Check Point Cloudguard Network Security Gateway on OCB Flexible Engine

Deployment and Configuration Guide v1.3

May 2021

Abstract

This Deployment and Configuration guide describe in details essential information to be known before deployment, how to configure OCB workload, deploy, integrate and configure Check Point Cloudguard Network Security Gateway. In the document, we are making sure integration was successful, addressing also licensing topic.

Audience

The information presented in this paper is aimed to guide Security Experts, Cloud Security Consultant on how to deploy and configure Check Point Cloudguard Network Security gateway on Orange Cloud for Business Flexible Engine.

William Mikanowski
Check Point Security Solutions Expert

-

TABLE OF CONTENTS

CLOUD TRANSFORMATION INTRODUCTION

Cloud transformation is all around us. For security professionals, it is a defining statement of our time, shaping the cyber security landscape. Nevertheless, cloud transformation is complex and challenging, with long-held operational models and fundamental business processes.

In the following paper, we will highlight some of the common cloud network security deployment that enterprise architecture teams are considering and how Orange and Check Point can be their cloud security trusted partner to succeed in that transformation journey.

Rebuilding your security infrastructure around a Zero Trust approach using disparate technologies might lead to complexities and inherent security gaps. To avoid that, Check Point recommends a more practical and holistic approach to implement Zero Trust, based on single consolidated cyber-security architecture.

The single consolidated security architecture enables organizations to fully implement all of the Zero Trust principles. Focused on threat prevention and centrally managed through a centralized security console, which empowers Zero Trust implementations with unparalleled security and efficiency.

This approach aligned with the Zero-Trust principle considers one the following element that is part of the cloud transformation project but definitively a first stage of protection.

Check Point Cloudguard Network Security Gateways enable micro-segmentation of the network across your entire IT infrastructure, across private/public clouds and corporate network environments. In addition, Integration with Check Point's Identity Awareness and Application Control enables a granular policy that is context-identity-aware and achieves a "Least Privileged" access control.

To know more about Check Point Cloud Security strategy, please refer to:

- Security Reference Architectures for Public Clouds Using CloudGuard Network Security
- Check Point Cloud Native Security Model

TO KNOW BEFORE THE DEPLOYMENT OF THE SOLUTION

PRE-REQUISITES & SUPPORTED PLATFORM

Image Name:
Check Point Cloudguard Network Security Gateway R80.40

For more information on R80.40, refer to sk160736 - Check Point R80.40
For more information on CloudGuard including documentation and known limitations, refer to sk132552 - Check Point CloudGuard solutions

Supported Version:
R80.40 GA Take 294 plus Jumbo HF Take_94 or above Jumbo HF GA releases

File Name: **Check_Point_R80_40_JUMBO_HF_Bundle_T94_sk165456_FULL.tgz**
Release Date: **07-Mar-2021**

For more information about Jumbo Hotfix Accumulator for R80.40, please refer to solution ID: sk165456

SUPPORTED DEPLOYMENT SCENARIOS

- Network Security Gateway deployment is the supported scenario currently.

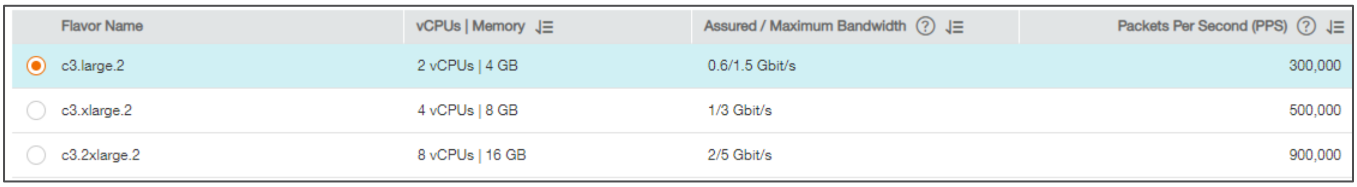
- Network Security Gateways in High Availability deployment expected to be supported scenario by end of Q221.

- Management of the security gateway can be delivered from existing customer on-premises Security Management Server or Multi-Domain Management, Check Point Cloud Management SaaS solution (Quantum Smart-1 Cloud) or using Orange MSSP management model (support is expected at later stage target during H221).

MINIMUM CONFIGURATION

- CPU: 2 vCPUs
- RAM: 4 GB
- Elastic Cloud Server Type: s3.large.2 (to be confirmed by Orange – Assured / Maximum Bandwidth)
- System Disk: 110GB
- Interfaces: 2 NICs (maximum 12 limited by Elastic Cloud Server) with 1 EIP

Elastic Cloud Server Types:



	Flavor Name	vCPUs | Memory	Assured / Maximum Bandwidth	Packets Per Second (PPS)
●	c3.large.2	2 vCPUs | 4 GB	0.6/1.5 Gbit/s	300,000
○	c3.xlarge.2	4 vCPUs | 8 GB	1/3 Gbit/s	500,000
○	c3.2xlarge.2	8 vCPUs | 16 GB	2/5 Gbit/s	900,000

PERFORMANCE

The performance numbers provided below are for CloudGuard Network Security (R80.40 release) on KVM platform.

Machine Size	**2 vCores**	**4 vCores**	**8 vCores**
NGFW (FW + IPS + Application Control)	3.2 Gbps	6 Gbps	11 Gbps
NGTP (FW + IPS + Application Control + URL Filtering + Anti-Virus + Anti-Bot)	1 Gbps	1.8 Gbps	3.6 Gbps

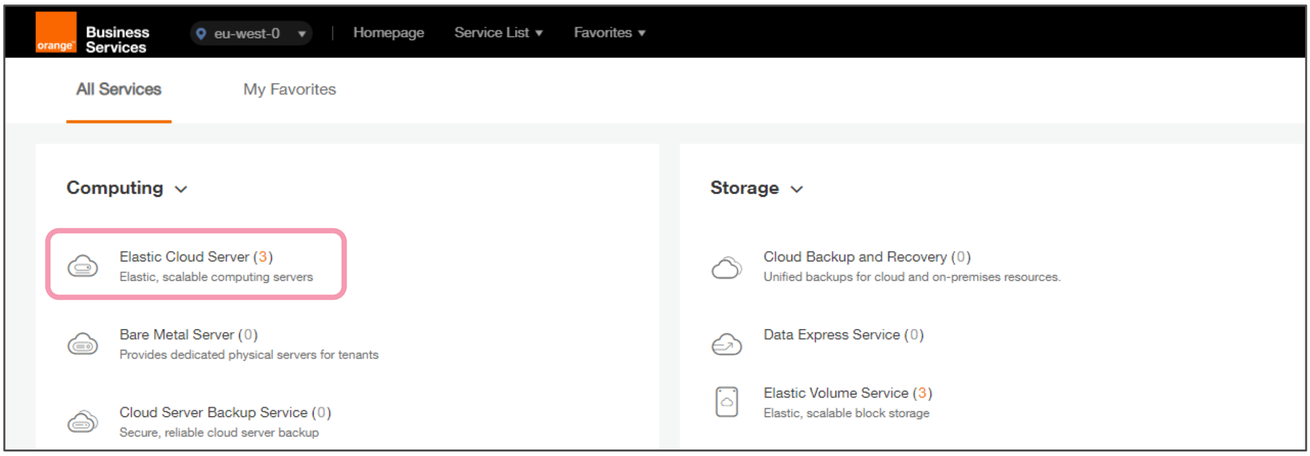
Notes:

- Next Generation Firewall (NGFW) throughput is measured with FW, IPS and Application Control, features enabled, using Check Point Enterprise testing conditions. SSL Decryption is not part of testing.
- Next Generation Threat Prevention (NGTP) throughput is measured with FW, IPS, Application Control, URL Filter, Anti-Virus, Anti-Bot features enabled, using Check Point Enterprise testing conditions. SSL Decryption is not part of testing.
- Testing conducted on Intel® Xeon® Gold 5218R Processor (27.5M Cache, 2.10 GHz) Testing RAM size was 4GB for 2vCores, 8GB for 4vCores, 16GB for 8 vCores.
- DUT (Device Under Test) R80.40 KVM image using VirtIO driver
- Recommendation is to run additional testing within your environment to ensure your performance requirements are met. Your performance may vary depending on underlying cloud vendor infrastructure performance.
- For SSL decryption figures, please approach your Check Point presales representative with the type of SSL flow analysis (inbound, outbound, both) needed, and percentage of SSL in overall traffic (75%, 90%, other).

ORANGE FLEXIBLE ENGINE WORKLOAD PREPARATION

CREATION OF AN ELASTIC CLOUD SERVER

Connect to your Orange Cloud for Business Flexible Engine tenant then go to All Services → Computing → Elastic Cloud Server page.



