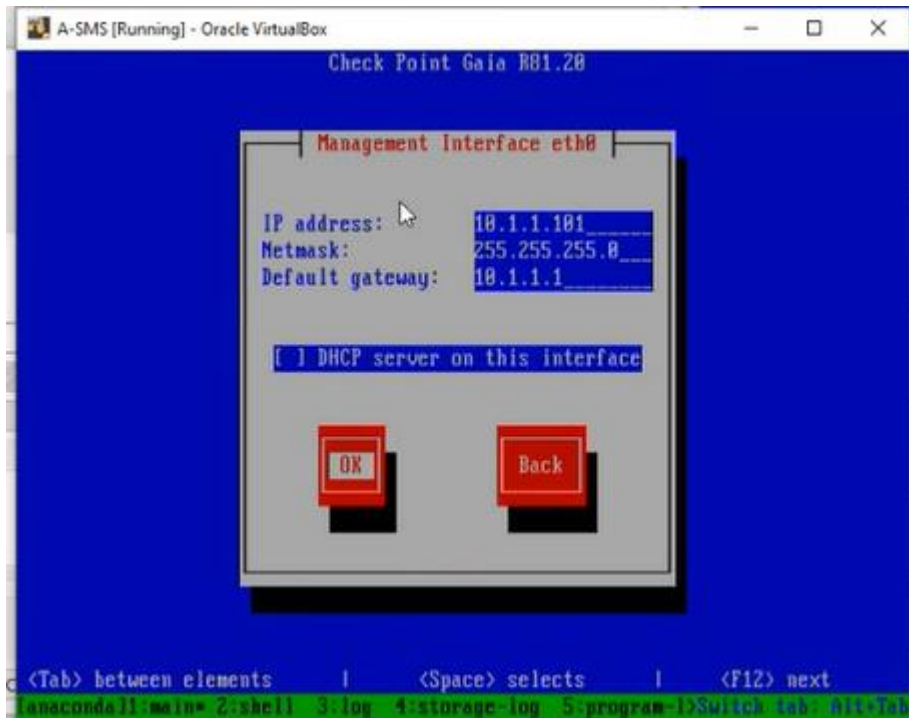
13. Choose the eth0 port to configure A-SMS interface. Click OK to continue.



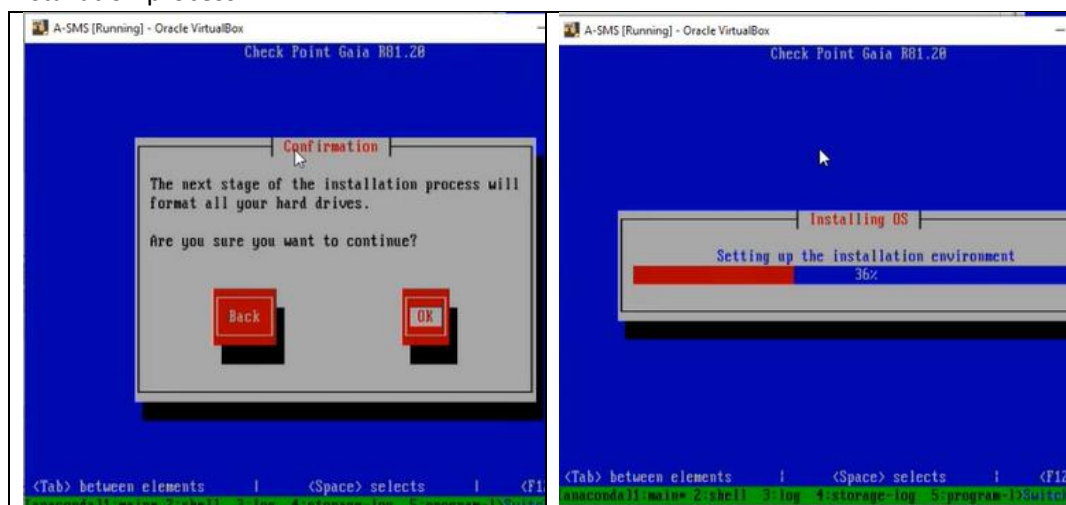
14. Enter the system configuration for A-SMS.

IP address	10.1.1.101
Netmask	255.255.255.0
Default Gateway	10.1.1.1
DHCP server on this interface	Disabled (Default)

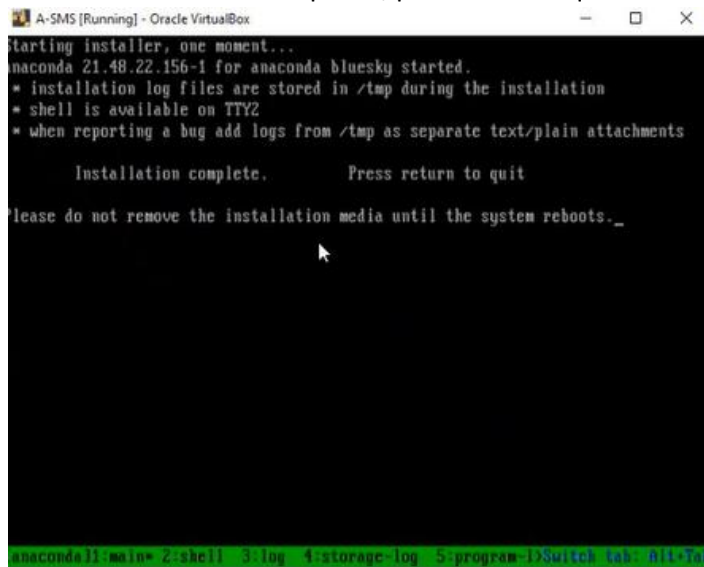
15. Select OK and press Enter to continue.



16. Select OK to confirm the installation of GAIA OS in the A-SMS. Press Enter to start the installation process.



17. After the installation completes, press Enter to quit the installer process.



```

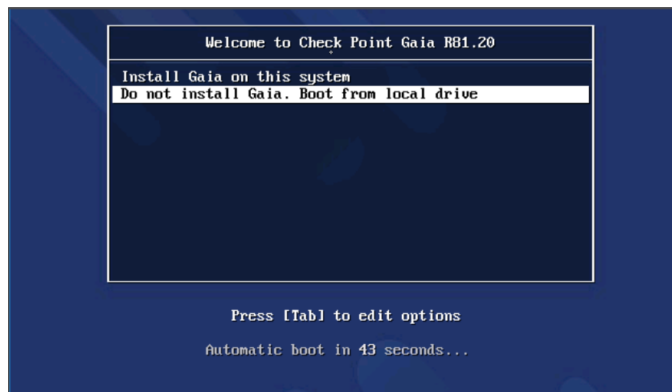
A-SMS [Running] - Oracle VirtualBox
Starting installer, one moment...
anaconda 21.48.22.156-1 for anaconda bluesky started.
* installation log files are stored in /tmp during the installation
* shell is available on TTY2
* when reporting a bug add logs from /tmp as separate text/plain attachments

Installation complete.      Press return to quit

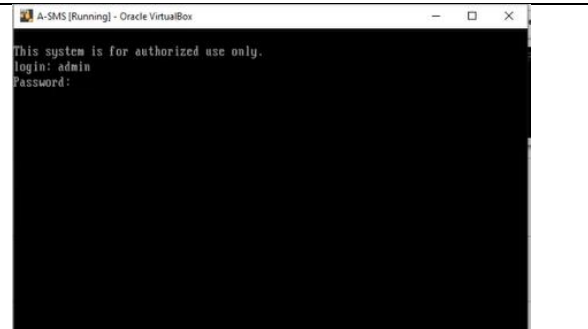
Please do not remove the installation media until the system reboots._

anacondall:main= 2:shell 3:log 4:storage-log 5:program-l3Switch tab: Rll+Tab
  
```

18. After the reboot, choose **Do not install Gaia. Boot from local drive** and press Enter.



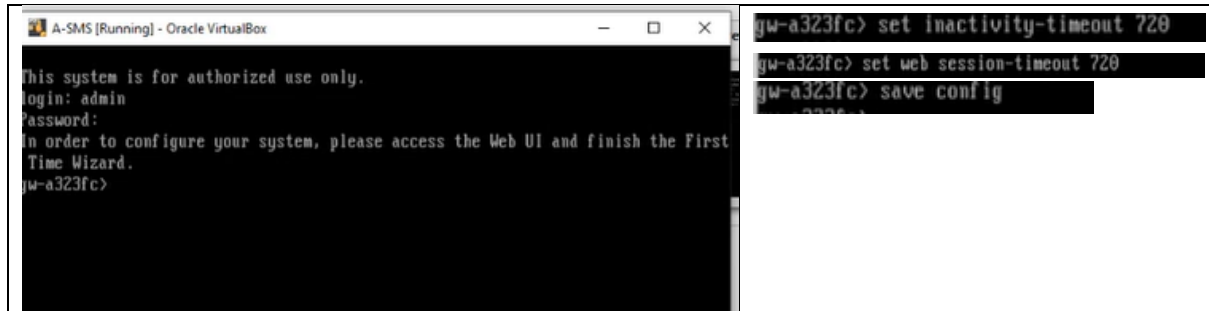
19. When the system reboots, it will ask for login details to login to the Gaia OS. Use the following details:

Username: admin Password: Chkp!234	
--	--

20. Once login, Set the inactivity and web session timeouts and save the configuration using save config

```

set inactivity-timeout 720
set web session-timeout 720
save config
  
```



21. Type Exit and press Enter to logout the A-SMS console window.

Checkpoint Appliances Installation Guide

ACCA7032 Enterprise Network Security

Chapter: 2.1 Configuring Security Management Server(A-SMS) through the First Time Wizard

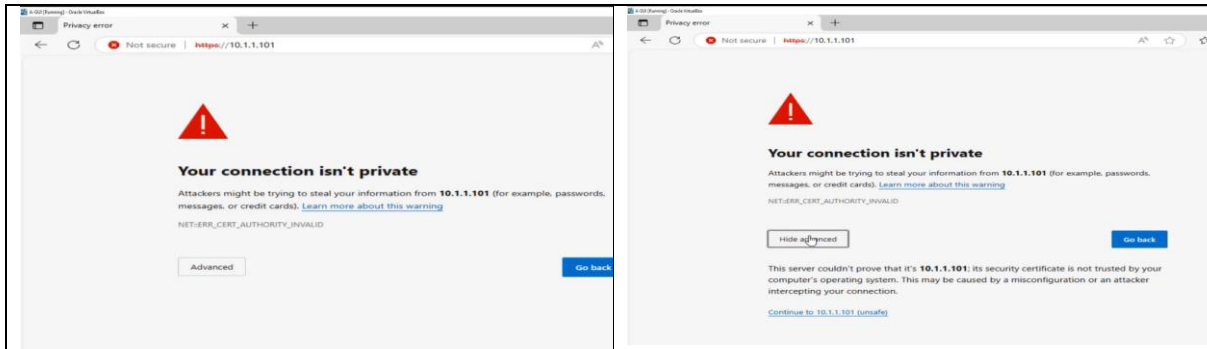
Access the Web UI and finish the First Time Wizard on the A-SMS machine.

2.1.1 Go to A-GUI, open a web browser.

2.1.2 Use the following URL to access the A-SMS through web portal from A-GUI

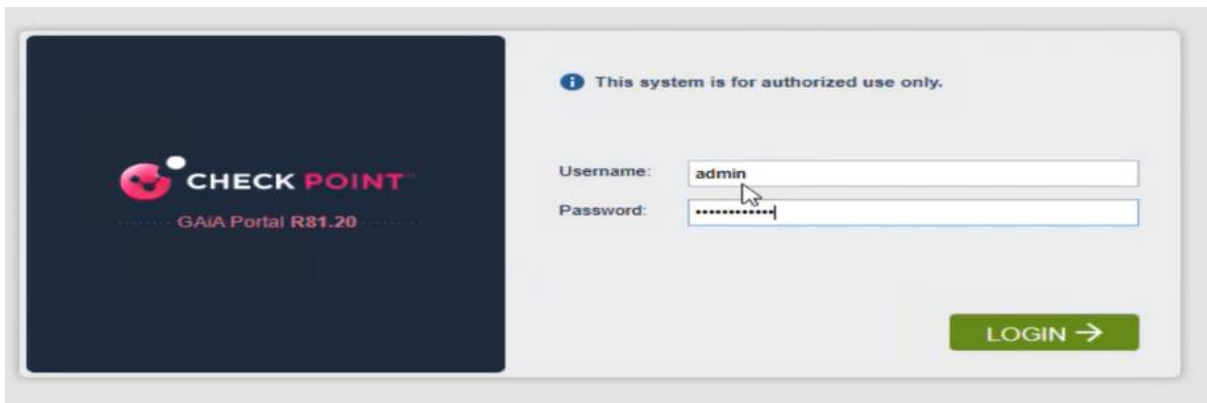
<http://10.1.1.101>

2.1.3 You might see a warning message as shown below, select **Advanced** and continue

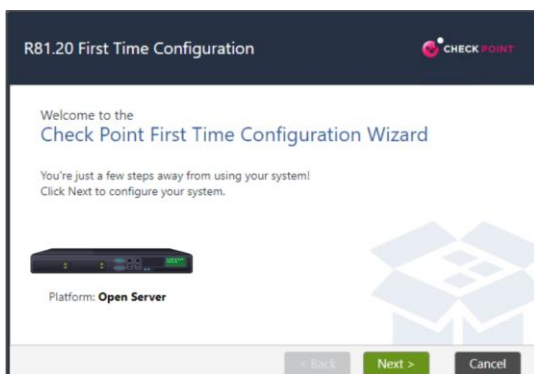


2.1.4 Use the admin login that you have created during the A-SMS installation to log in to the A-SMS using Gaia portal from Web GUI.

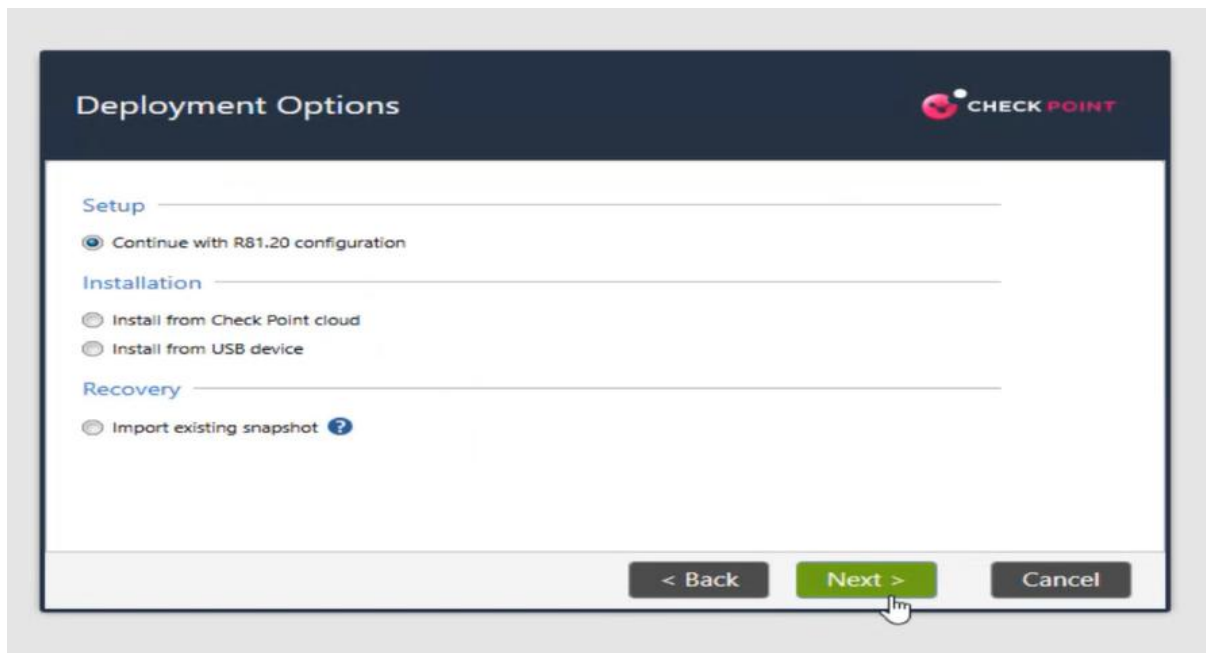
Username: admin
Password: Chkp!234



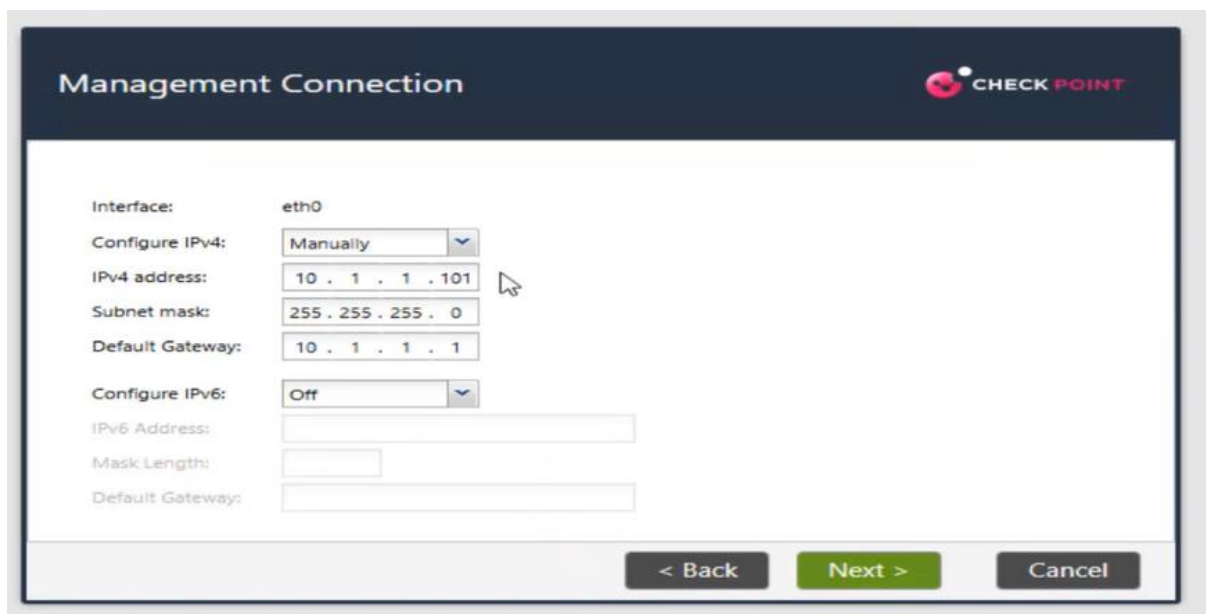
You will see the following welcome screen from the First Time Wizard to configure A-SMS



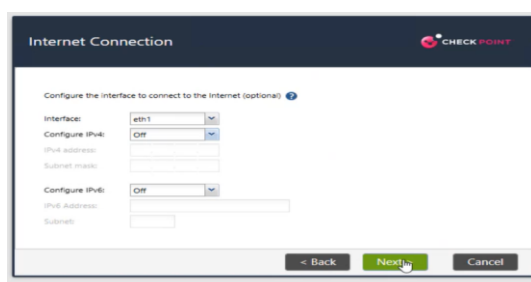
2.1.5 Select **Continue with R81.20 configuration** and click **Next** to continue



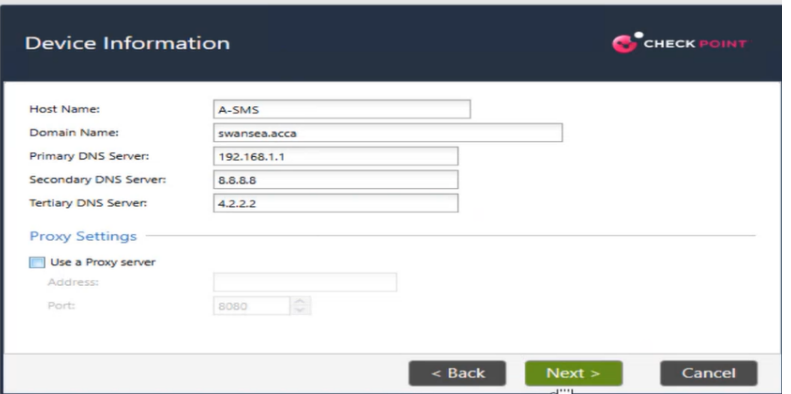
2.1.6 Check the settings on the **Management Connection** page is correct and click on **Next** to continue.



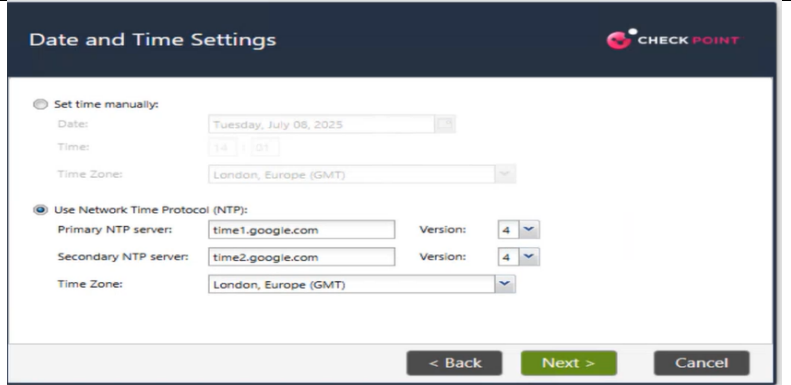
Leave the settings as it is from the following screen.



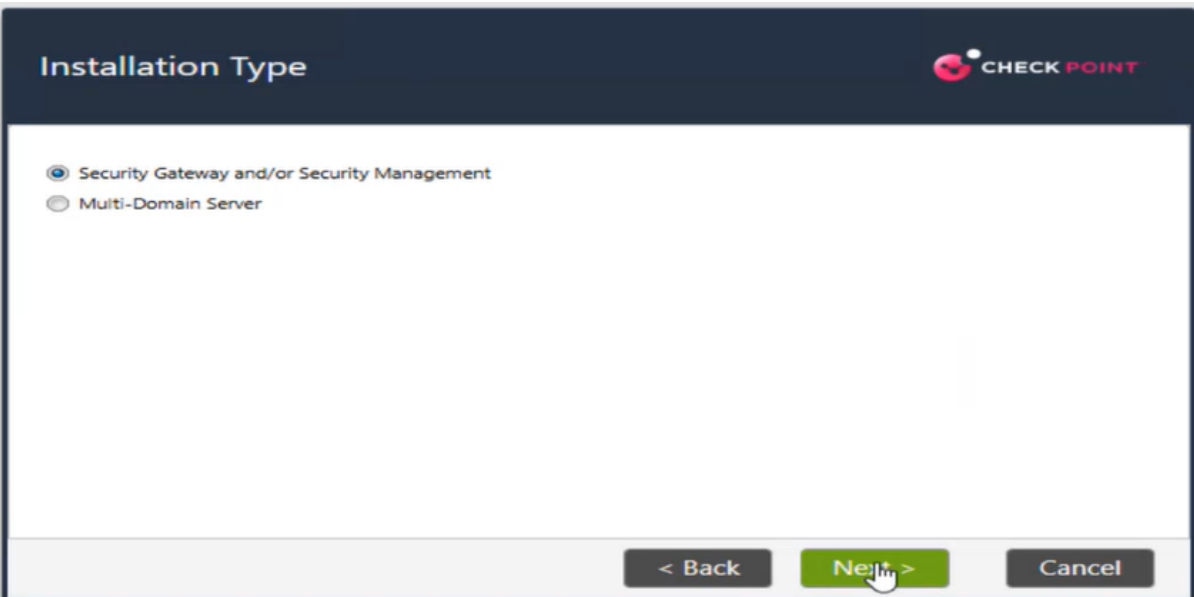
2.1.7 Configure the A-SMS using the Device Information and select **Next** to continue

Hostname : A-SMS Domain Name : swansea.acca Primary DNS Server : 192.168.1.1 Secondary DNS : 8.8.8.8 Tertiary DNS Server : 4.2.2.2	
---	--

2.1.8 Select use **Network Time Protocol** on the Date and Time Settings page. Configure the NTP servers with time.google.com. Also choose **London,Europe(GMT)** for the Time Zone. Select **Next** to continue.

Primary NTP Server : time1.google.com Secondary NTP Server : time2.google.com	
--	---

2.1.9 On the installation type, select **Security Gateway and/or Security Management** and select **Next** to continue.



2.1.10 Select **Security Management** option from the Products page and ensure **Security Gateway** is disabled. Verify the **Define Security Management** is set to Primary. Select **Next** to continue

2.1.11 Choose **Define a new administrator** from the Security Management Administrator page and configure new administrator. You can use any username and password (This is going to be used to login to A-SMS from Smart Console. For this documentation, the following details were used. Select **Next** to continue

Administrator Name : cadmin Password : Chkp!234	
--	--

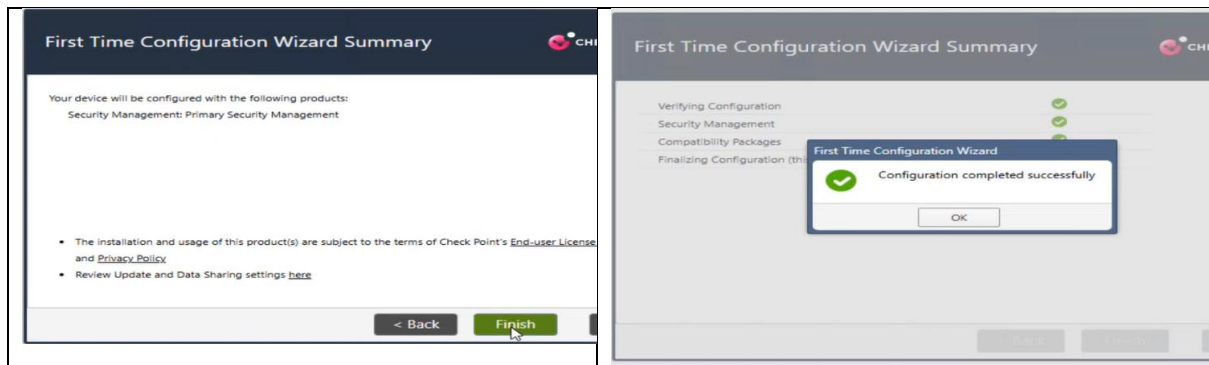
2.1.12 Select the **Network** option the **Security Management GUI Clients** page and use the following details. Choose **Next** to continue

IP Address : 10.1.1.0 Subnet : 255.255.255.0	
---	--

Checkpoint Appliances Installation Guide

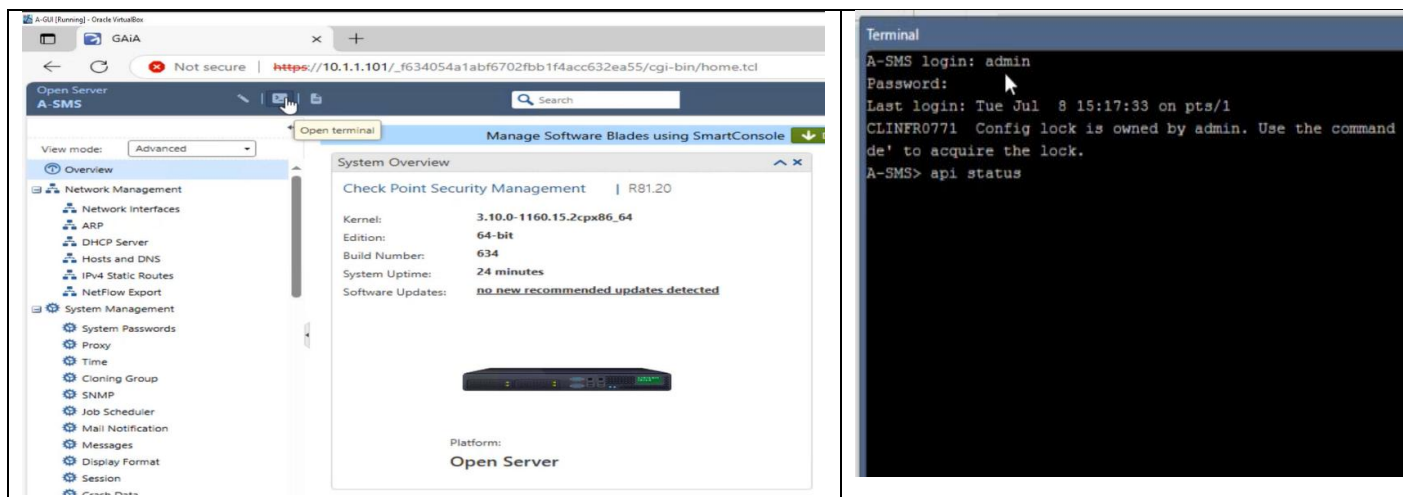
ACCA7032 Enterprise Network Security

2.1.13 Make sure the First Time Configuration Wizard Summary shows only **Security Management: Primary Security Management**, select **Finish** to finalise the configuration.

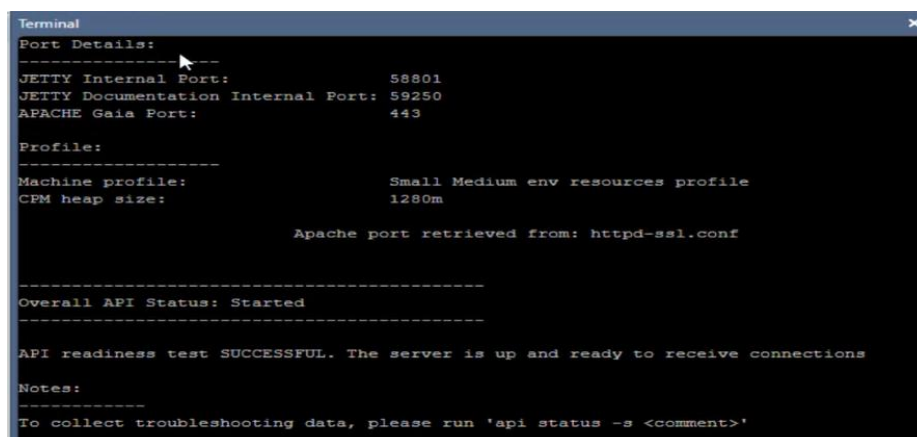


2.1.14 Select **OK** to confirm the configuration.

2.1.15 Click Open Terminal and run the command **api status** to check the API readiness test to check the status of the A-SMS startup process.

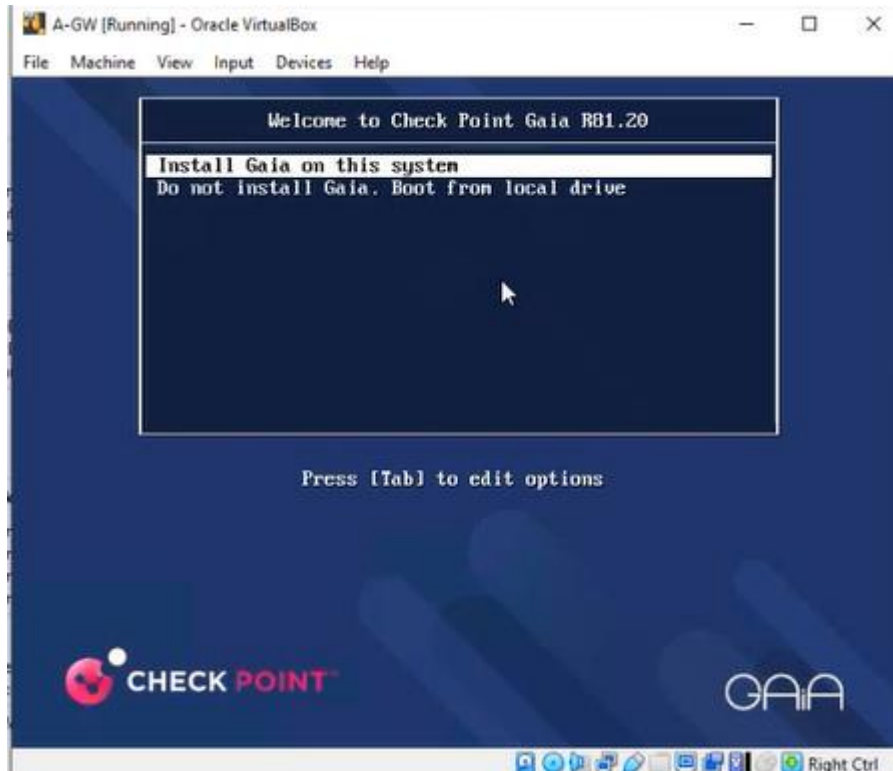


2.1.16 You should see API readiness test Successful. You may need to run the command more than once to get the SUCCESSFUL message. Exit the terminal using **exit** command.