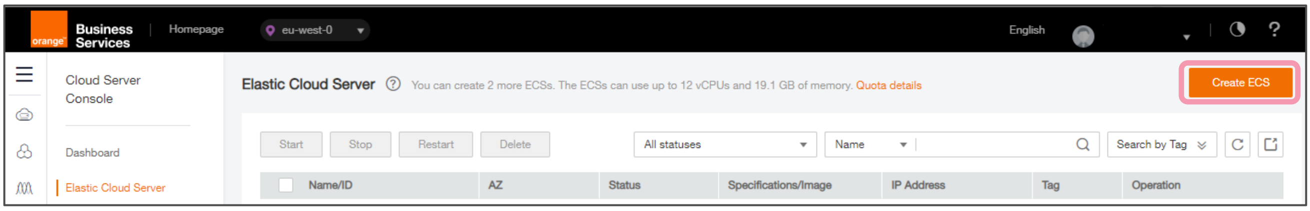
Computing ⌄

- Elastic Cloud Server (3)
  Elastic, scalable computing servers
- Bare Metal Server (0)
  Provides dedicated physical servers for tenants
- Cloud Server Backup Service (0)
  Secure, reliable cloud server backup

Storage ⌄

- Cloud Backup and Recovery (0)
  Unified backups for cloud and on-premises resources.
- Data Express Service (0)
- Elastic Volume Service (3)
  Elastic, scalable block storage

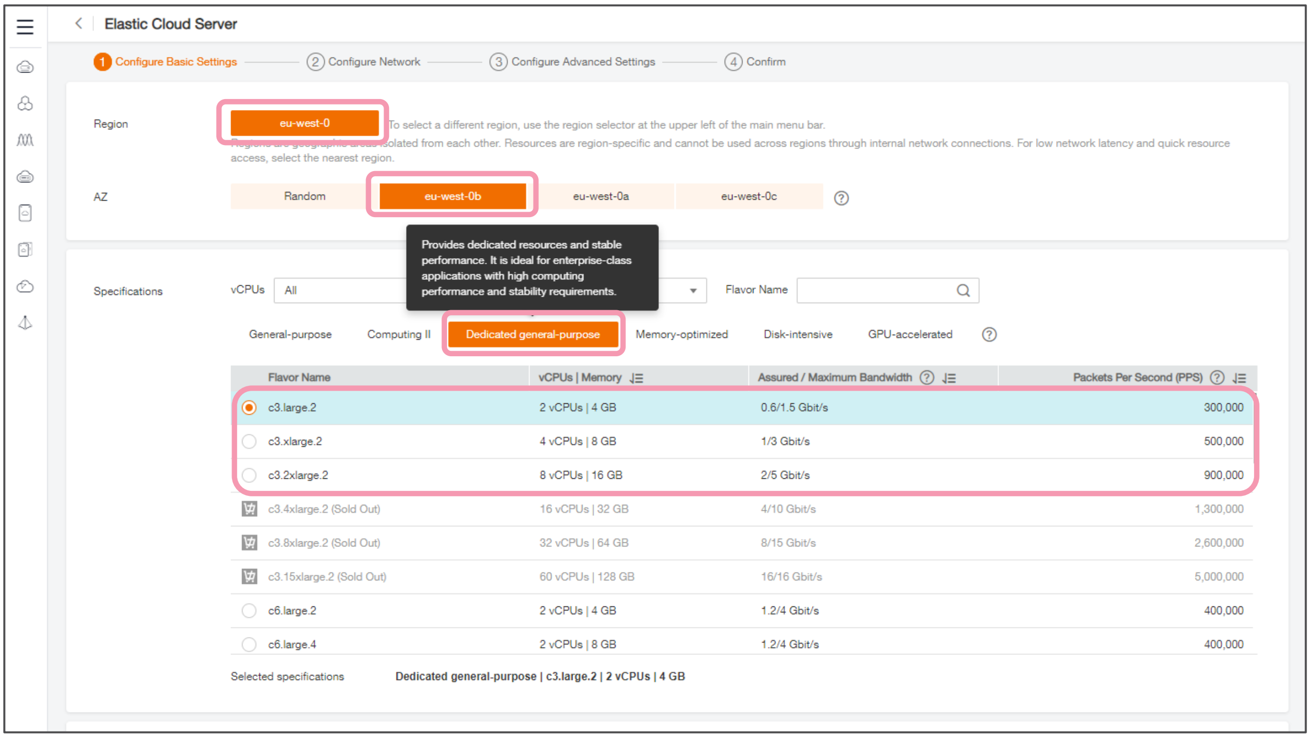
Click on Create ECS button.



Elastic Cloud Server ⓘ You can create 2 more ECSs. The ECSs can use up to 12 vCPUs and 19.1 GB of memory. Quota details

□	Name/ID	AZ	Status	Specifications/Image	IP Address	Tag	Operation

Select Region, AZ and image Flavor name with target Specifications type.



Region: eu-west-0 To select a different region, use the region selector at the upper left of the main menu bar. Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

AZ: eu-west-0b

Provides dedicated resources and stable performance. It is ideal for enterprise-class applications with high computing performance and stability requirements.

Specifications: vCPUs All

	Flavor Name	vCPUs | Memory	Assured / Maximum Bandwidth	Packets Per Second (PPS)
●	c3.large.2	2 vCPUs | 4 GB	0.6/1.5 Gbit/s	300,000
○	c3.xlarge.2	4 vCPUs | 8 GB	1/3 Gbit/s	500,000
○	c3.2xlarge.2	8 vCPUs | 16 GB	2/5 Gbit/s	900,000
	c3.4xlarge.2 (Sold Out)	16 vCPUs | 32 GB	4/10 Gbit/s	1,300,000
	c3.8xlarge.2 (Sold Out)	32 vCPUs | 64 GB	8/15 Gbit/s	2,600,000
	c3.15xlarge.2 (Sold Out)	60 vCPUs | 128 GB	16/16 Gbit/s	5,000,000
○	c6.large.2	2 vCPUs | 4 GB	1.2/4 Gbit/s	400,000
○	c6.large.4	2 vCPUs | 8 GB	1.2/4 Gbit/s	400,000

Selected specifications **Dedicated general-purpose | c3.large.2 | 2 vCPUs | 4 GB**

Finally, select Public Image named Check Point Cloudguard Network Security Gateway R80.40.

On System Disk parameter, select Common I/O and allow a minimum of 110 GB.

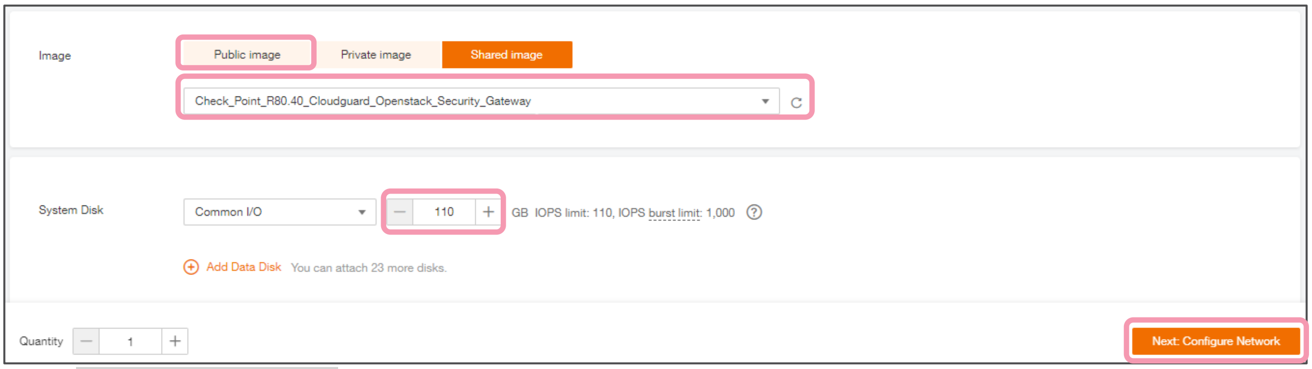


Image: Public image | Private image | Shared image

Check_Point_R80.40_Cloudguard_Openstack_Security_Gateway

System Disk: Common I/O — 110 + GB IOPS limit: 110, IOPS burst limit: 1,000

Add Data Disk You can attach 23 more disks.