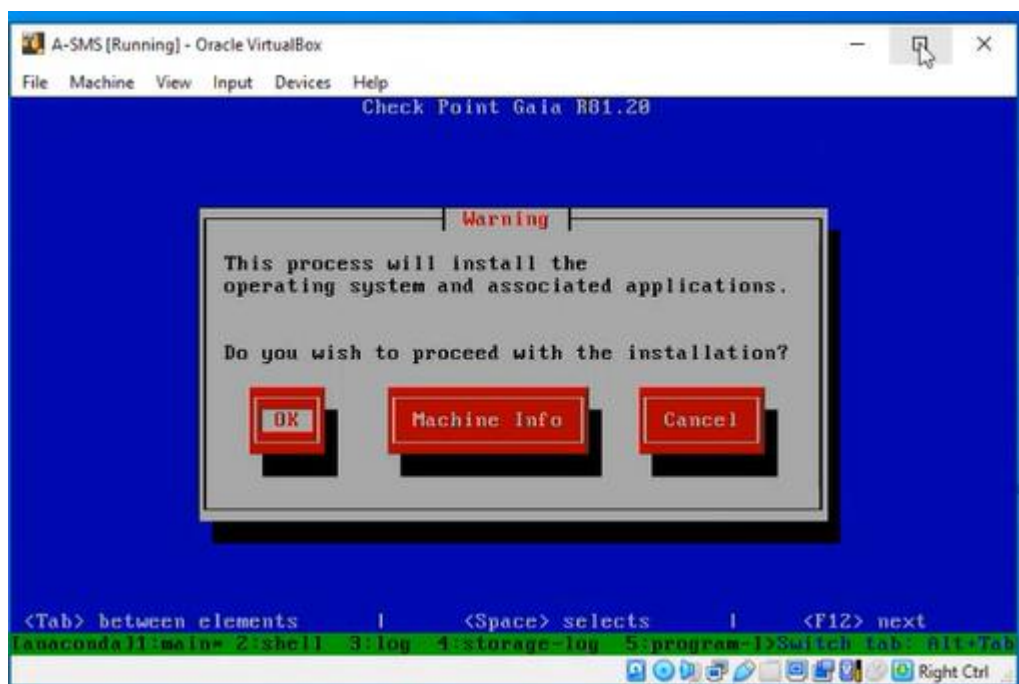


Chapter 3: Installation of the Check Point Gateway (A-GW)

1. Install GAIA OS (Refer to the Table above for Configurations).
2. Make sure you select Ubuntu in the OS.
3. Turn on A-GW machine.



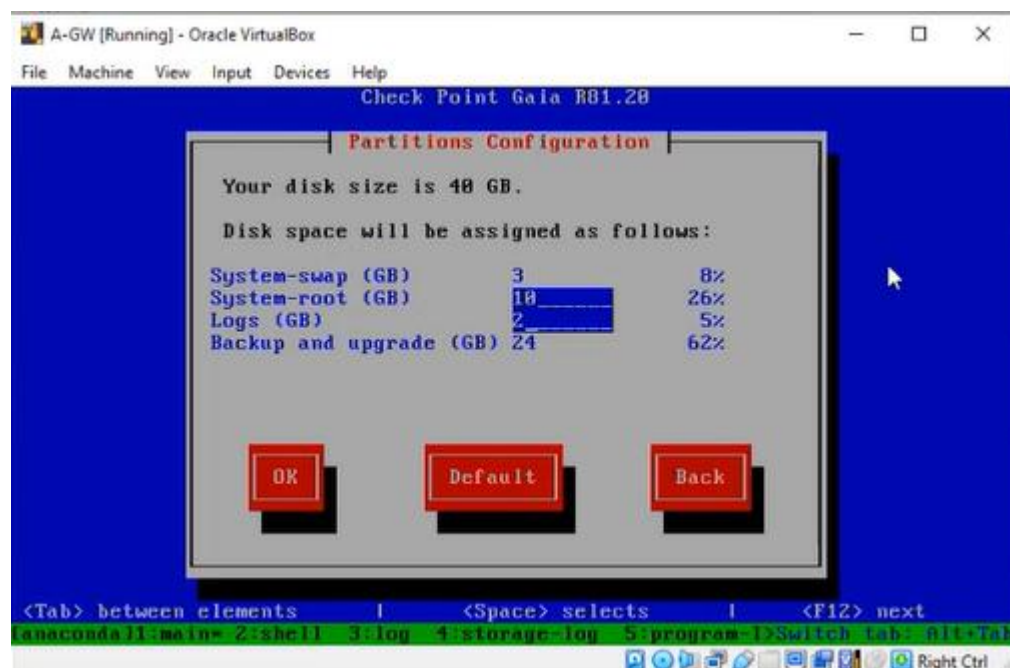
4. A warning message will appear, select **OK** to continue the installation and press **Enter**



5. Select a keyboard language. US is the default, select **Great Britain** version:



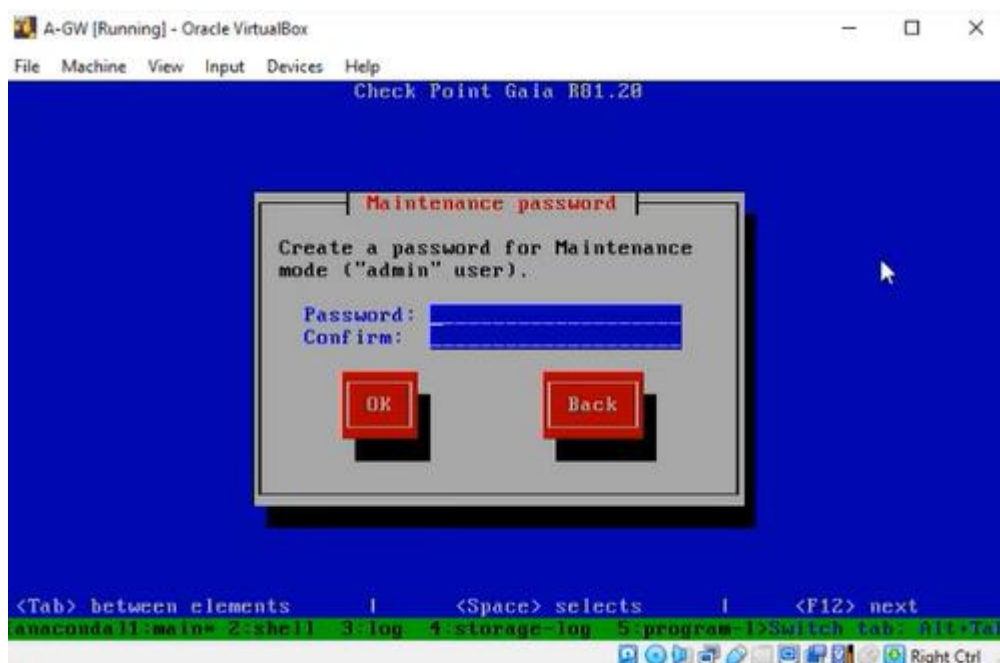
6. Check the partition configuration. The disk space depends on your system configuration. So, don't change it. Press TAB key to select the **OK** button and press Enter.



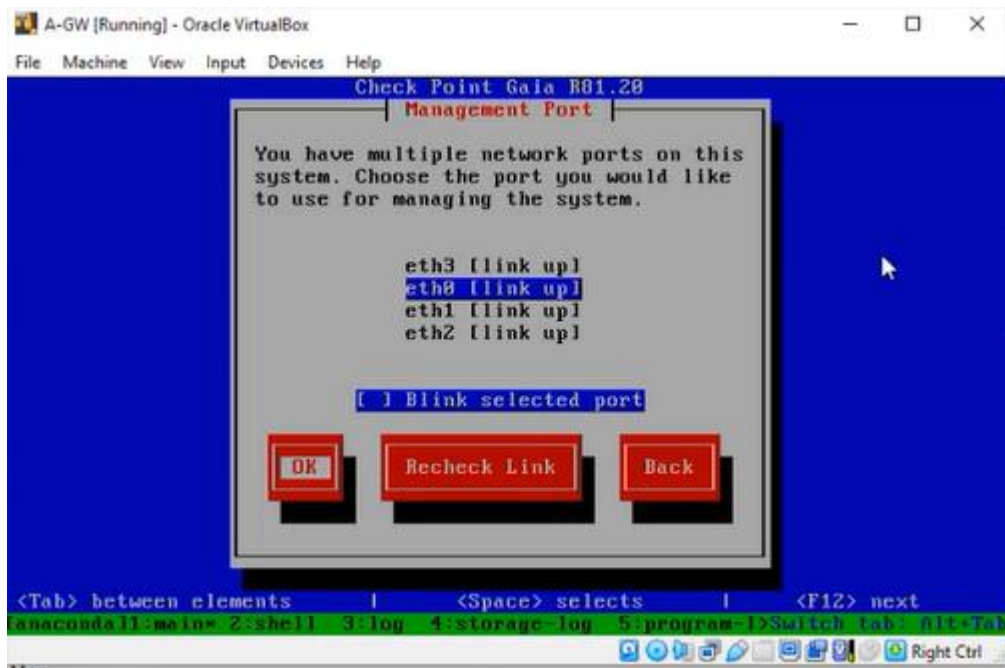
7. Enter the password for the admin account and confirm it. You can use any password. For this document, **Chkp!234** is used as password.



8. Enter the password for Maintenance admin password. For this documentation, **Chkp!234** has been used as a password. You can choose any password of your choice. Make sure you remember it. Click **OK** to continue.



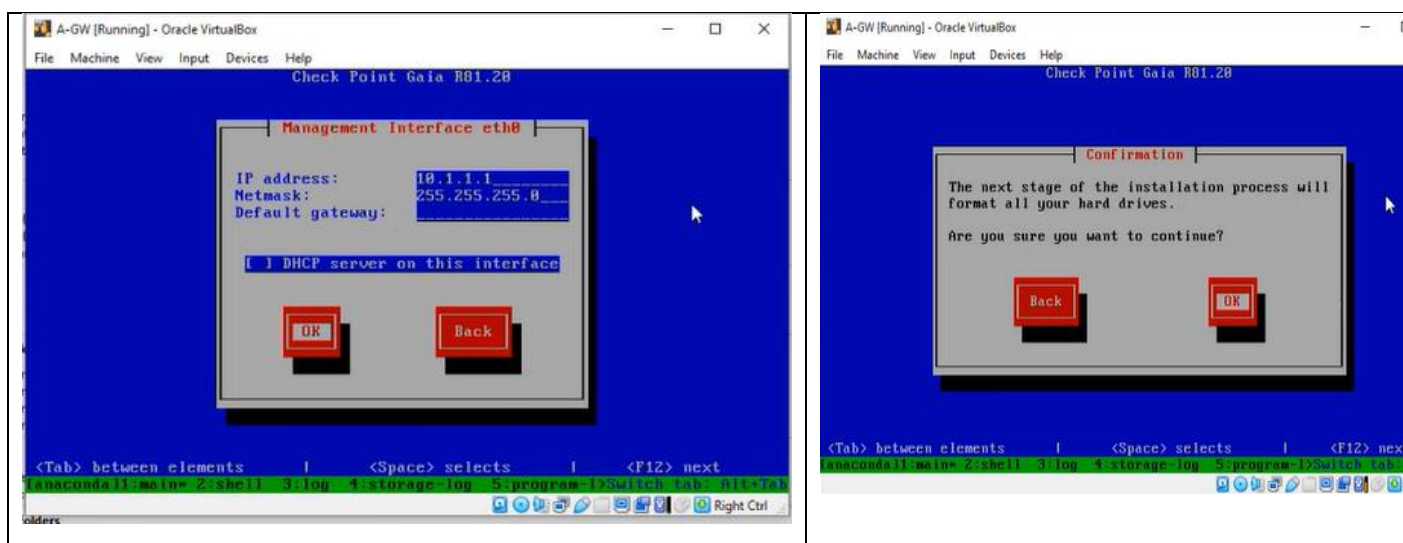
9. Select eth0 interface and configure the A-GW



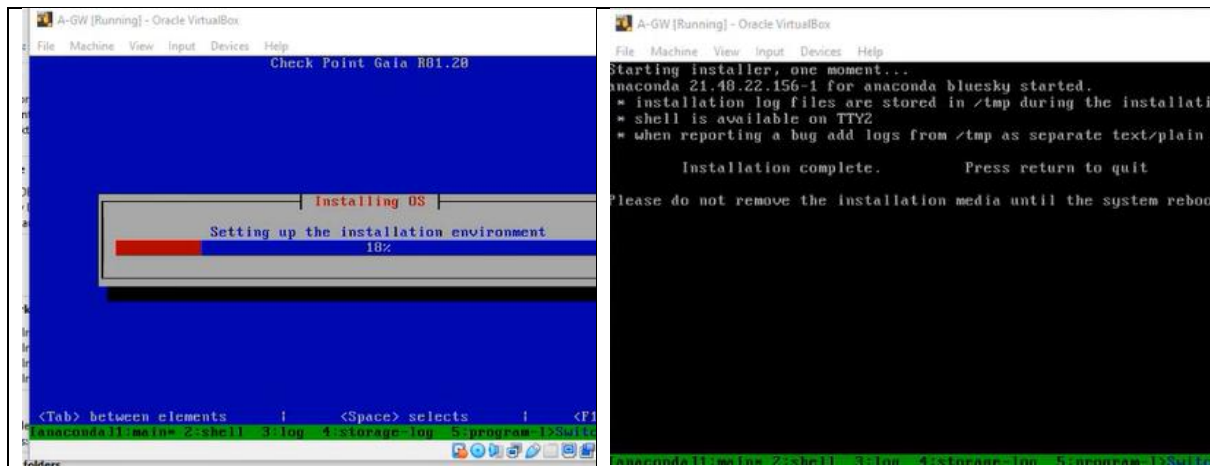
10. Enter the system configuration for A-GW.

IP address	10.1.1.1
Netmask	255.255.255.0
Default Gateway	
DHCP server on this interface	Disabled (Default)

11. Select **OK** and press **Enter** to continue.



You will see the following screen.



This is the end of the A-GW installation.

Checkpoint Appliances Installation Guide

ACCA7032 Enterprise Network Security

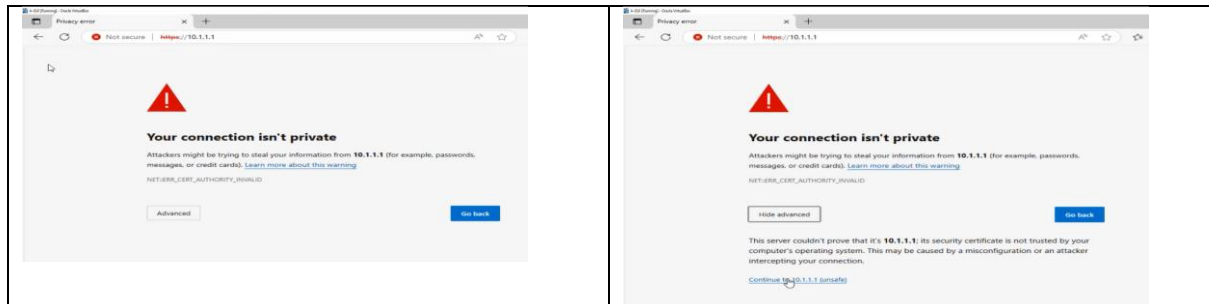
Chapter 3.1 Running the First Time Wizard on the Security Gateway

Access the Web UI and finish the First Time Wizard on the A-GW machine.

3.1.1 Go to A-GUI, open a web browser.

3.1.2 Use the following URL to access the A-GW through web portal from A-GUI <http://10.1.1.1>

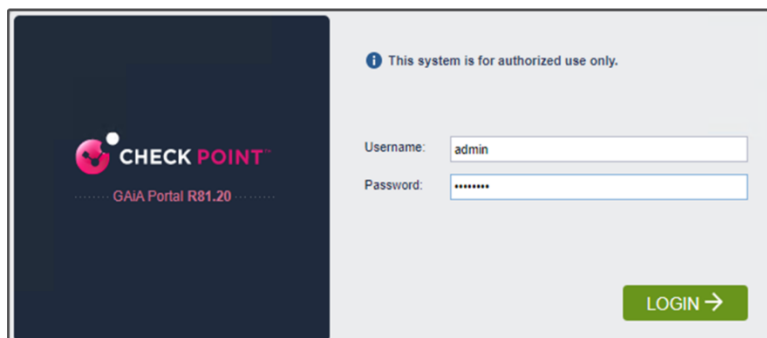
3.1.3 You might see a warning message as shown below, select Advanced and continue



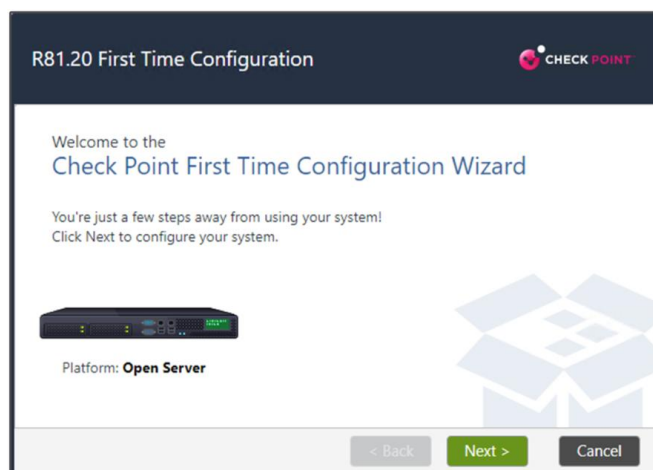
3.1.4 Use the admin login that you have created during the A-SMS installation to log in to the A-GW using Gaia portal from Web GUI.

Username: admin

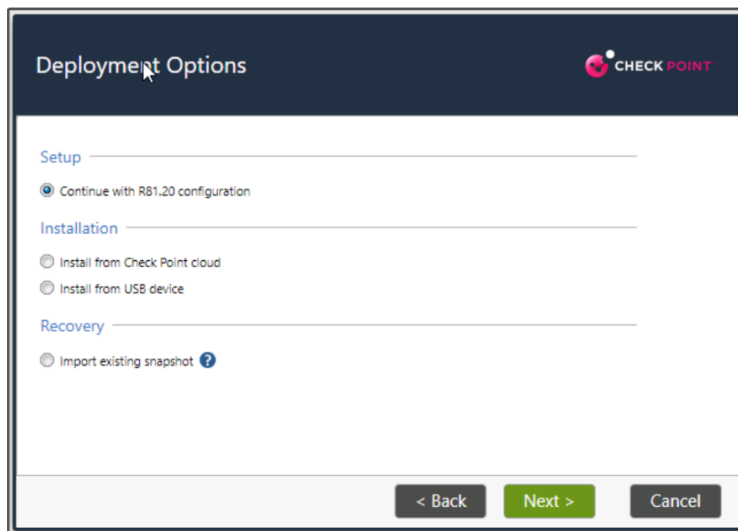
Password: Chkp!234



You will see the following welcome screen from the First Time Wizard to configure A-GW

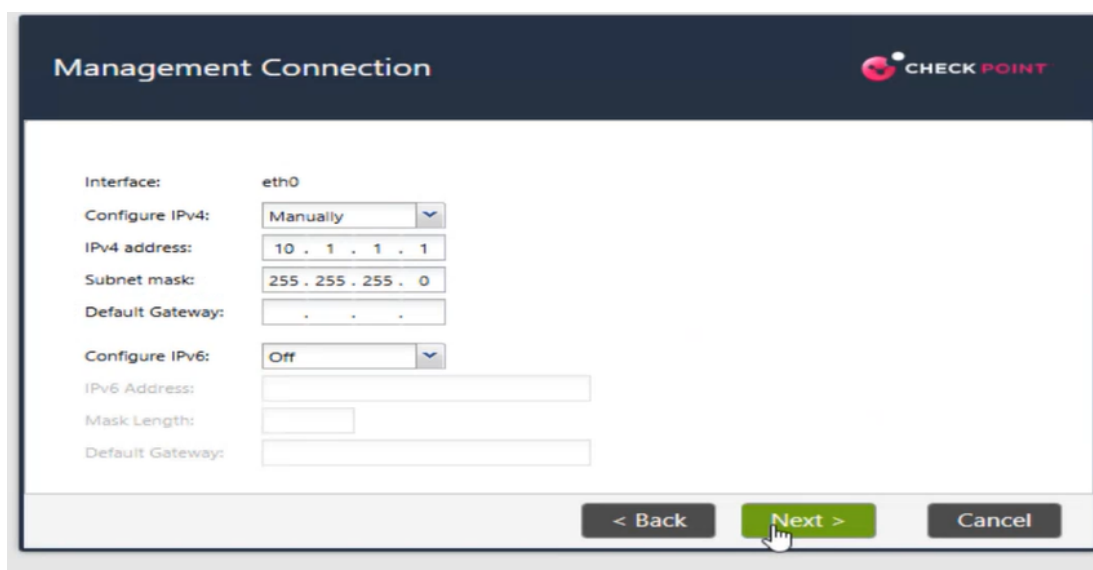


3.1.5 Select **Continue with R81.20 configuration** and click **Next** to continue



The screenshot shows the 'Deployment Options' window with the Check Point logo in the top right. The window is divided into three sections: 'Setup', 'Installation', and 'Recovery'. In the 'Setup' section, the option 'Continue with R81.20 configuration' is selected with a radio button. The 'Installation' section has two options: 'Install from Check Point cloud' and 'Install from USB device', both unselected. The 'Recovery' section has one option: 'Import existing snapshot' with a question mark icon, also unselected. At the bottom, there are three buttons: '< Back' (disabled), 'Next >' (active/highlighted in green), and 'Cancel' (disabled).

3.1.6 Check the settings on the Management Connection page is correct and click on Next to continue.



The screenshot shows the 'Management Connection' window with the Check Point logo in the top right. The window contains configuration fields for network settings. Under 'Interface', 'eth0' is selected. Under 'Configure IPv4', 'Manually' is selected in a dropdown. The IPv4 address is '10 . 1 . 1 . 1', the subnet mask is '255 . 255 . 255 . 0', and the default gateway is ' . . .'. Under 'Configure IPv6', 'Off' is selected in a dropdown. The IPv6 address, mask length, and default gateway fields are empty. At the bottom, there are three buttons: '< Back' (disabled), 'Next >' (active/highlighted in green with a mouse cursor pointing to it), and 'Cancel' (disabled).

Leave the settings as it is from the following screen.

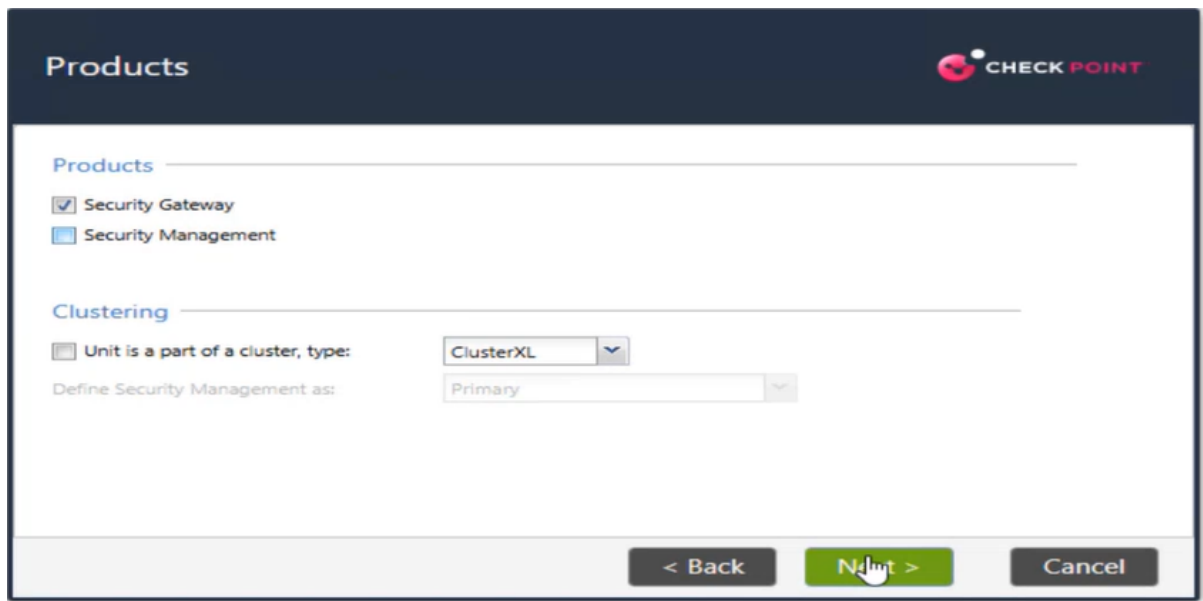
3.1.7 Configure the A-GW using the **Device Information** and select **Next** to continue

Hostname : A-GW Domain Name : swansea.acca Primary DNS Server : 192.168.1.1 Secondary DNS : 8.8.8.8 Teritary DNS Server : 4.2.2.2	
--	--

3.1.8 Select use **Network Time Protocol** on the **Date and Time Settings** page. Configure the NTP servers with **time.google.com**. Also choose London,Europe(GMT) for the Time Zone. Select **Next** to continue.

Primary NTP Server : time1.google.com Secondary NTP Server : time2.google.com	
---	--

3.1.9 Make sure **Security Management** option is disabled from the Products page and ensure **Security Gateway** is enabled. Verify the **Define Security Management** is set to Primary. Select **Next** to continue

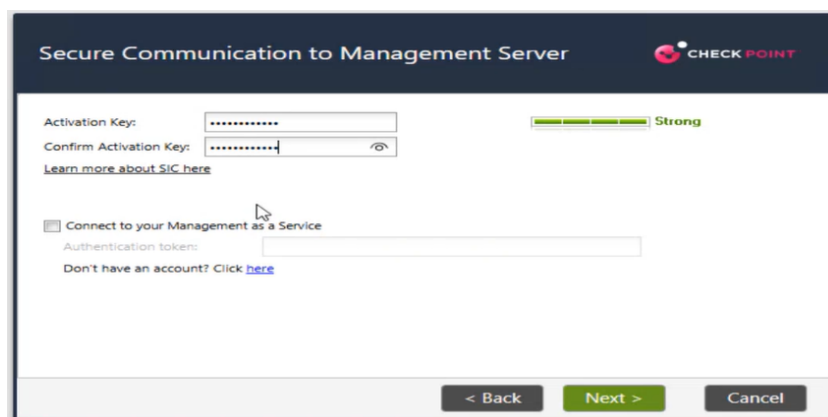


3.1.10 Verify **No** is selected on the **Dynamically Assigned IP** and press **Next** to continue

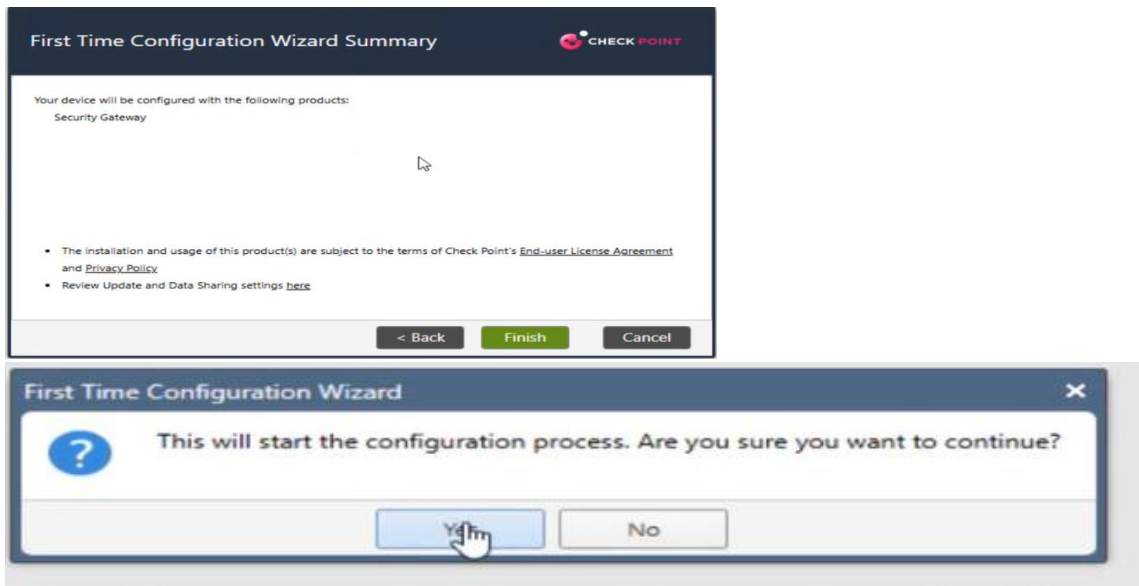


3.1.11 On the Secure Communication to Management Server page, enter the Activation key. This key is used to establish the Secure Internal Communication (SIC). For this activity, **Chkp!234** has been used for the activation key.

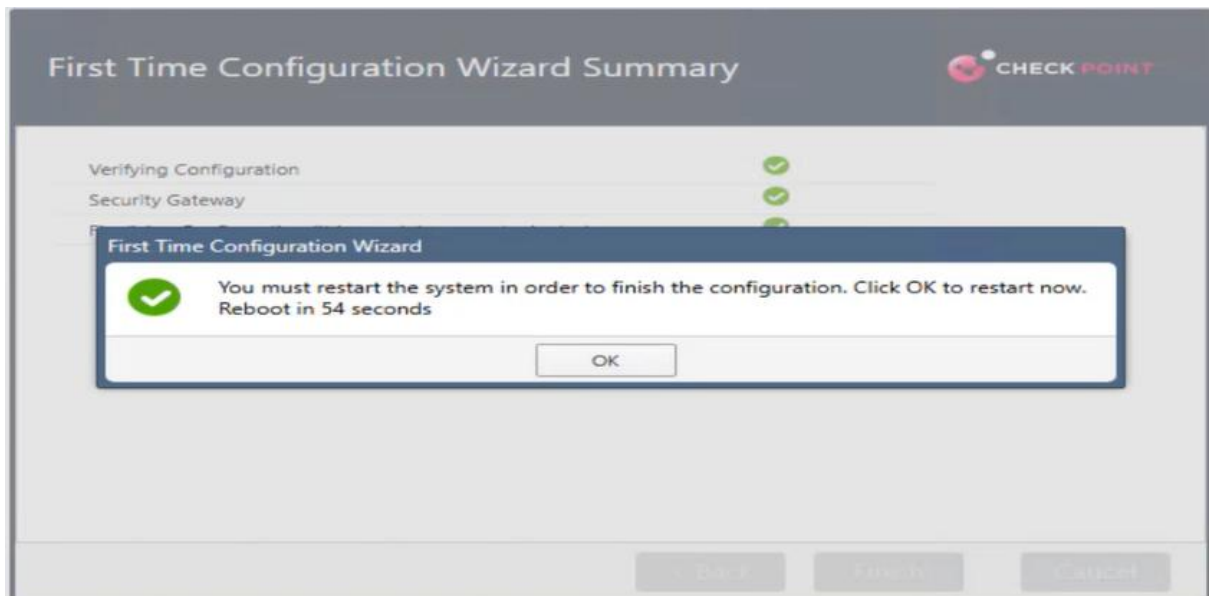
Activation Key : Chkp!234



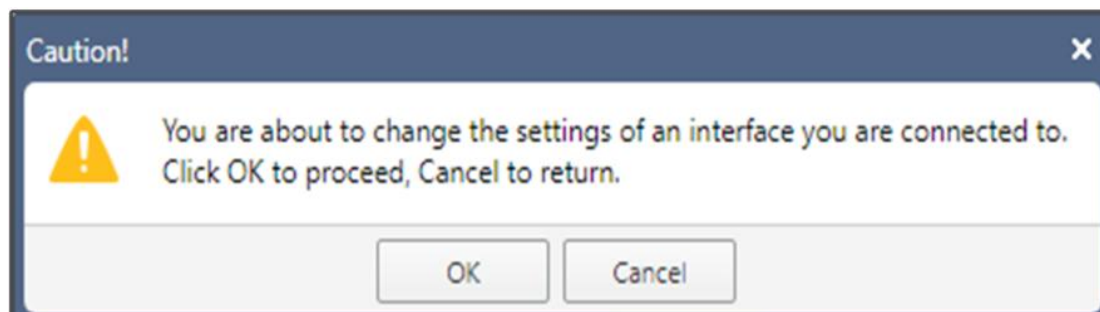
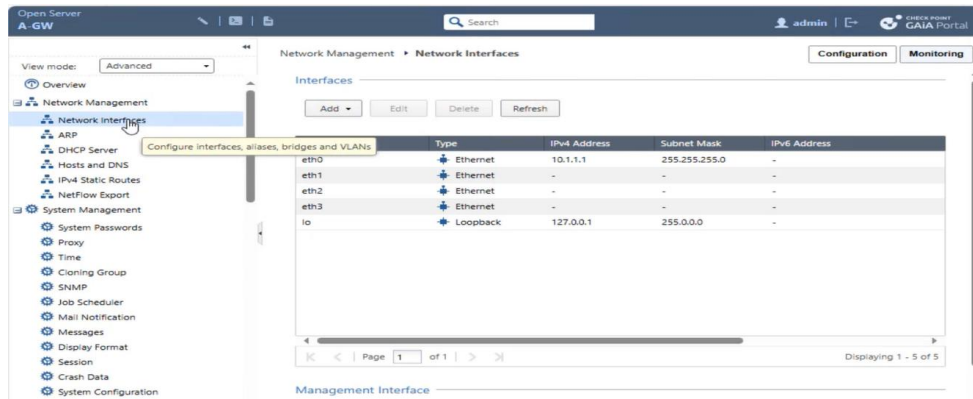
3.1.12 Verify only **Security Gateway** is listed on the **First Time Configuration Wizard Summary** page and press **Finish** to start the configuration process. Press **Yes** to the following process to continue.