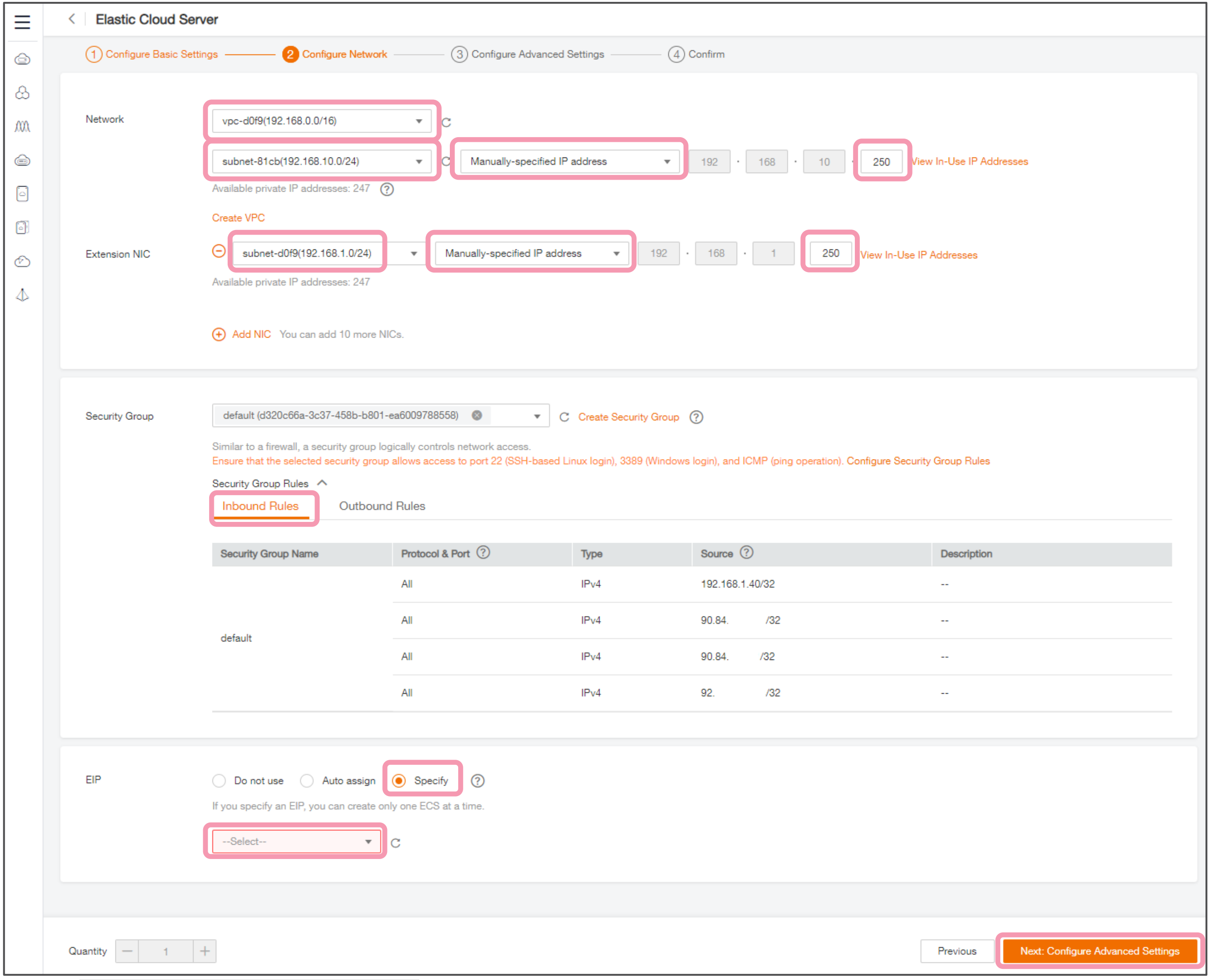
Quantity — 1 +

Click Next Configure Network button.

Configure at least two Network interfaces for the Security Gateway instance on two different subnets, using Manually-specified IP address option.

Before the first Security Policy push on Security Gateway, make sure to restrict as much as possible the access to the instance using proper Inbound Rules of the Security Group Rules. Don't forget to remove the restrictions afterwards.

Finalize the Network configuration by assigning an already defined EIP (Elastic IP) IP public address to the external interface of your Security Gateway instance in order to allow updates or being able to manage it from your Management Security Server on premises over the Internet.



Elastic Cloud Server

① Configure Basic Settings — ② Configure Network — ③ Configure Advanced Settings — ④ Confirm

Network: vpc-d0f9(192.168.0.0/16)

subnet-81cb(192.168.10.0/24) | Manually-specified IP address | 192 . 168 . 10 . 250 View In-Use IP Addresses

Available private IP addresses: 247

Create VPC

Extension NIC: subnet-d0f9(192.168.1.0/24) | Manually-specified IP address | 192 . 168 . 1 . 250 View In-Use IP Addresses

Available private IP addresses: 247

Add NIC You can add 10 more NICs.

Security Group: default (d320c66a-3c37-458b-b801-ea6009788558) Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules

Security Group Name	Protocol & Port	Type	Source	Description
default	All	IPv4	192.168.1.40/32	--
	All	IPv4	90.84. /32	--
	All	IPv4	90.84. /32	--
	All	IPv4	92. /32	--

EIP: ○ Do not use ○ Auto assign ● Specify

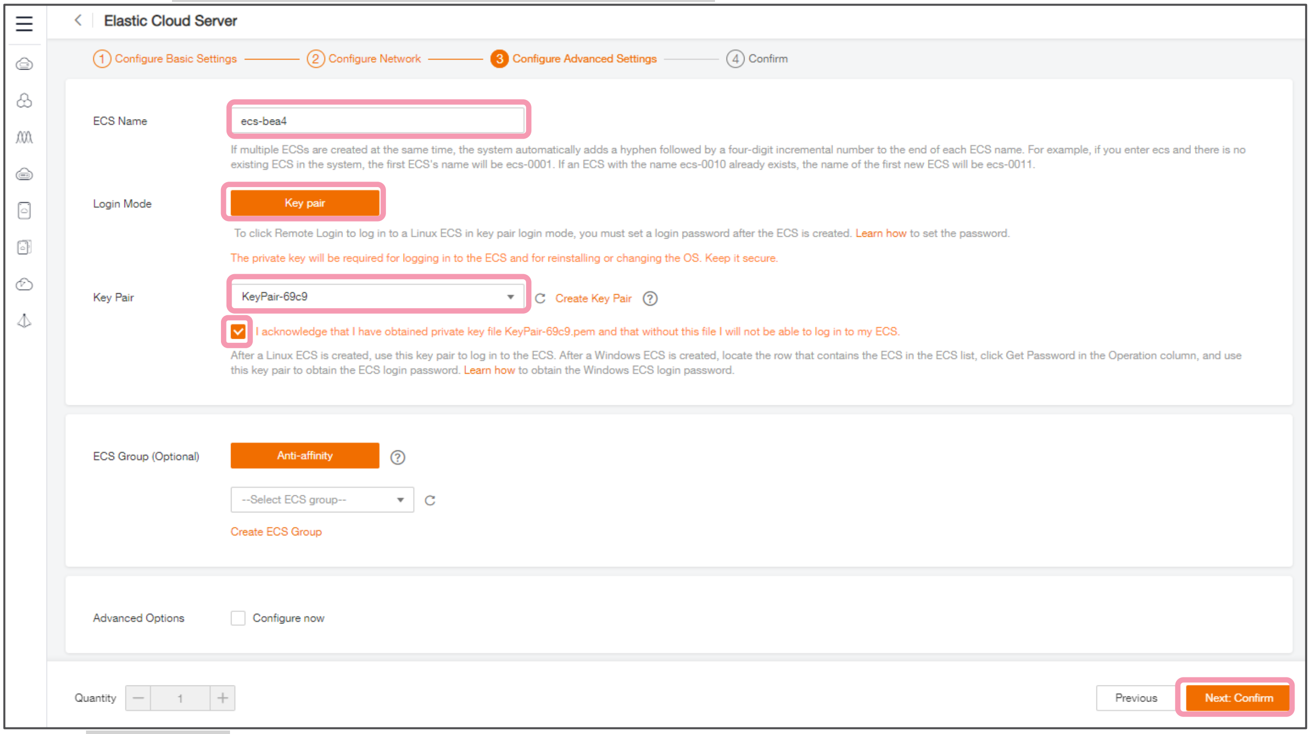
If you specify an EIP, you can create only one ECS at a time.

--Select--

Quantity — 1 +

Click Next Configure Advanced Settings button.

Indicates an ECS Name, Select Key pair that already been created or click Create Key Pair.
Tick the box I acknowledge that I have obtain private key file …



Elastic Cloud Server

1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

ECS Name: ecs-bea4

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to the end of each ECS name. For example, if you enter ecs and there is no existing ECS in the system, the first ECS's name will be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Key pair

To click Remote Login to log in to a Linux ECS in key pair login mode, you must set a login password after the ECS is created. Learn how to set the password.

The private key will be required for logging in to the ECS and for reinstalling or changing the OS. Keep it secure.

Key Pair: KeyPair-69c9 — Create Key Pair

☑ I acknowledge that I have obtained private key file KeyPair-69c9.pem and that without this file I will not be able to log in to my ECS.

After a Linux ECS is created, use this key pair to log in to the ECS. After a Windows ECS is created, locate the row that contains the ECS in the ECS list, click Get Password in the Operation column, and use this key pair to obtain the ECS login password. Learn how to obtain the Windows ECS login password.

ECS Group (Optional): Anti-affinity

--Select ECS group--

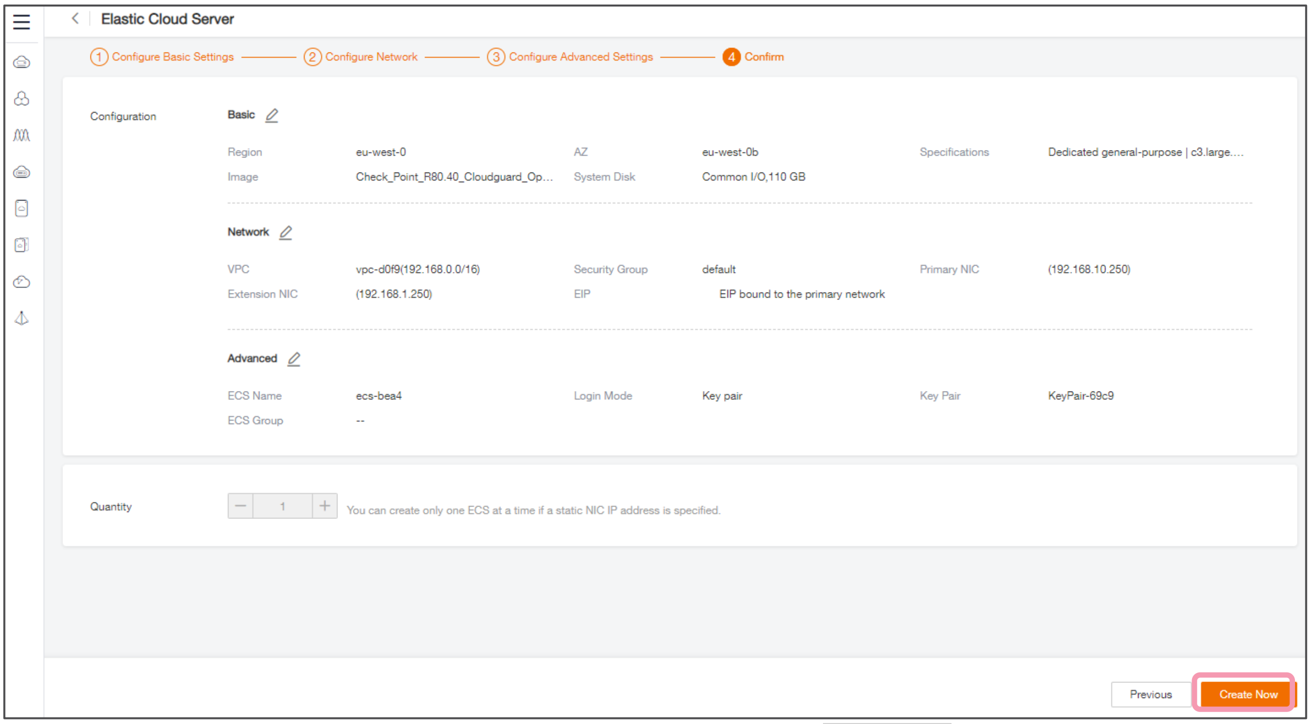
Create ECS Group

Advanced Options: □ Configure now

Quantity: 1

Previous | Next: Confirm

Click Next Confirm button.



Elastic Cloud Server

1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Configuration

Basic

Region	eu-west-0	AZ	eu-west-0b	Specifications	Dedicated general-purpose | c3.large.…
Image	Check_Point_R80.40_Cloudguard_Op…	System Disk	Common I/O,110 GB		

Network

VPC	vpc-d0f9(192.168.0.0/16)	Security Group	default	Primary NIC	(192.168.10.250)
Extension NIC	(192.168.1.250)	EIP	EIP bound to the primary network		

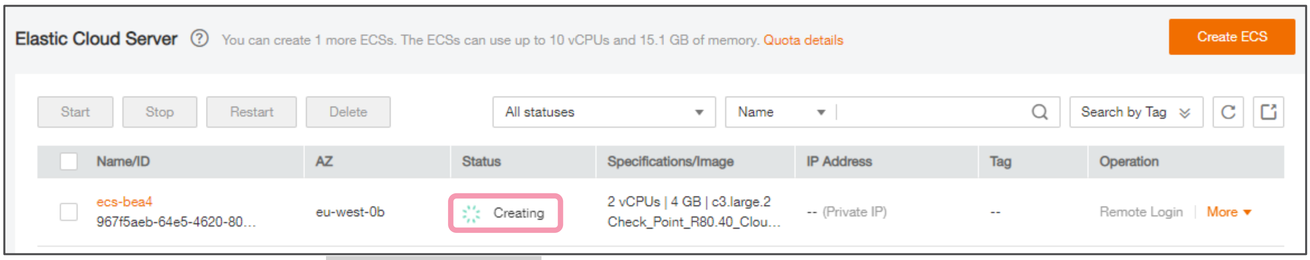
Advanced

ECS Name	ecs-bea4	Login Mode	Key pair	Key Pair	KeyPair-69c9
ECS Group	--				

Quantity: 1 — You can create only one ECS at a time if a static NIC IP address is specified.

Previous | Create Now

Review closely the configuration to avoid misconfiguration and click Create Now button.



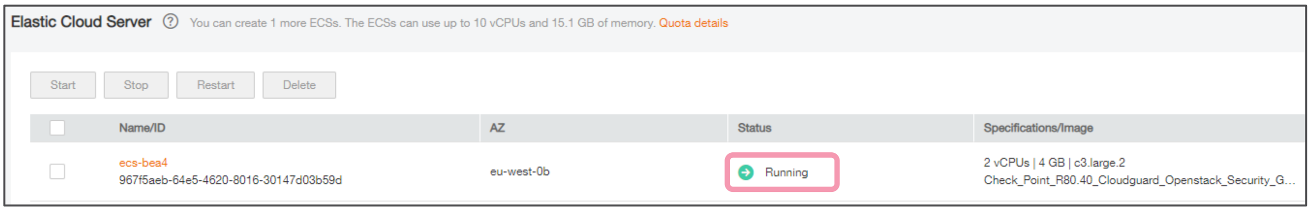
Elastic Cloud Server — You can create 1 more ECSs. The ECSs can use up to 10 vCPUs and 15.1 GB of memory. Quota details

Create ECS

Start | Stop | Restart | Delete — All statuses — Name — Search by Tag

Name/ID	AZ	Status	Specifications/Image	IP Address	Tag	Operation
ecs-bea4 967f5aeb-64e5-4620-80…	eu-west-0b	Creating	2 vCPUs | 4 GB | c3.large.2 Check_Point_R80.40_Clou…	-- (Private IP)	--	Remote Login | More

Check the status of your Elastic Cloud Server Security Gateway creation to make sure it finished after few minutes from Creating to Running state.


Elastic Cloud Server
You can create 1 more ECSs. The ECSs can use up to 10 vCPUs and 15.1 GB of memory. Quota details
Start
Stop
Restart
Delete

□	Name/ID	AZ	Status	Specifications/Image
□	ecs-bea4 967f5aeb-64e5-4620-8016-30147d03b59d	eu-west-0b	Running	2 vCPUs | 4 GB | c3.large.2 Check_Point_R80.40_Cloudguard_Openstack_Security_G...

Once in Running state, make sure to change the following configuration to your instance before moving to next step.

Important notes:

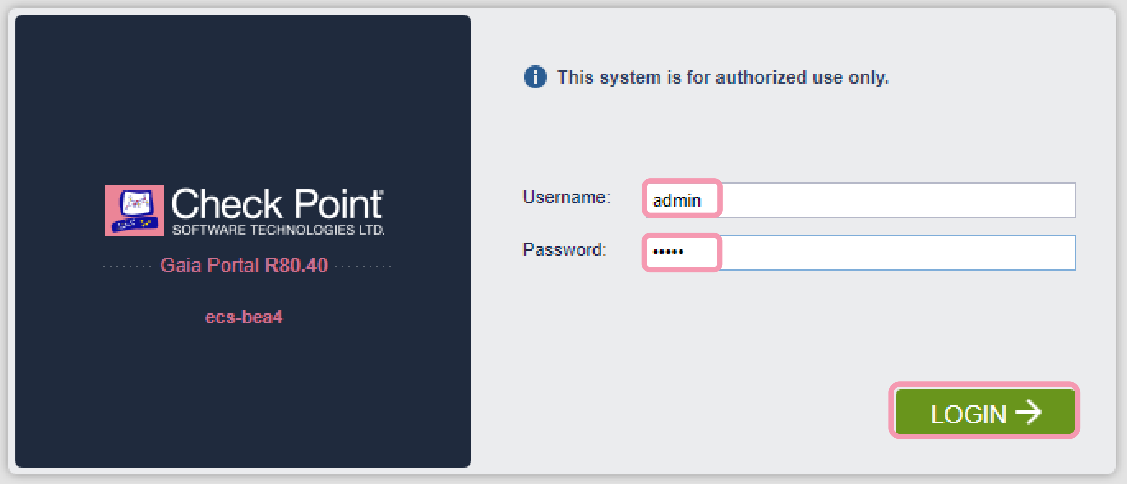
1. On NIC Section, Make sure to deactivate the Source/Destination Check for all interfaces of the ECS.
2. Don’t forget to set the EIP Bandwidth Size limit accordingly (1 Gbps by example) and to make sure it is bind to external interface topology of your Security Gateway.
3. Restrict Security Groups policy as much as possible when gateway policy is not installed yet. Don’t forget to remove the restrictions afterwards.

Once above three changes are **effective**, please move to next section.

NETWORK SECURITY GATEWAY – INTEGRATION STEPS

FIRST TIME WIZARD CONFIGURATION

Connect to https://<IP_of_Elastic_Cloud_Server_Instance> using your browser.



Check Point SOFTWARE TECHNOLOGIES LTD.

Gaia Portal R80.40

ecs-bea4

This system is for authorized use only.