3.1.13 You will be seeing the following screen. Once done, press **Ok** to restart the A-GW.



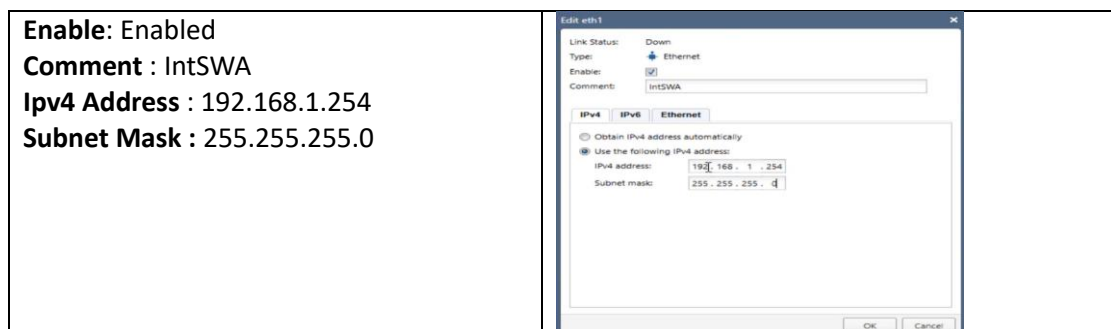
3.1.14 After A-GW finishes its reboot, log in to the Gaia Portal again. Navigate to **Network Interfaces**. Select the **eth0** and choose **Edit**. You will see a **Caution!** message indicating that you are trying to edit the interface you are connected to. Select **Ok** button to continue



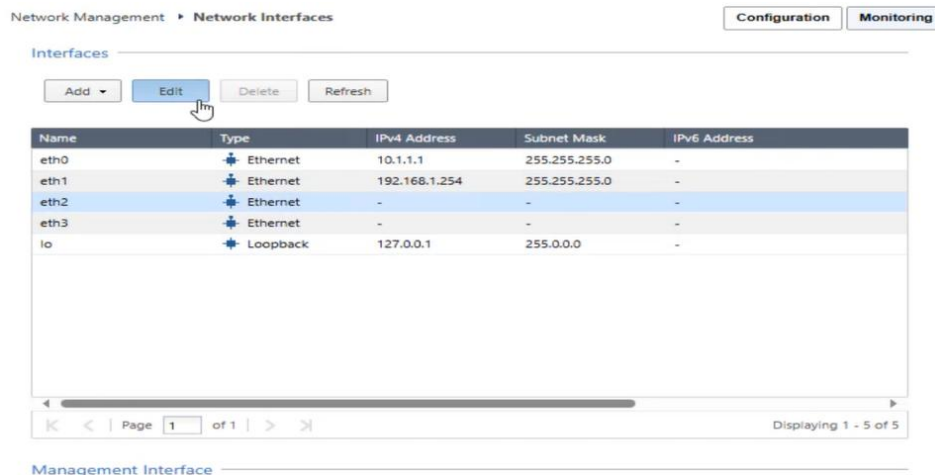
3.1.15 Check the configuration of **eth0** and verify the following settings and press **OK** to close the configuration window for **eth0**

Enable: Enabled
Comment : Swansea.acca
Ipv4 Address : 10.1.1.1
Subnet Mask : 255.255.255.0

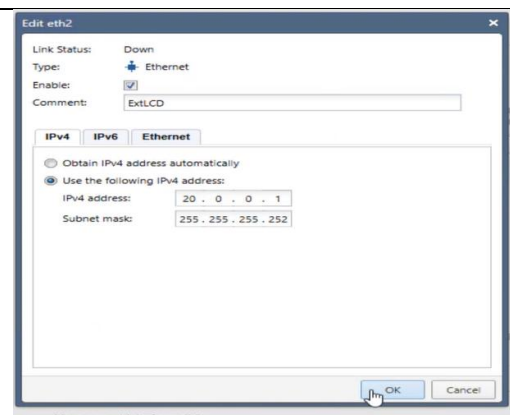
3.1.16 Select **eth1** , click on **Edit** and configure the **eth1** interface with the following details



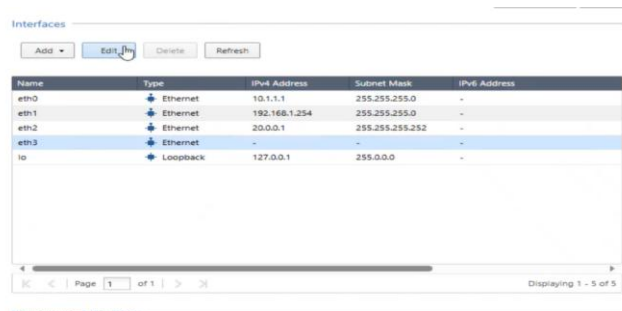
3.1.17 Select **eth2** , click on **Edit** and configure the **eth2** interface with the following details



Enable: Enabled
Comment : ExtLCD
Ipv4 Address : 20.0.0.1
Subnet Mask : 255.255.255.252



3.1.18 Select **eth3** , click on **Edit** and configure the **eth3** interface with the following details



Enable: Enabled
Comment : ExtInt
 Choose **Obtain IPv4 address automatically.**

Edit eth3

✕

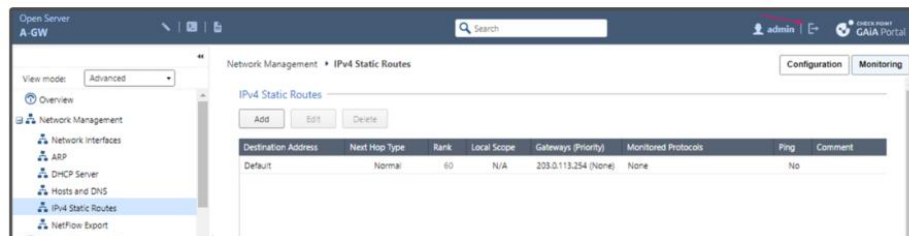
Link Status: Down
 Type: Ethernet
 Enable: ☒
 Comment: ExtInt

IPv4
IPv6
Ethernet

☒ Obtain IPv4 address automatically
☐ Use the following IPv4 address:
 IPv4 address:
 Subnet mask:

OK Cancel

3.1.19 Click **Sign Out** to log out of the **A-GW** Gaia Portal. Close the browser.

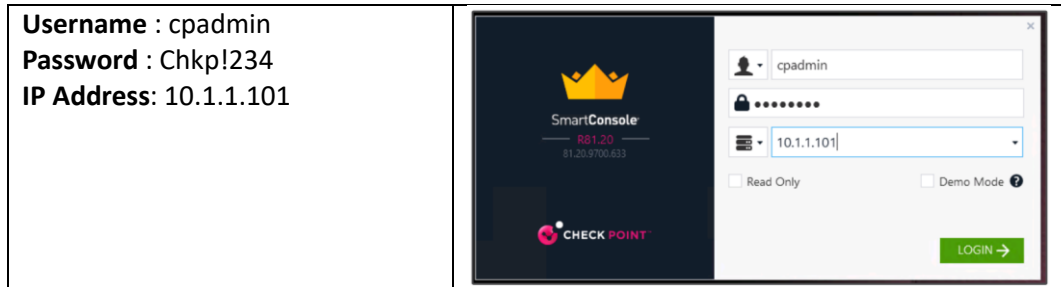


This is the end of the Lab.

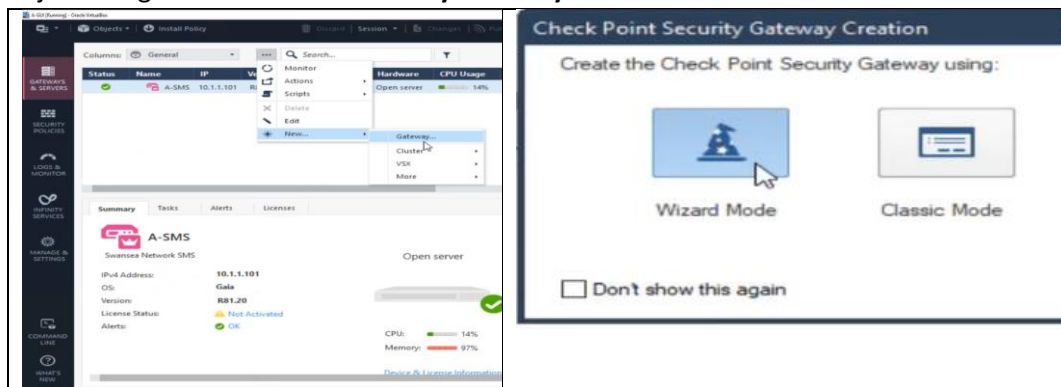
Chapter 4 Establishing Secure Internal Communication

To create a Security Gateway object in SmartConsole, complete the following steps.

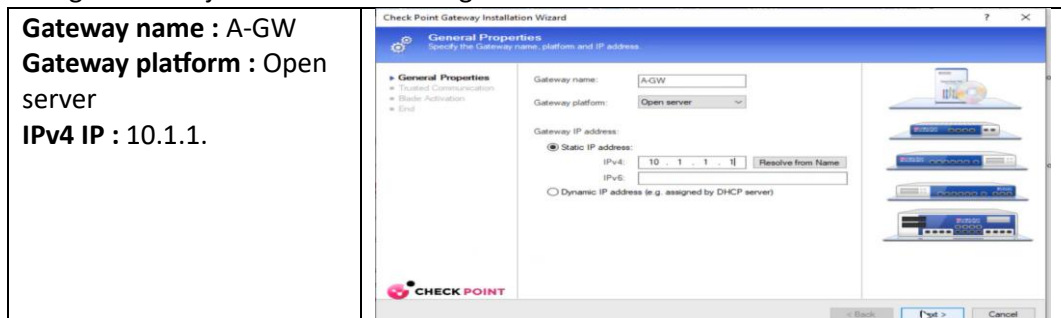
1. On A-GUI, log into A-SMS using SmartConsole.



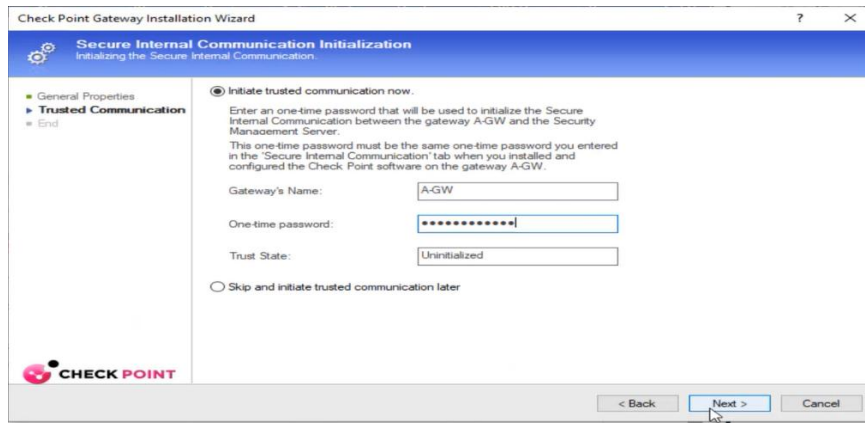
2. Select **Gateway** from the **New** menu, select **Wizard Mode** to create the new Gateway object using the **Check Point Security Gateway Creation Wizard**.



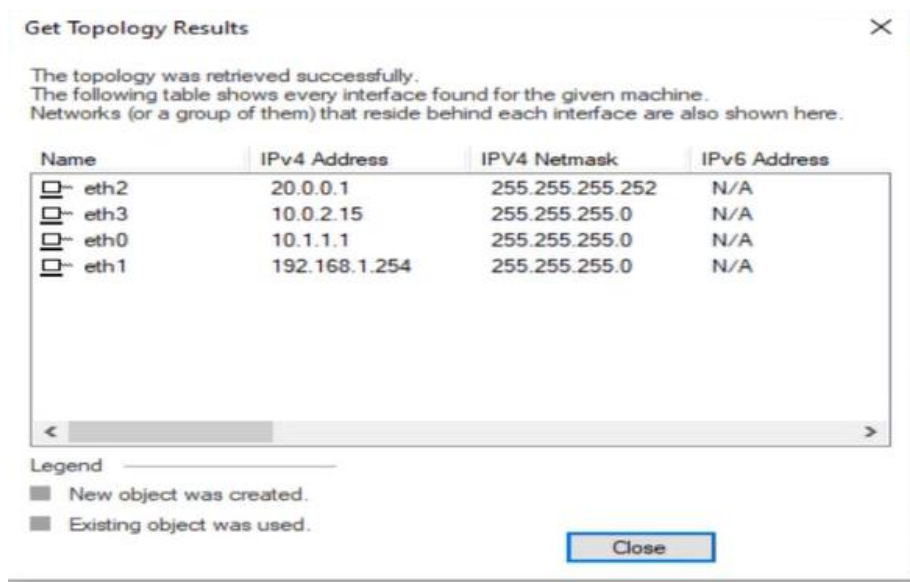
3. Configure the object with the following details and select **Next**



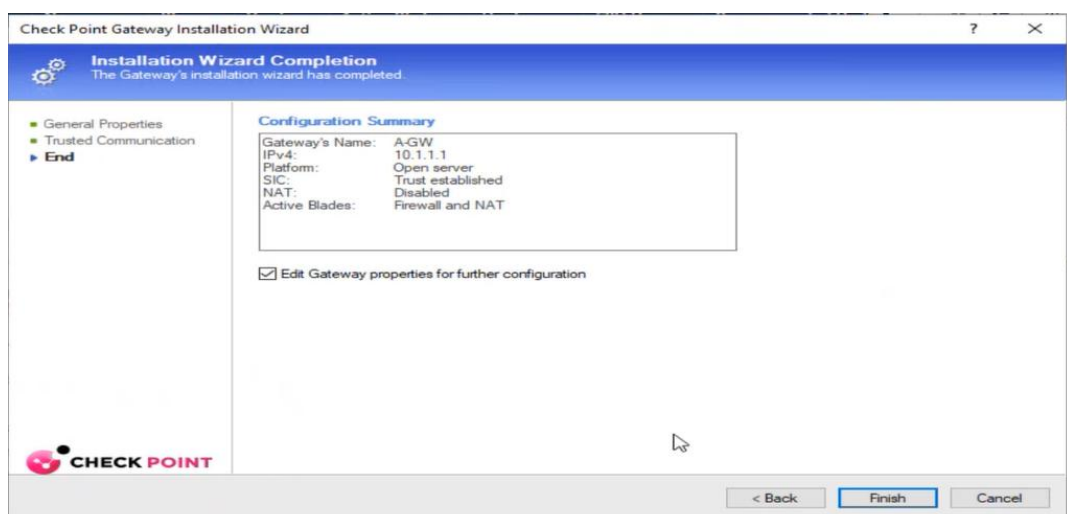
4. Enter the one-time password, **Chkp!234** and select **Next**



5. You should be able to see the configuration information from the **Get Topology Results**, once verified select **Close**.



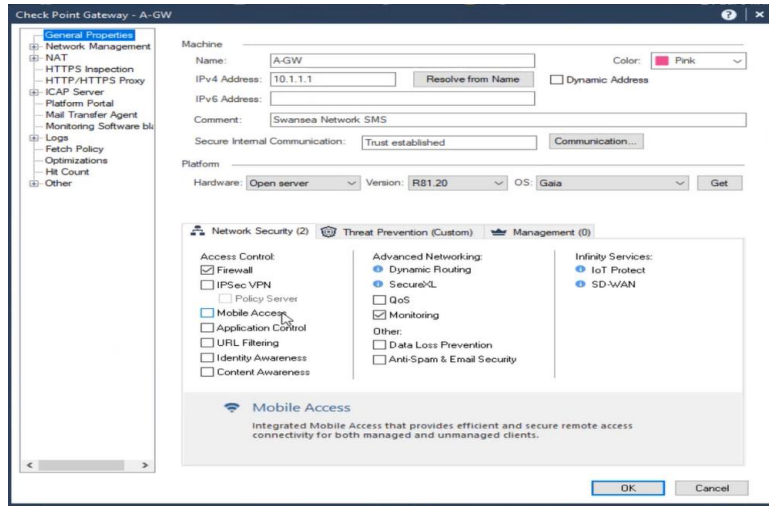
6. Select **Finish** to complete the **Check Point Gateway Installation Wizard**.