Username: admin

Password: •••••

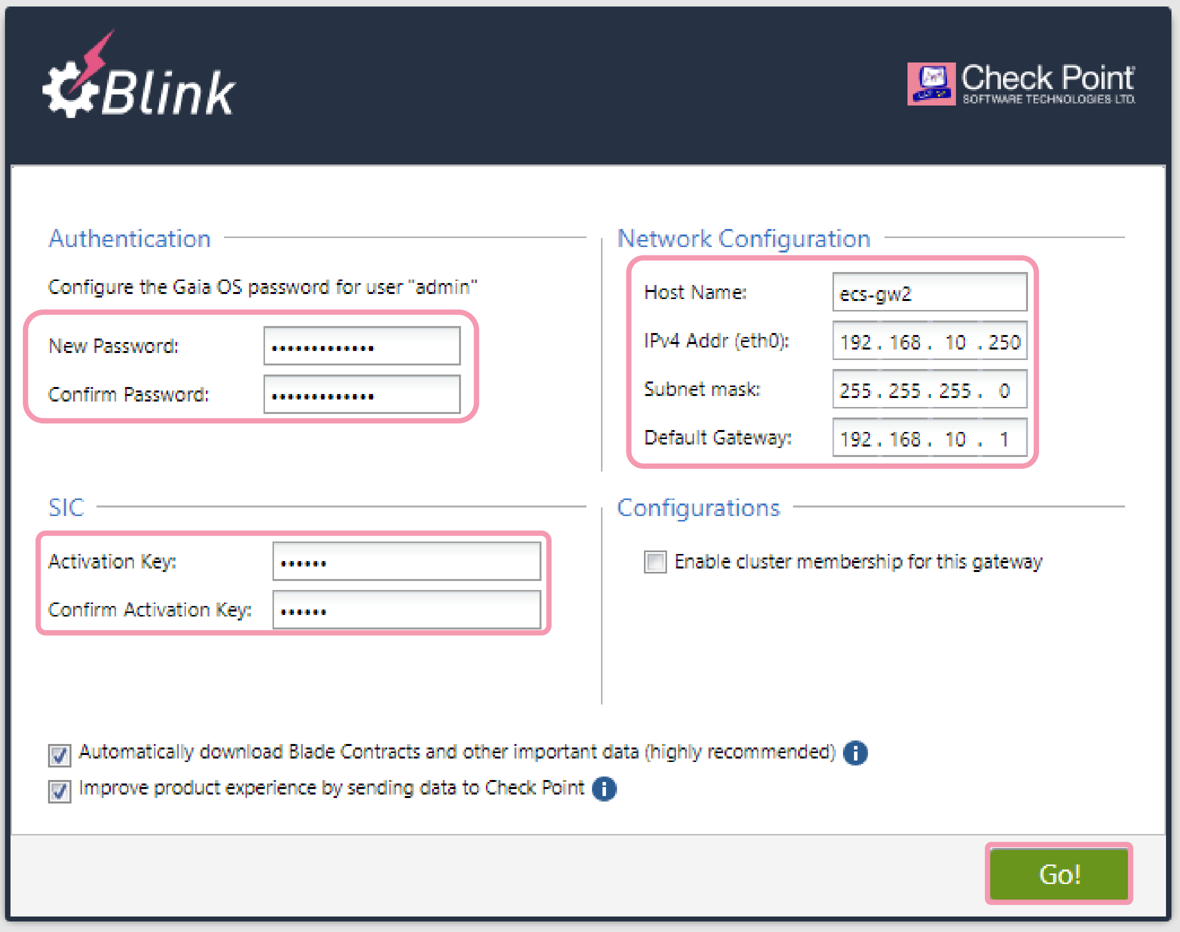
LOGIN →

Once connected, follow the first time wizard user using `admin` as Username & `admin` as Password. Click LOGIN button.

Then set a New password for admin user and Confirm Password.

Create a SIC (Secure Internal Communication) Activation Key one time password that will be used to establish the trust between the Security Gateway and your Security Management Server.

Configure Host Name and the external interface private IP (tied to the EIP) its Subnet mask and Default Gateway. Then click on Go! button.



Blink

Check Point SOFTWARE TECHNOLOGIES LTD.

Authentication

Configure the Gaia OS password for user "admin"

New Password: ••••••••••••••

Confirm Password: ••••••••••••••

Network Configuration

Host Name: ecs-gw2

IPv4 Addr (eth0): 192 . 168 . 10 . 250

Subnet mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 10 . 1

SIC

Activation Key: ••••••

Confirm Activation Key: ••••••

Configurations

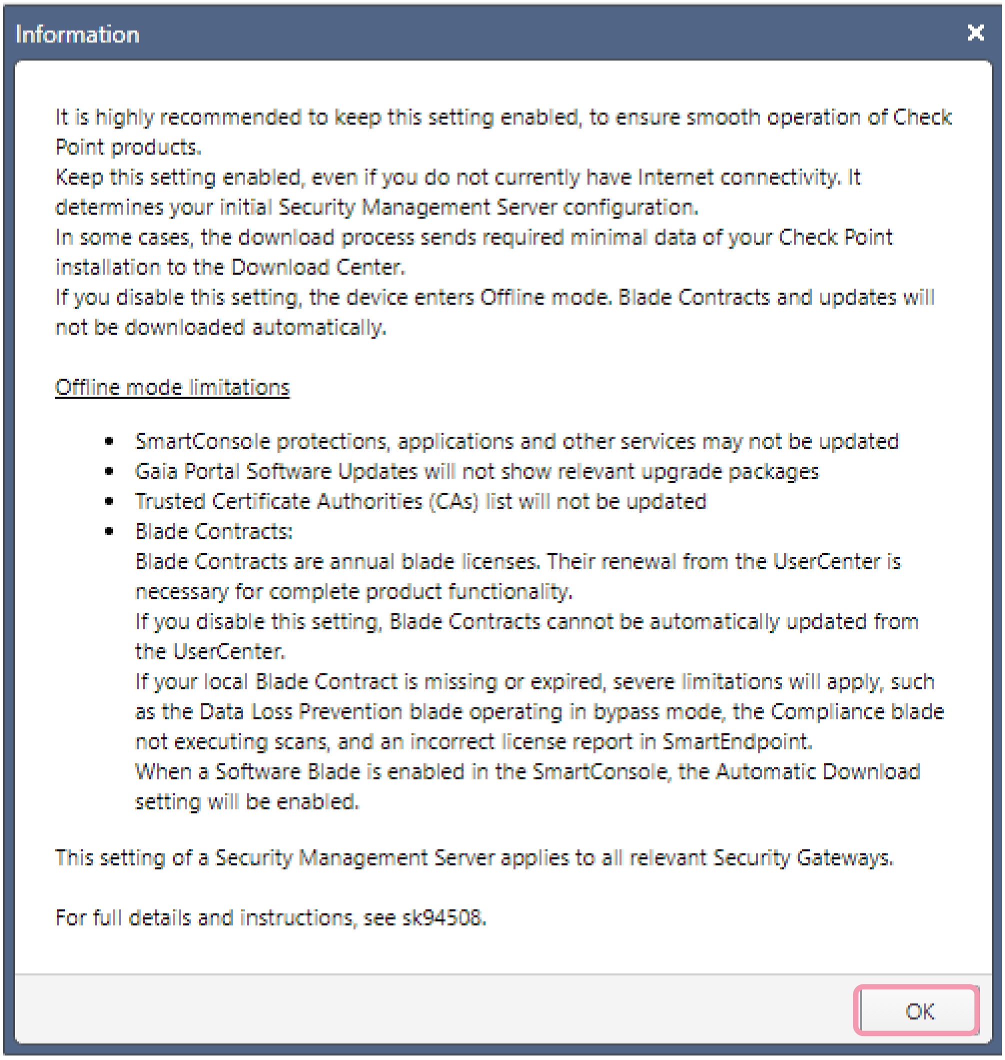
☐ Enable cluster membership for this gateway

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

☑ Improve product experience by sending data to Check Point

Go!

Note: It is highly recommended to leave the first option activated. Full details on next page.



Information

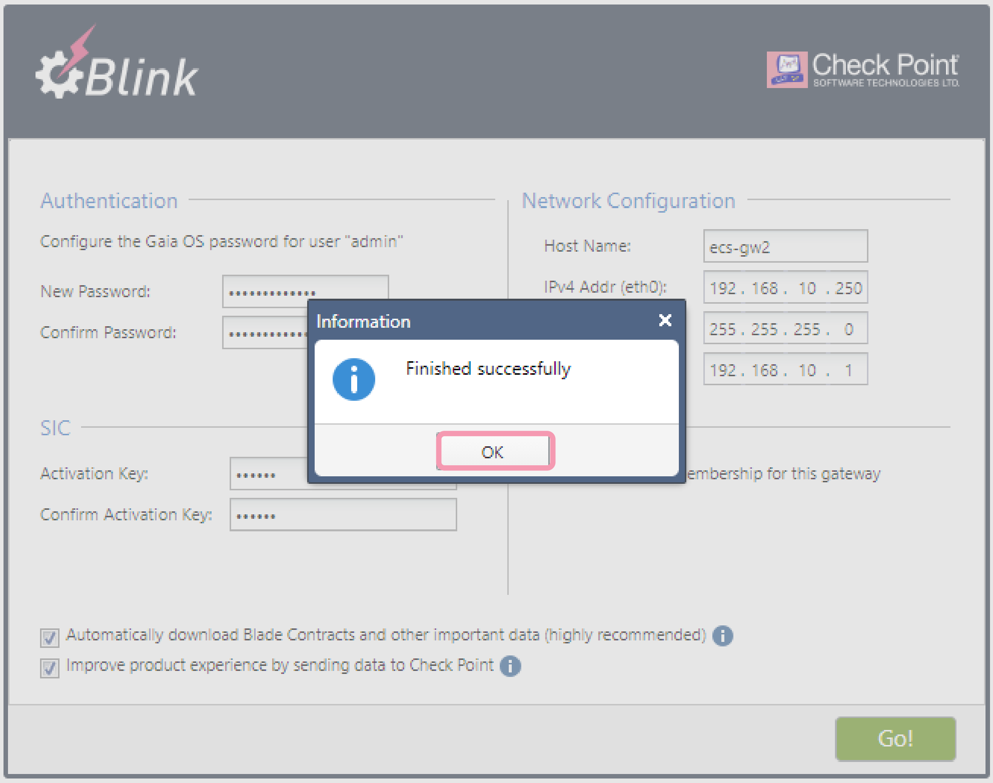
It is highly recommended to keep this setting enabled, to ensure smooth operation of Check Point products.
Keep this setting enabled, even if you do not currently have Internet connectivity. It determines your initial Security Management Server configuration.
In some cases, the download process sends required minimal data of your Check Point installation to the Download Center.
If you disable this setting, the device enters Offline mode. Blade Contracts and updates will not be downloaded automatically.

Offline mode limitations

- SmartConsole protections, applications and other services may not be updated
- Gaia Portal Software Updates will not show relevant upgrade packages
- Trusted Certificate Authorities (CAs) list will not be updated
- Blade Contracts:
  Blade Contracts are annual blade licenses. Their renewal from the UserCenter is necessary for complete product functionality.
  If you disable this setting, Blade Contracts cannot be automatically updated from the UserCenter.
  If your local Blade Contract is missing or expired, severe limitations will apply, such as the Data Loss Prevention blade operating in bypass mode, the Compliance blade not executing scans, and an incorrect license report in SmartEndpoint.
  When a Software Blade is enabled in the SmartConsole, the Automatic Download setting will be enabled.

This setting of a Security Management Server applies to all relevant Security Gateways.

For full details and instructions, see sk94508.



Blink

Authentication

Configure the Gaia OS password for user "admin"

New Password: ••••••••••••••

Confirm Password: ••••••••••••

Network Configuration

Host Name: ecs-gw2

IPv4 Addr (eth0): 192 . 168 . 10 . 250

255 . 255 . 255 . 0

192 . 168 . 10 . 1

SIC

Activation Key: ••••••

Confirm Activation Key: ••••••

embership for this gateway

Information

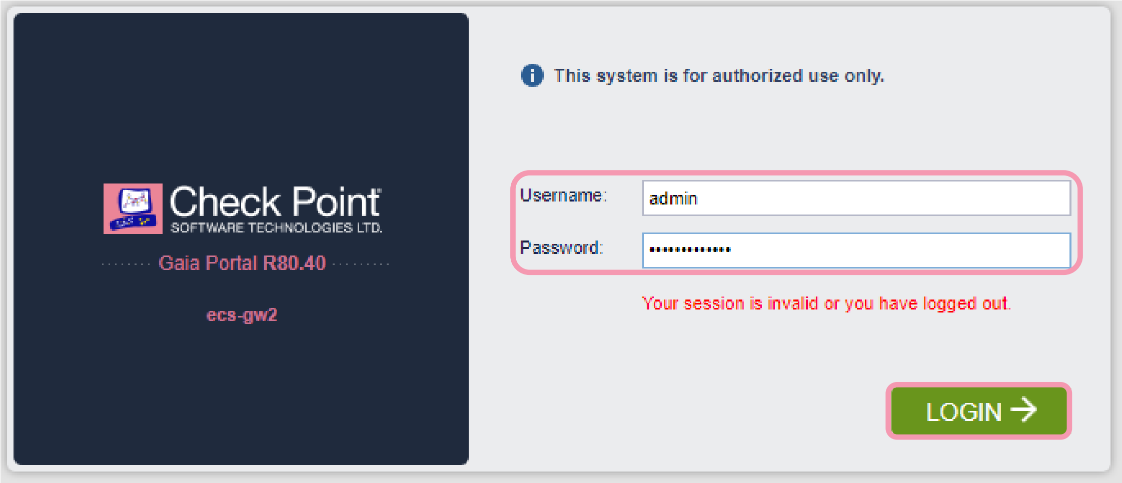
Finished successfully

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

☑ Improve product experience by sending data to Check Point

Once configuration is complete and finished successfully (process is immediate), click OK button.

Session is disconnected; please reconnect using newly defined password, then click LOGIN → button.



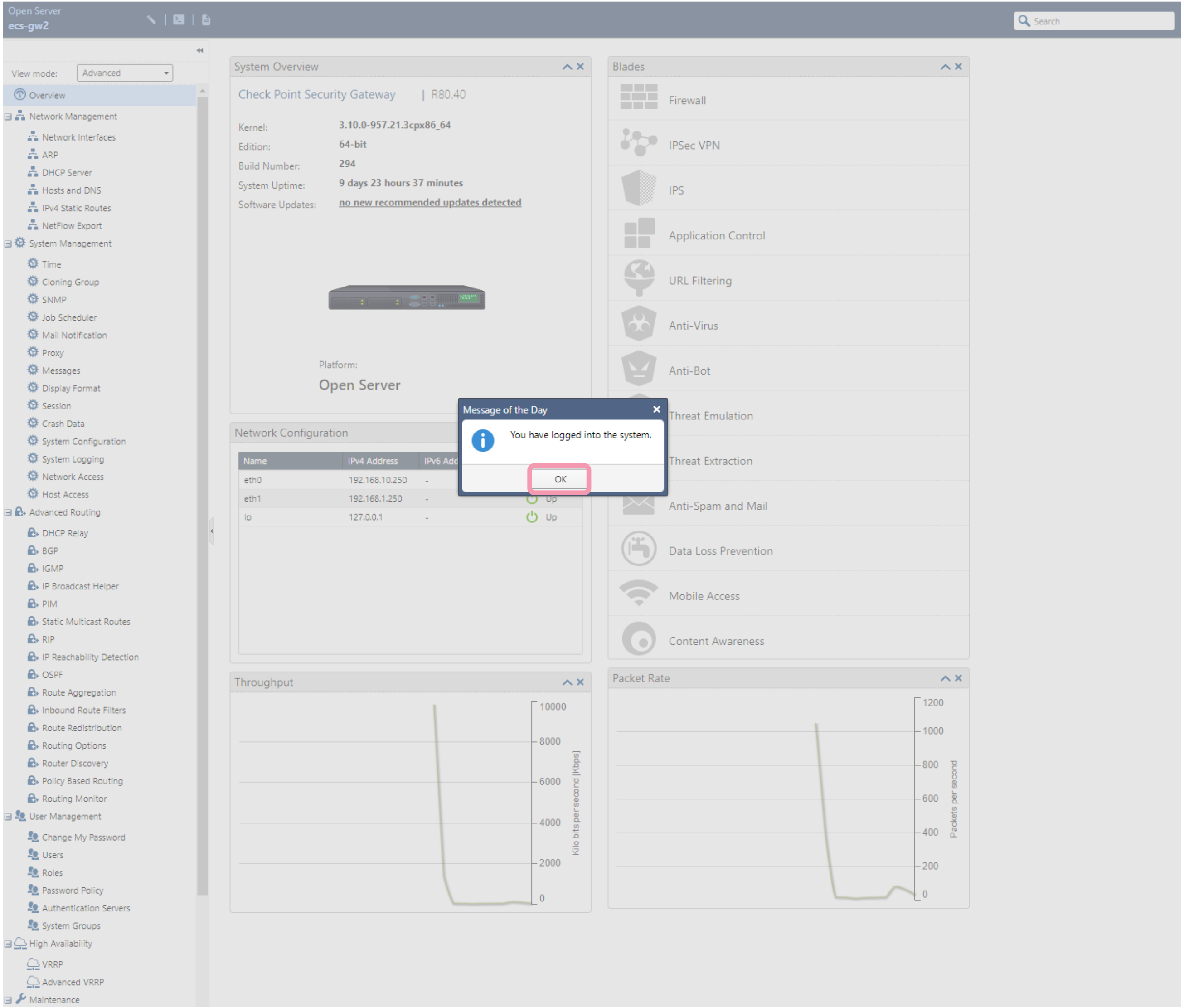
This system is for authorized use only.

Username: admin

Password: ••••••••••••••

Your session is invalid or you have logged out.

You are now logged to the Gaia OS WebUI console. Click OK button.