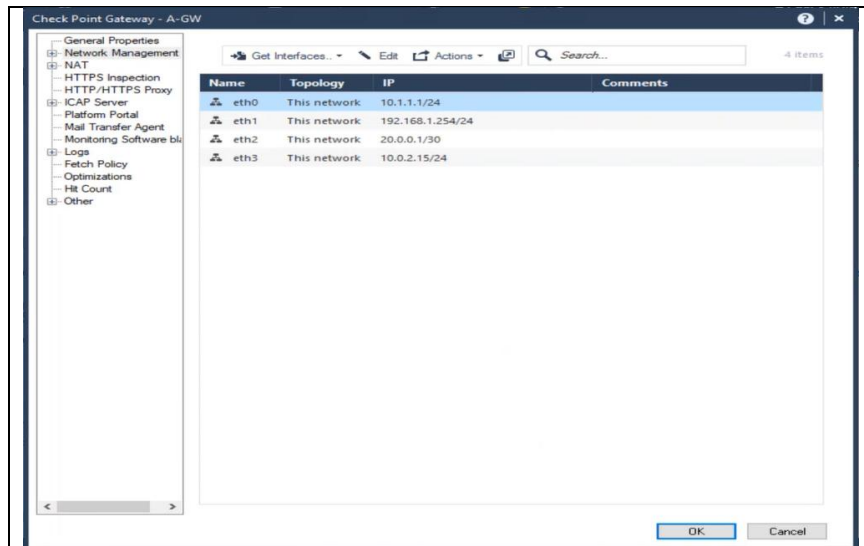
7. Go to the General Properties for A-GW, enable the **Firewall and Monitoring**.

Checkpoint Appliances Installation Guide

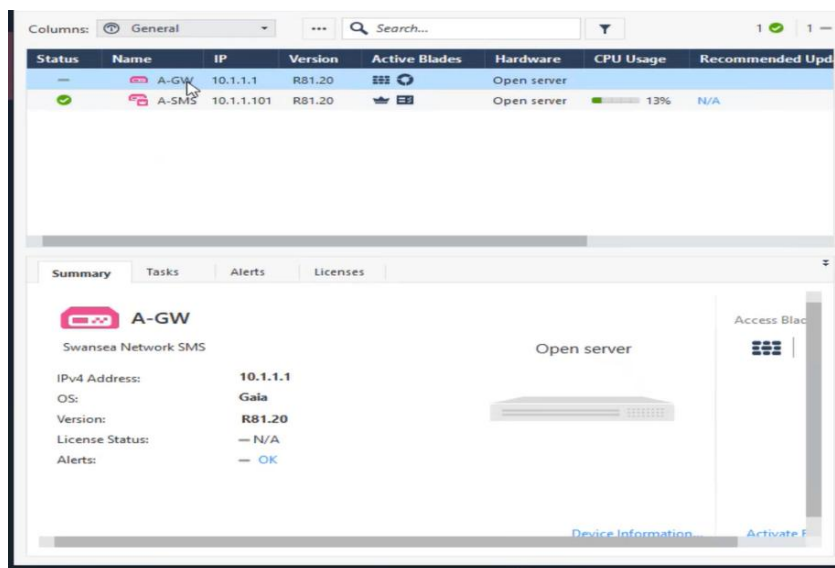
ACCA7032 Enterprise Network Security



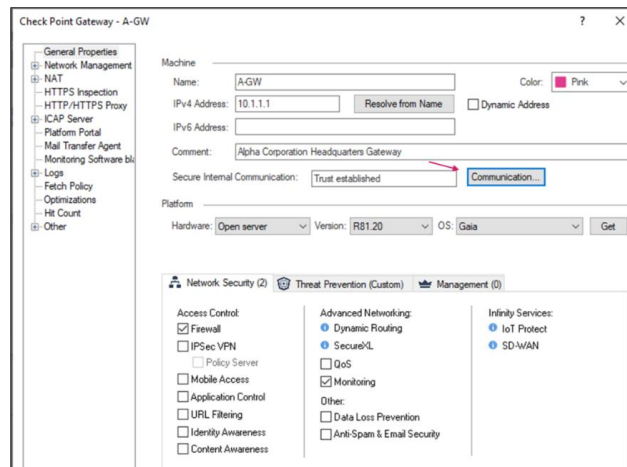
8. Verify the IP addresses and topologies match this image.



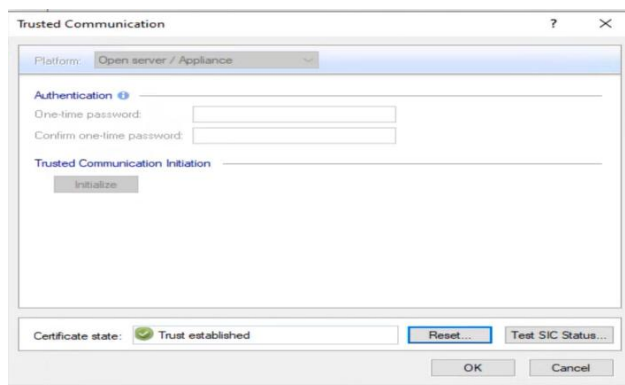
9. Select the **Gateway & Servers** view. Double click the **A-GW** object



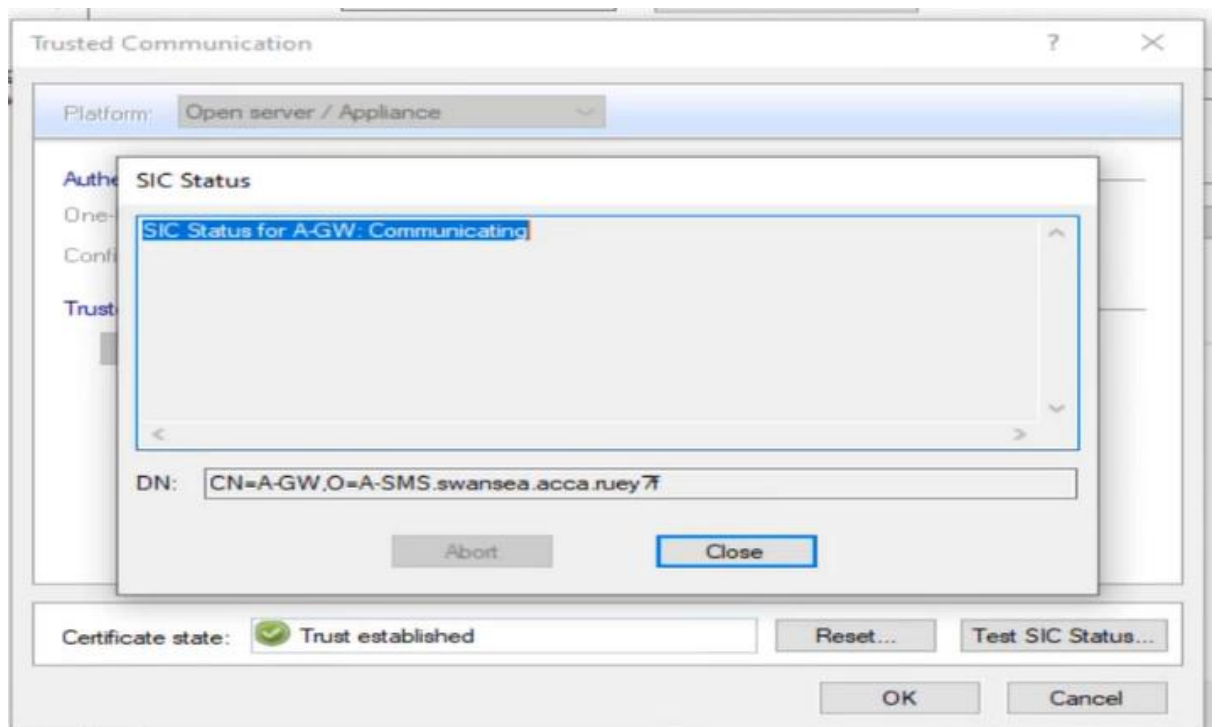
10. Select **Communication**



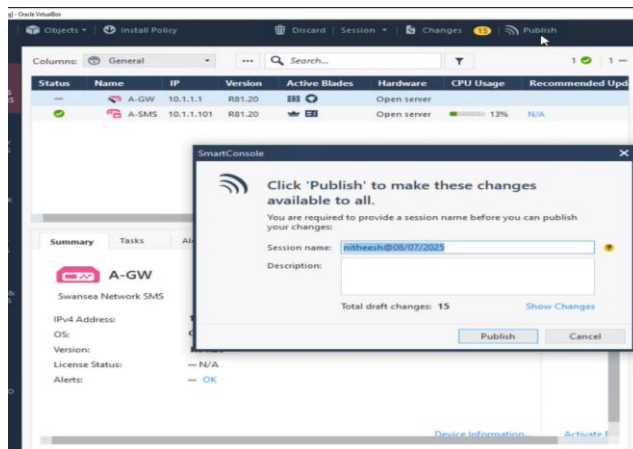
11. Select the **Test SIC Status** communication



12. If SIC has been established properly, you will see a status of **Communicating**.



13. Select the **Close** button to close the **SIC Status** window and select **OK** to close the **Trusted Communication** window. Select **OK** to close the **A-GW** object.
14. Select **Publish** button on the global toolbar to save the changes to the database.



Chapter 5: Managing Licence

To Analyse the Current Licence Status

1. Login to the SmartConsole from A-GUI machine using the credentials below.

Username : cpadmin Password : Chkp!234 IP Address : 10.1.1.101	Select the Gateways & Servers
--	---

2. Select **A-GW** object and check the licence status from the summary tab below. You should see **Not Activated**

The screenshot displays the Checkpoint Management Center (MCP) interface. At the top, there is a search bar and a filter icon. Below this is a table listing the appliances in the system.

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Upd
✓	A-GW	10.1.1.1	R81.20	...	Open server	17%	N/A
✓	A-SMS	10.1.1.101	R81.20	...	Open server	12%	N/A

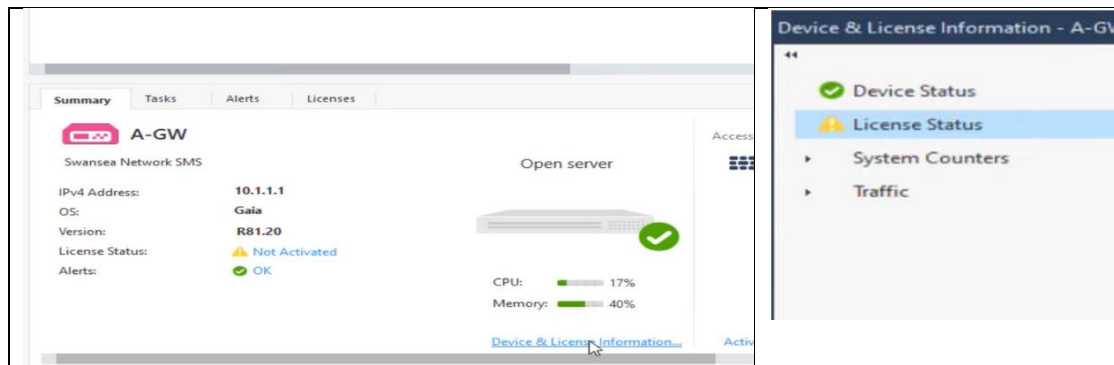
Below the table, there is a detailed view of the selected appliance, A-GW. The view includes a summary of the appliance's configuration and status.

A-GW Summary:

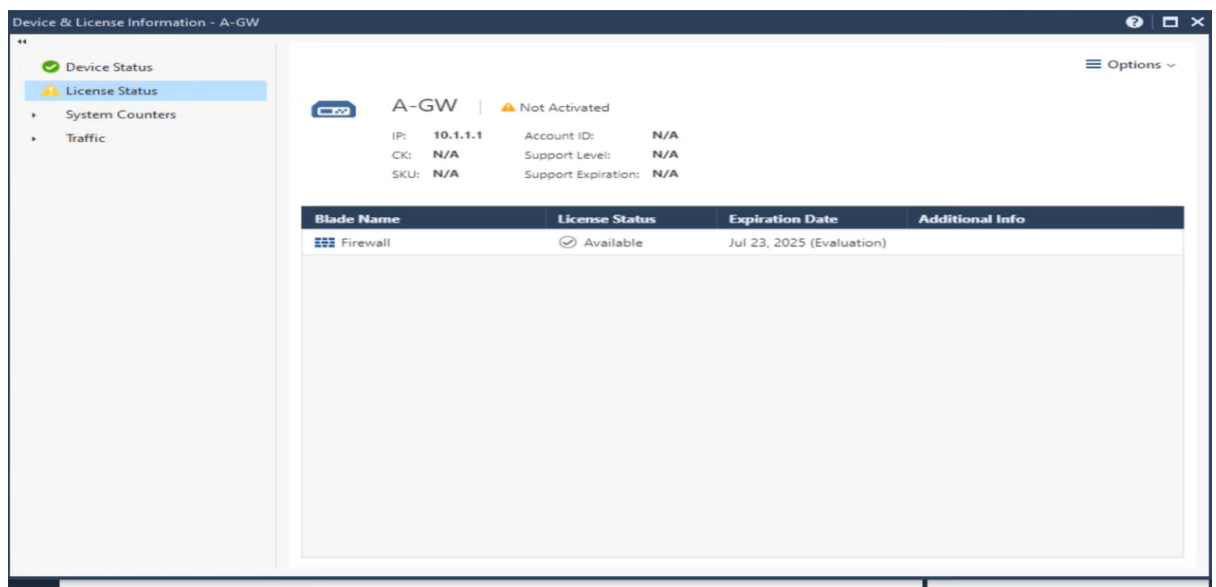
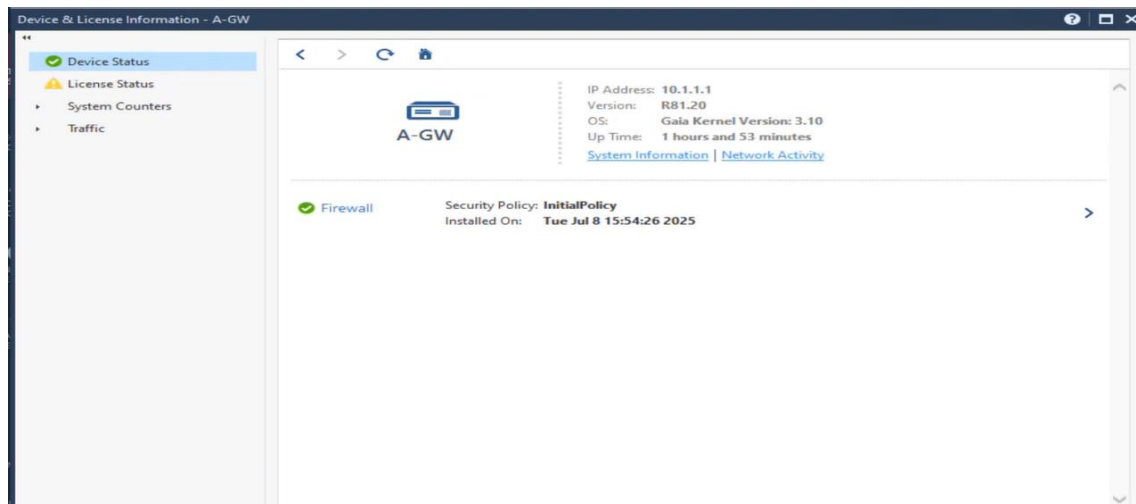
- Name:** A-GW
- Swansea Network SMS**
- IPv4 Address:** 10.1.1.1
- OS:** Gaia
- Version:** R81.20
- License Status:** ⚠ Not Activated
- Alerts:** ✓ OK
- Hardware:** Open server
- CPU Usage:** 17%
- Memory Usage:** 40%

On the right side of the detailed view, there is a section for "Access Blades" and a "Device & License Information" link.

3. Select the **Device & Licence Information** and select **License status** from the left object pane and verify the Expiration date and **close/exit** the **Device & Information** window.



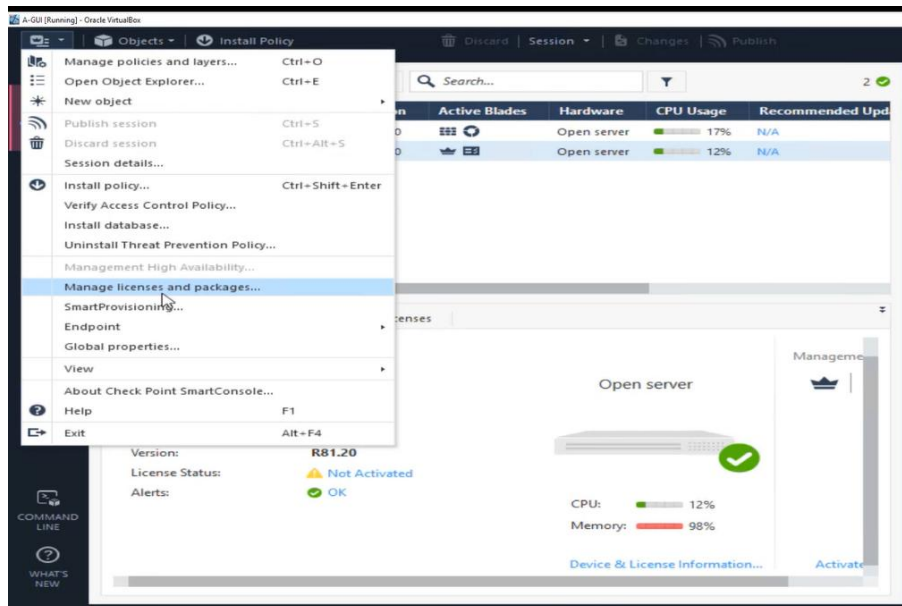
4. Examine the licence for A-SMS and **Exit** the window.