Check Point Security Gateway | R80.40

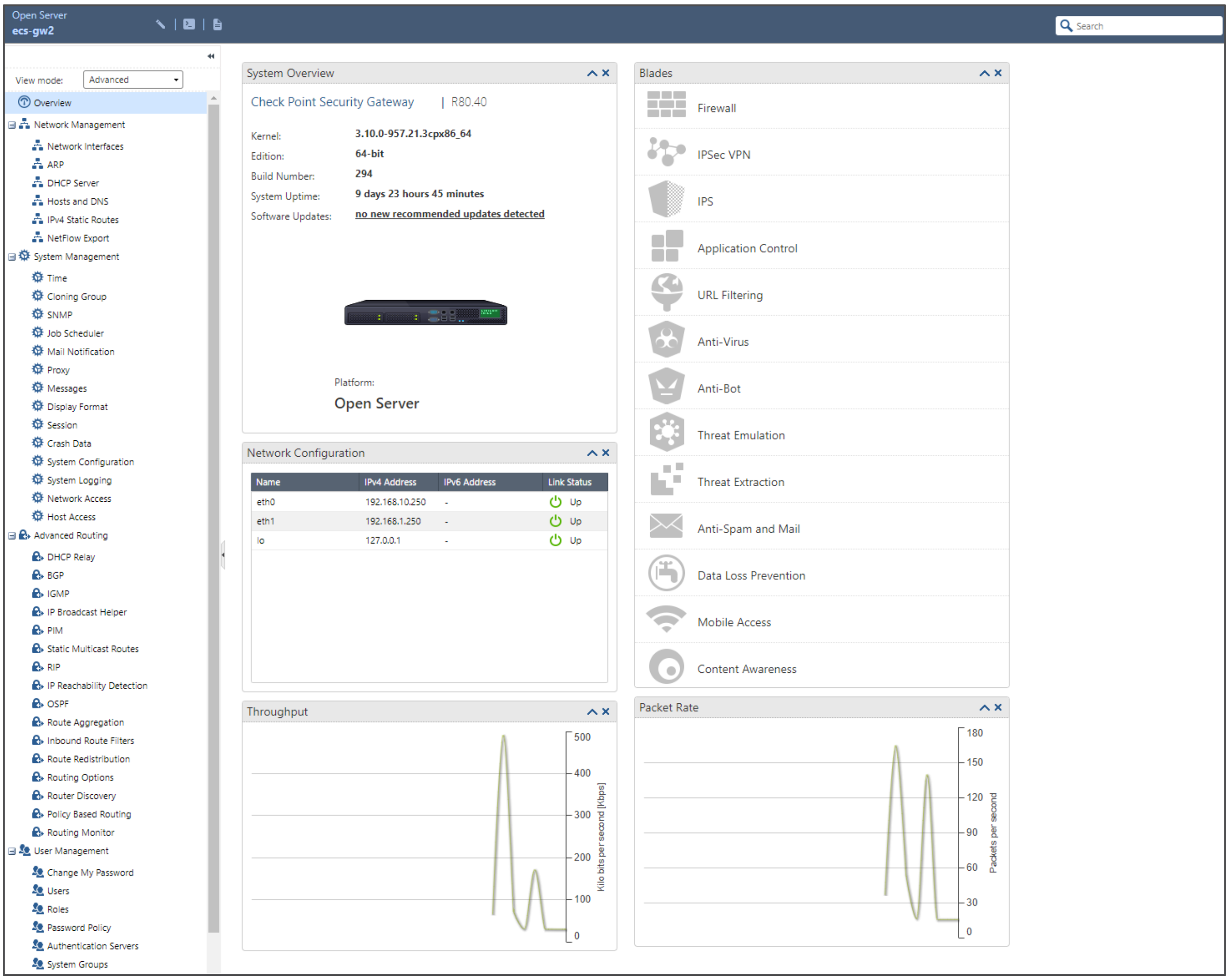
Kernel:	3.10.0-957.21.3cpx86_64
Edition:	64-bit
Build Number:	294
System Uptime:	9 days 23 hours 37 minutes
Software Updates:	no new recommended updates detected

Platform:
Open Server

Name	IPv4 Address	IPv6 Add	
eth0	192.168.10.250	-	
eth1	192.168.1.250	-	Up
lo	127.0.0.1	-	Up

Message of the Day

You have logged into the system.



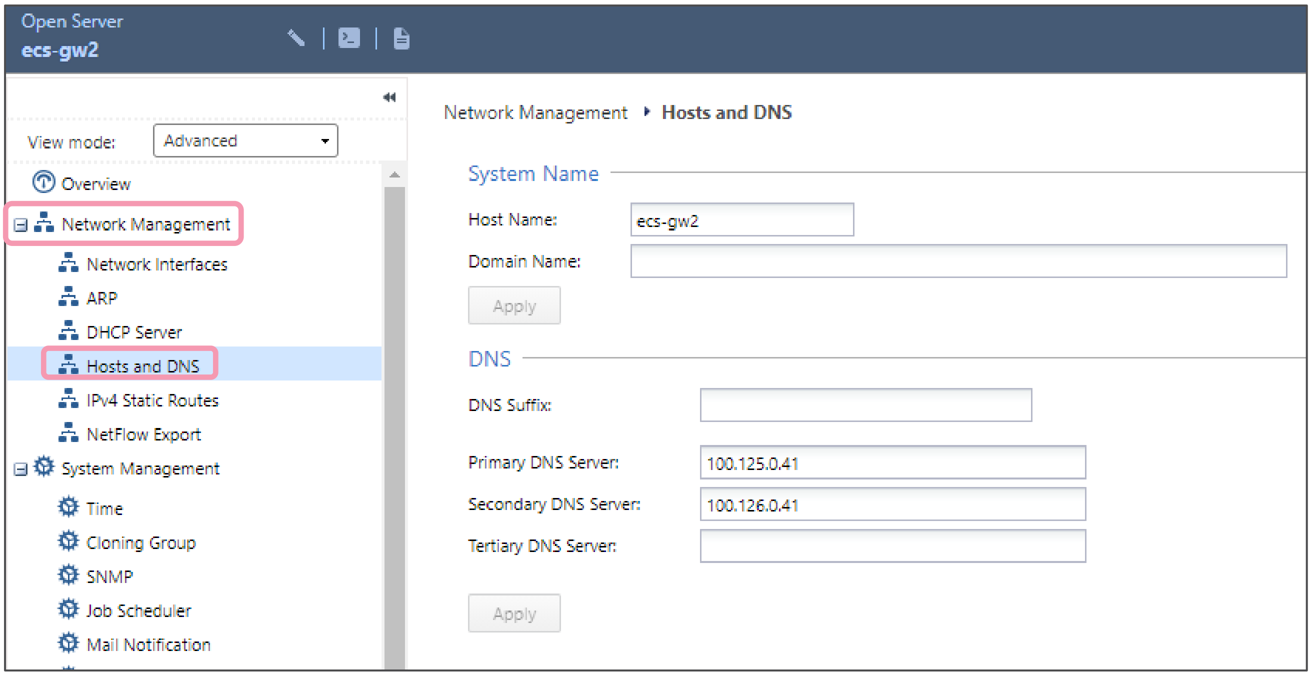
Check Point Security Gateway | R80.40

Kernel:	3.10.0-957.21.3cpx86_64
Edition:	64-bit
Build Number:	294
System Uptime:	9 days 23 hours 45 minutes
Software Updates:	no new recommended updates detected

Platform:
Open Server

Name	IPv4 Address	IPv6 Address	Link Status
eth0	192.168.10.250	-	Up
eth1	192.168.1.250	-	Up
lo	127.0.0.1	-	Up

Please make sure DNS configuration is correct going to Network Management menu then Hosts and DNS section.



Network Management ▸ Hosts and DNS

System Name

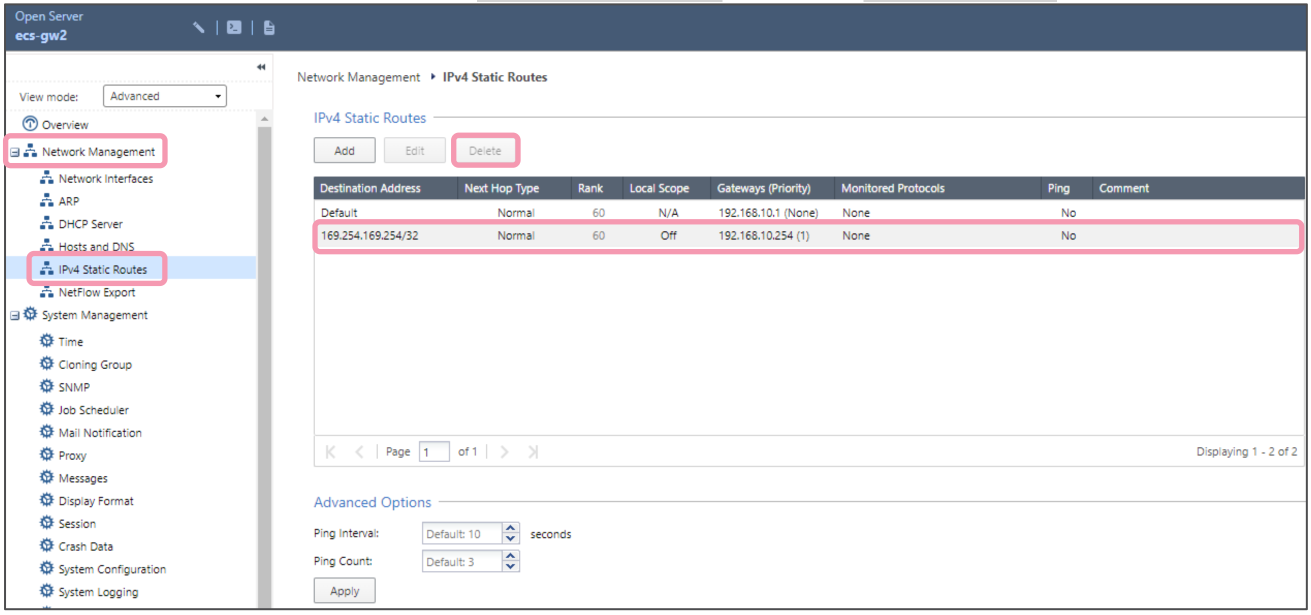
Host Name:	ecs-gw2
Domain Name:	

DNS

DNS Suffix:	
Primary DNS Server:	100.125.0.41
Secondary DNS Server:	100.126.0.41
Tertiary DNS Server:	

Important note:

Make sure to delete local route going to Network Management menu then IPv4 Static Routes section.