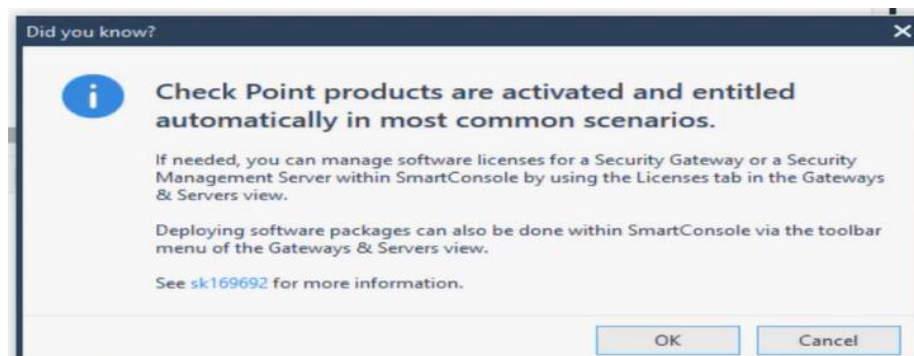
Chapter 4A :Attaching a Licence Using SmartUpdate

SmartUpdate is an utility to manage and maintain licence. In this chapter, we will go through how to attach licences using SmartUpdate.

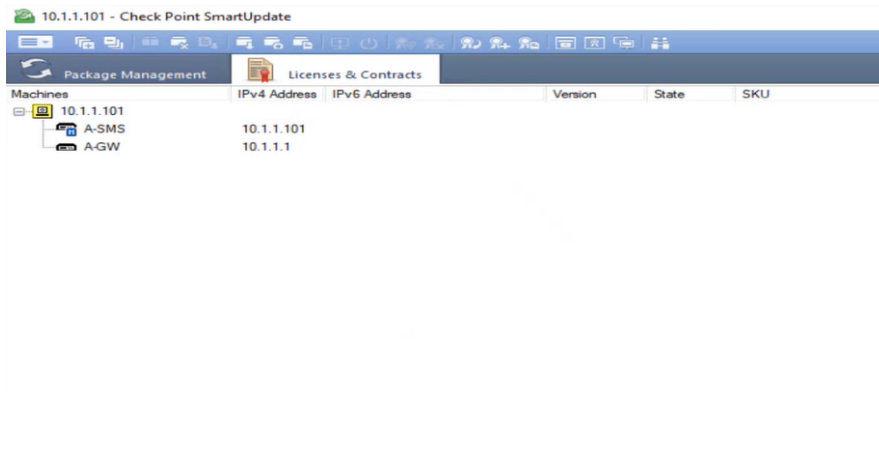
1. Choose **Manage licence and packages** from the SmartConsole application menu.



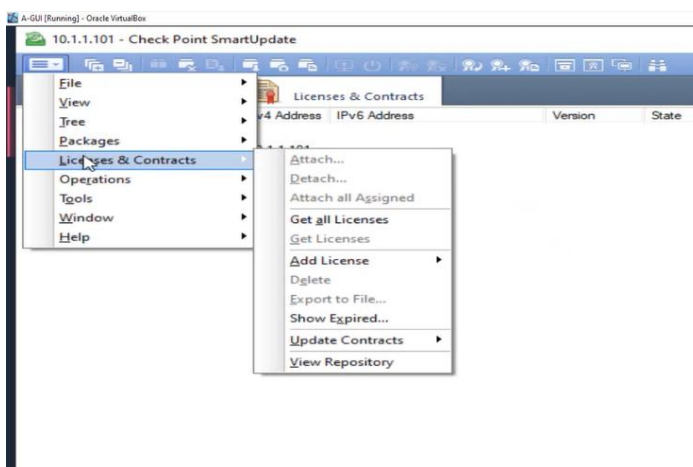
2. Select **OK** to proceed further.



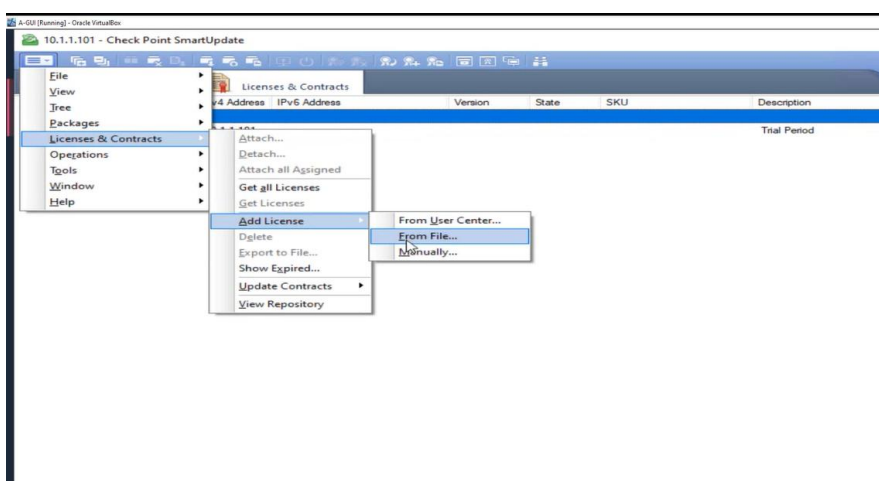
3. Select the **Licence and Contracts** tab at the top of the window.



4. From the SmartConsole menu, choose, **Licence & Contracts** and select **View Repository**



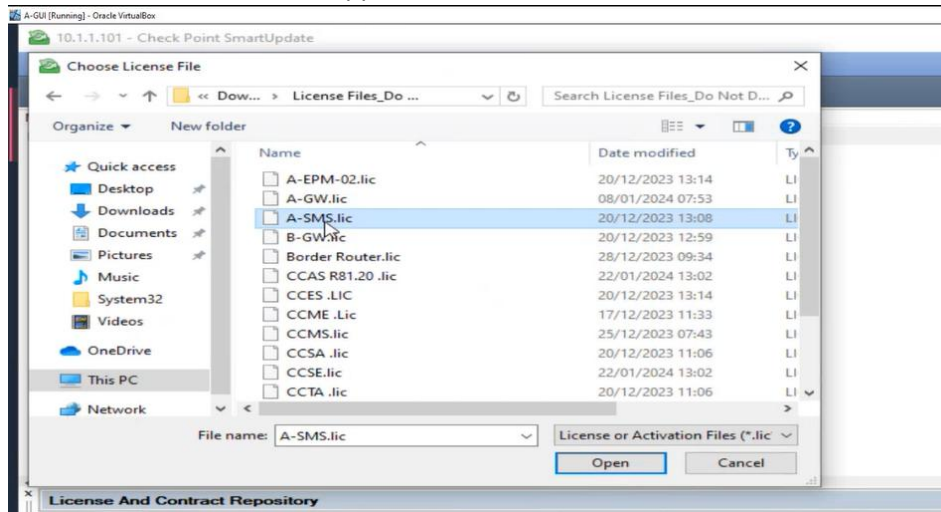
5. Right click in the Licence and Contracts Repository pane, choose **Add Licence** and select **From File** option.



Checkpoint Appliances Installation Guide

ACCA7032 Enterprise Network Security

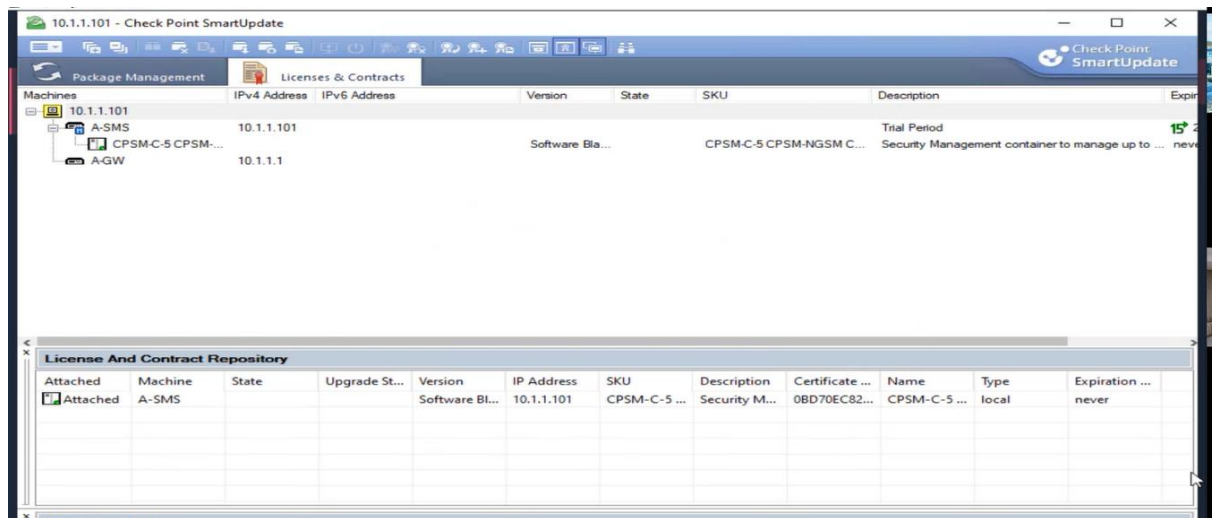
- Go to the licence directory that you have downloaded from Moodle. You could see all the licence for the Check Point appliances. Select A-SMS.lic



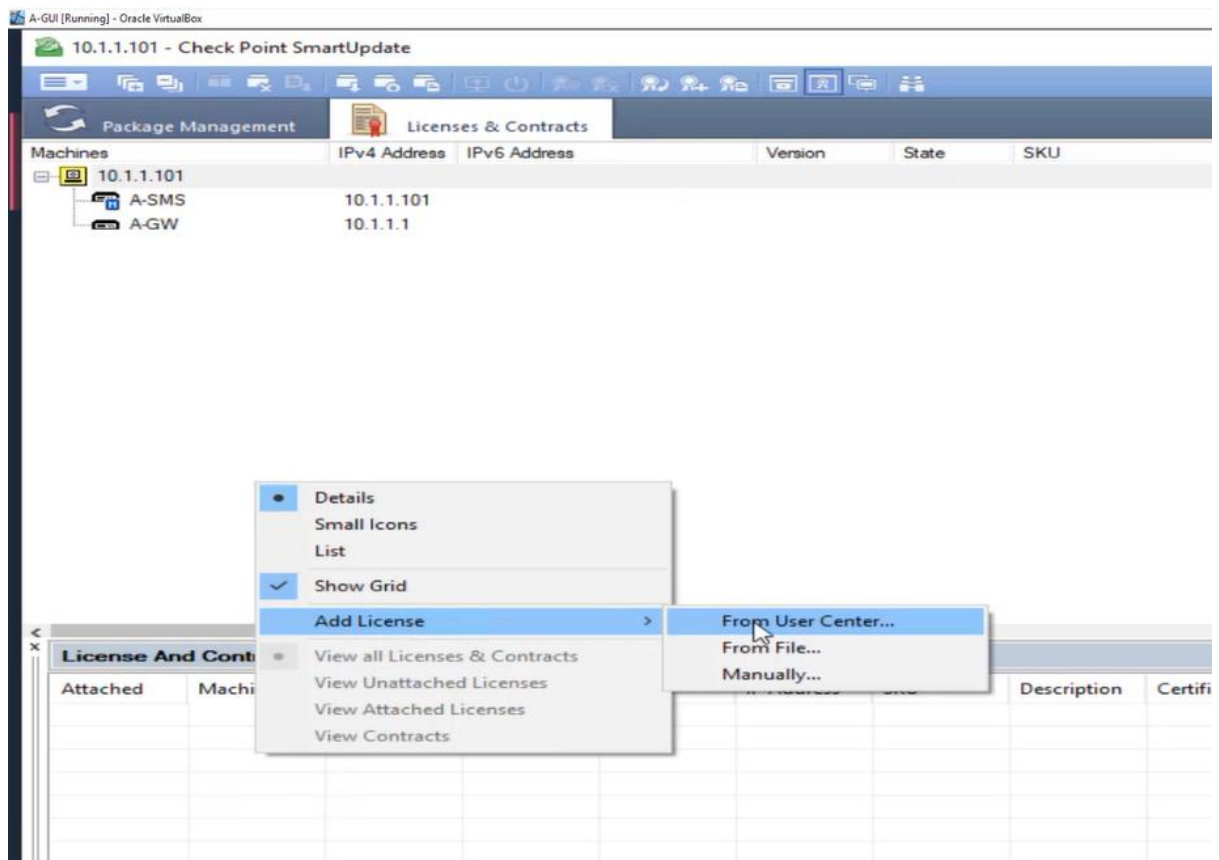
- Select **OK** to acknowledge to the message.



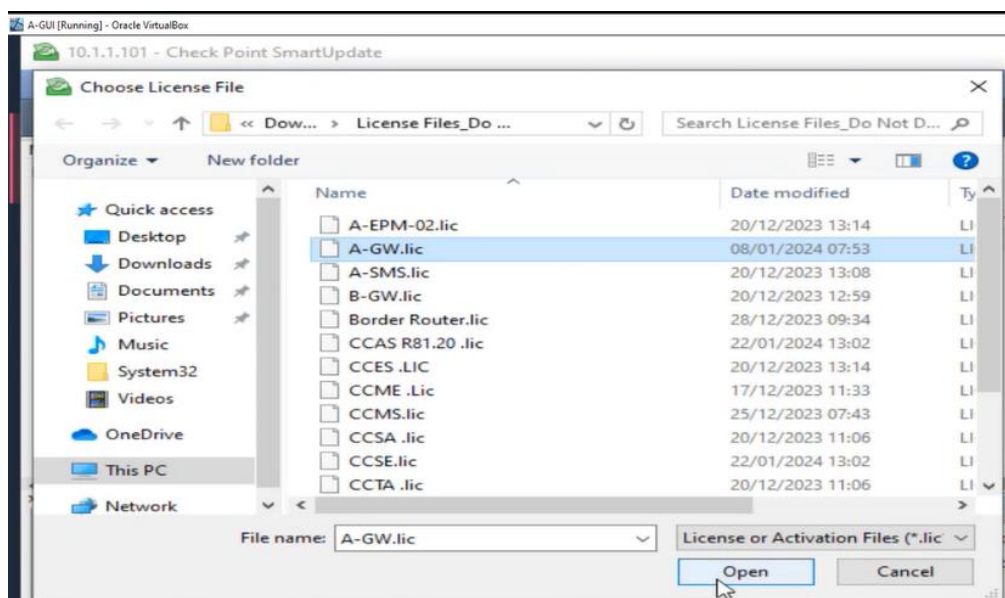
- You could see the local licence was attached to the SMS server.



1. Right click in the **Licence & Contracts** repository pane. Select **Add licence** and choose **From File**.



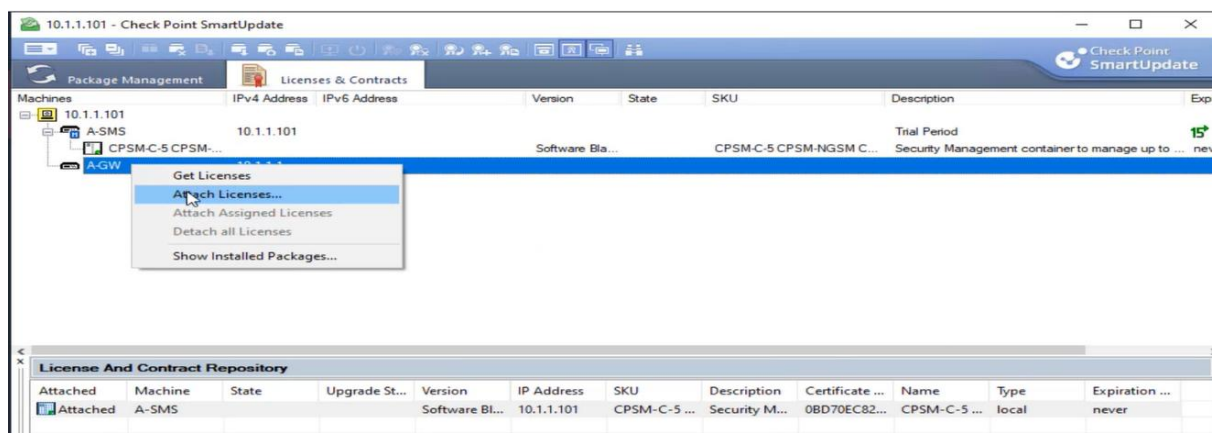
2. Go to the licence directory that you have downloaded from Moodle. You could see all the licence for the Check Point appliances. Select A-GW.lic



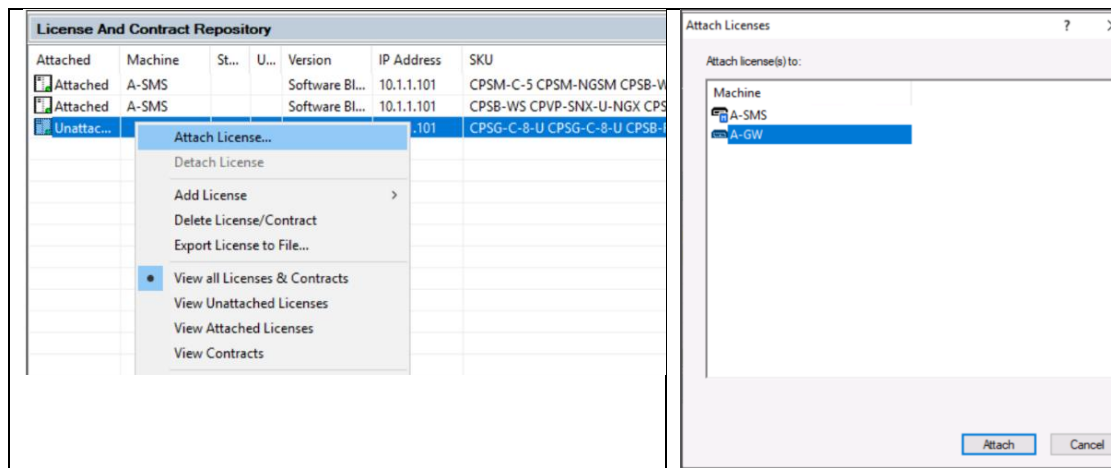
3. Select **Ok** to acknowledge the licence was added to the repository.



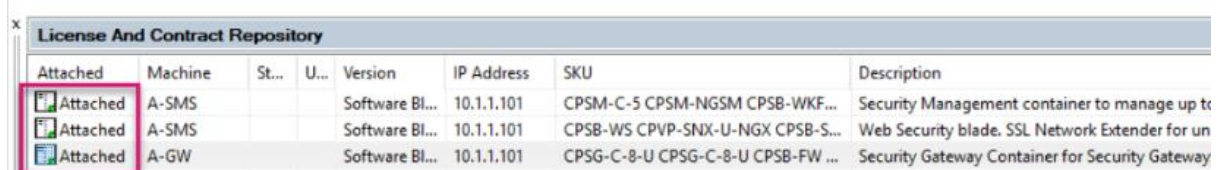
4. The licence is added to the repository but it is not attached to the Security Gateway.



5. Right click on the Unattached licence and select Attach Licence. Choose A-GW from the option given below

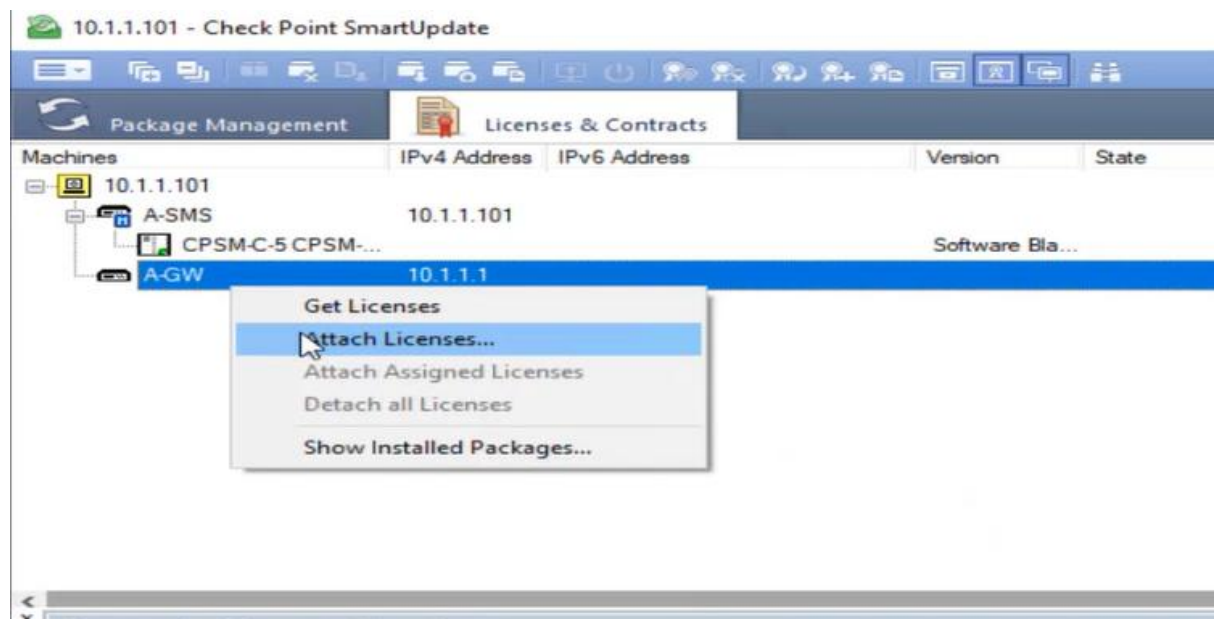


6. Make sure now, Smart Update shows all the licence were installed on both machines.

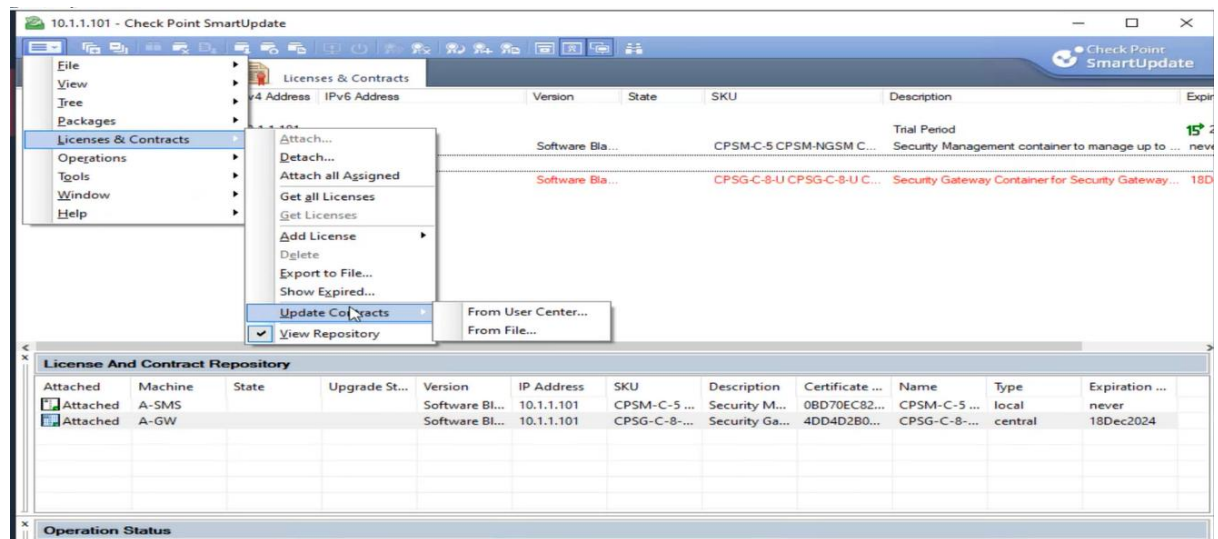


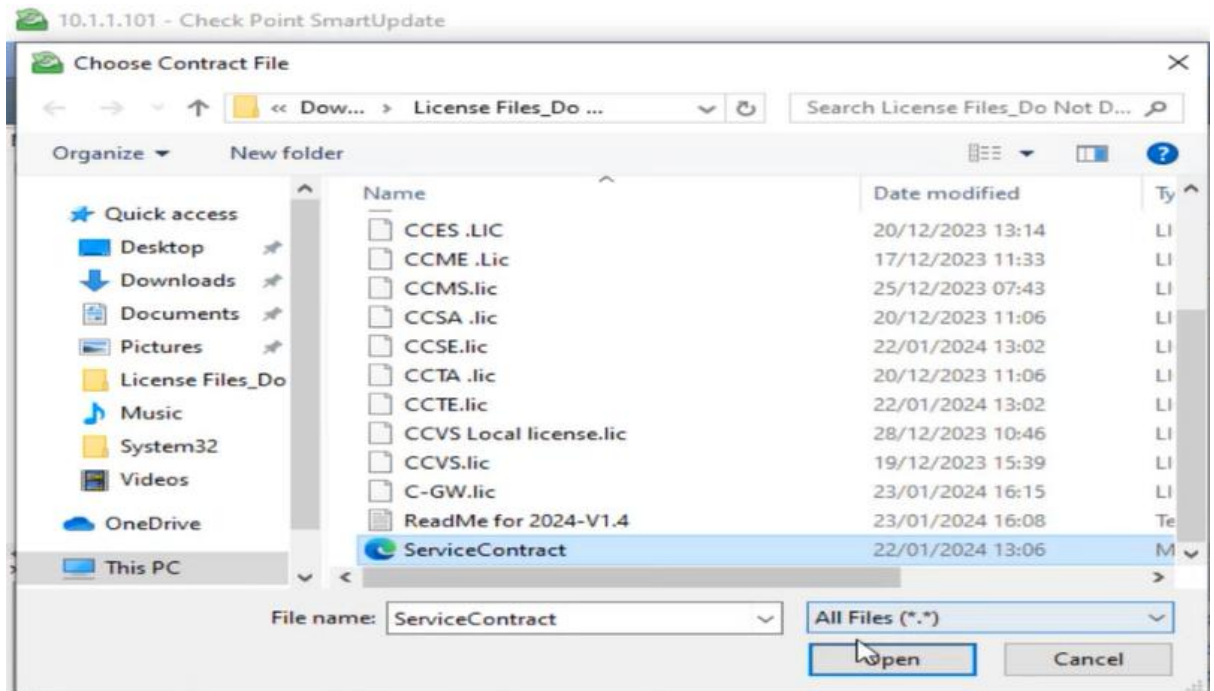
Update the Service Contracts.

1. Explore the Licence & Contracts view, you will see on the right, **Has Contracts** column



2. Select SmartConsole menu and choose **Licence & Contracts** and select **Update** Contracts and choose **From File**. Navigate to **ServiceContract.xml**. Select and open it.





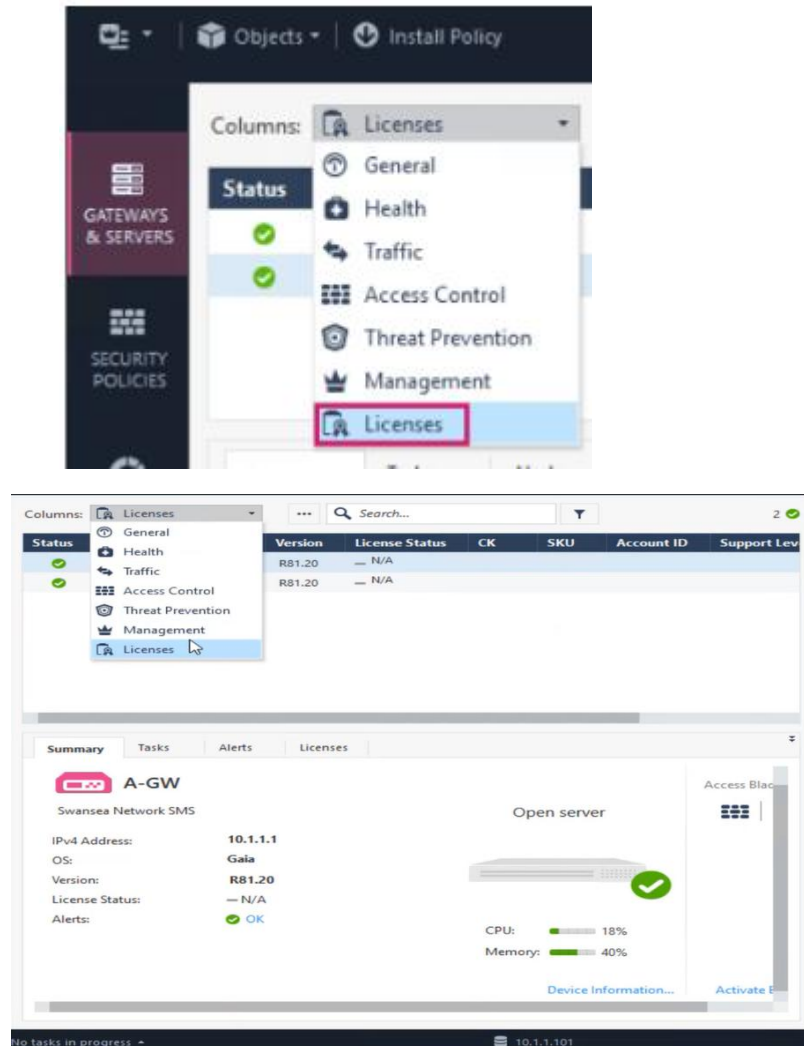
3. Verify both A-GW and A-SMS has contracts. Close the SmartUpdate.

Package Management		Licenses & Contracts											
Machines	IPv4 Address	IPv6 Address	Version	State	SKU	Description	Expiration D...	Has Contracts					
10.1.1.101	10.1.1.101												
A-SMS													
CPSM-C-5 CPSM...			Software Bla...		CPSM-C-5 CPSM-NGSM C...	Security Management container to manage up to ...	never	Yes					
CPSB-WS CPVP...			Software Bla...		CPSB-WS CPVP-SINX-U-N...	Web Security blade. SSL Network Extender for u...	23Apr2024	Yes					
A-GW	10.1.1.1												
CPSG-C-8-U CPS...			Software Bla...		CPSG-C-8-U CPSG-C-8-U C...	Security Gateway Container for Security Gateway...	23Apr2024	Yes					

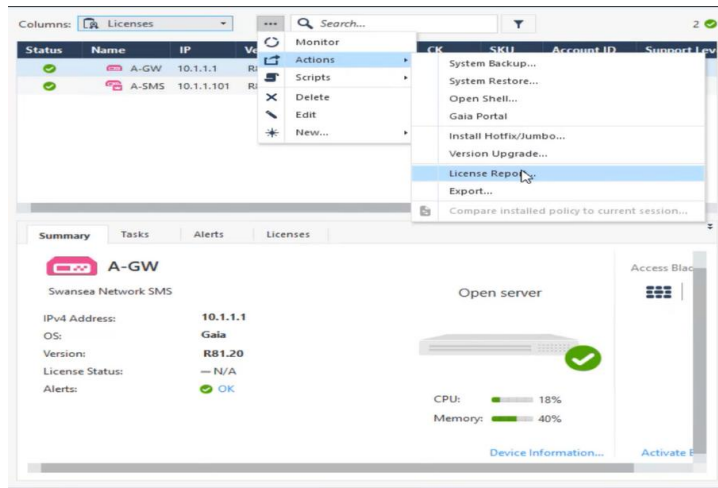
4. Now the contracts have been attached to A-GW is complete.
5. Press X to close the SmartUpdate window.

Generating a Licence Report

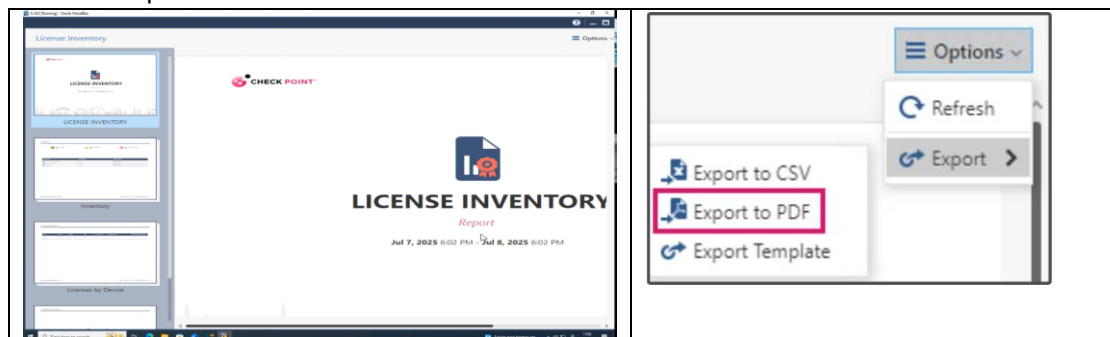
1. In SmartConsole, navigate to Gateway & Servers and choose **Licences** option



2. Select the **Action** button and choose **Licence Report**.



3. A licence report will be created.



4. Go through the inventory report and you can see the blades are available and active. Also, you can see any inactive blades detail as well.
5. Select the **options** menu and select Export to PDF. The PDF is ready, it is ready to download.

This is the end of Managing and Licence lab.