Network Management ▸ **IPv4 Static Routes**

IPv4 Static Routes

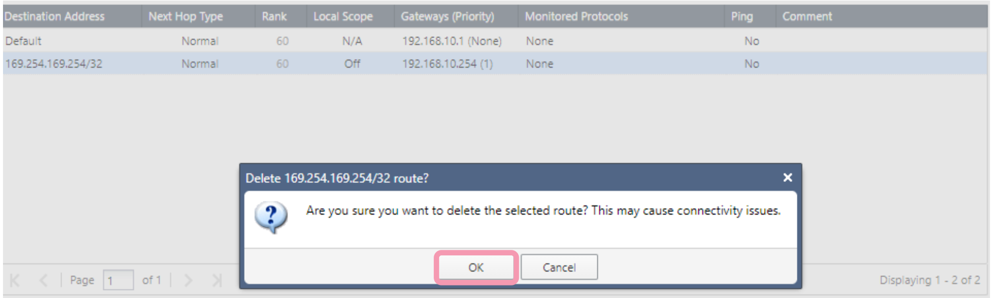
Destination Address	Next Hop Type	Rank	Local Scope	Gateways (Priority)	Monitored Protocols	Ping	Comment
Default	Normal	60	N/A	192.168.10.1 (None)	None	No	
169.254.169.254/32	Normal	60	Off	192.168.10.254 (1)	None	No	

Advanced Options

Ping Interval: Default: 10 seconds

Ping Count: Default: 3

Select 169.254.169.254/32 route, click Delete button.

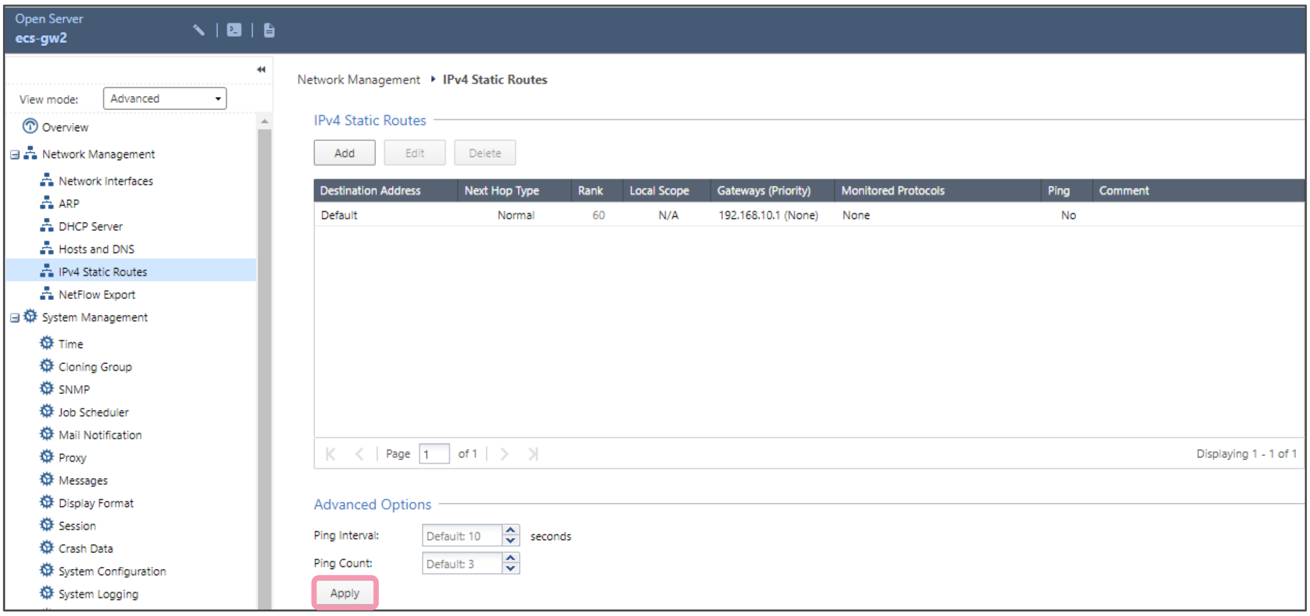


Destination Address	Next Hop Type	Rank	Local Scope	Gateways (Priority)	Monitored Protocols	Ping	Comment
Default	Normal	60	N/A	192.168.10.1 (None)	None	No	
169.254.169.254/32	Normal	60	Off	192.168.10.254 (1)	None	No	

Delete 169.254.169.254/32 route?

Are you sure you want to delete the selected route? This may cause connectivity issues.

If correct route selected, then click OK button.



Network Management ▸ **IPv4 Static Routes**

IPv4 Static Routes

Destination Address	Next Hop Type	Rank	Local Scope	Gateways (Priority)	Monitored Protocols	Ping	Comment
Default	Normal	60	N/A	192.168.10.1 (None)	None	No	

Advanced Options

Ping Interval: Default: 10 seconds

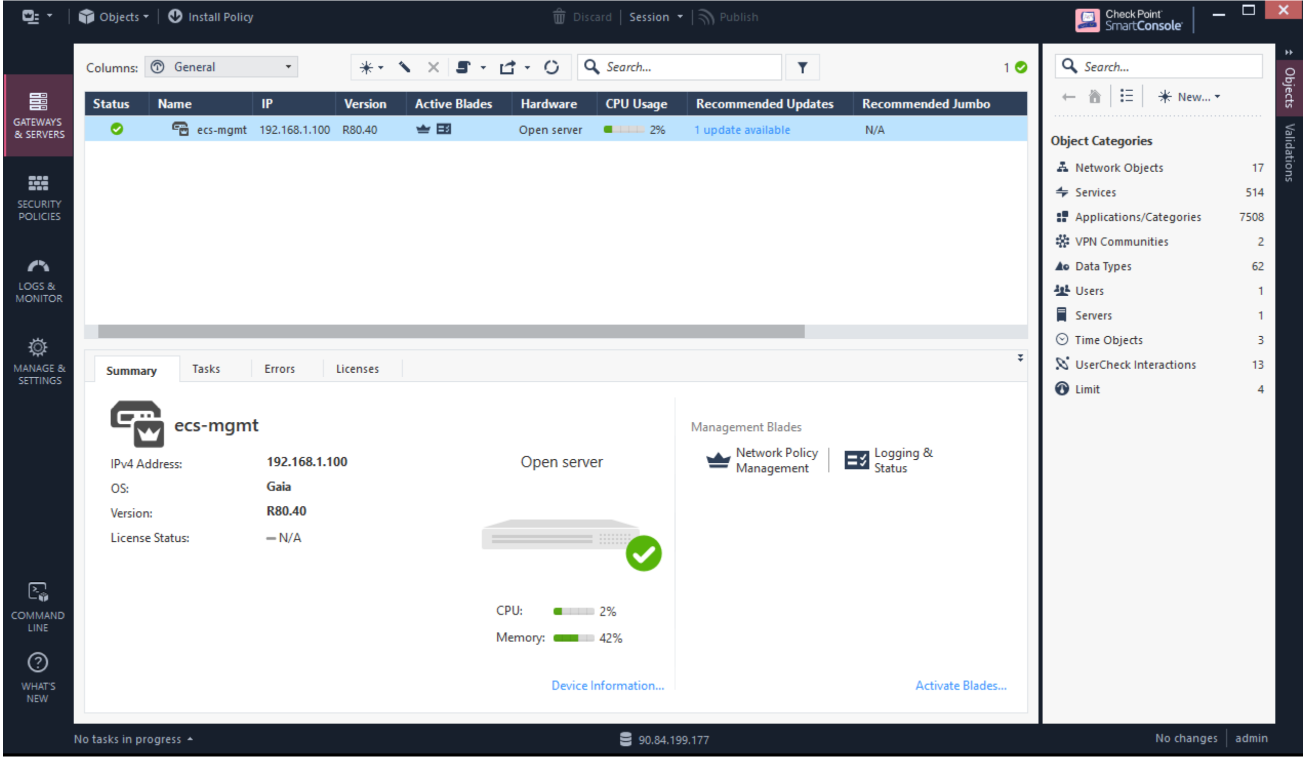
Ping Count: Default: 3

Don’t forget to click Apply button.

CONFIGURATION & MANAGEMENT INTEGRATION

Once gateway OS configuration is finalized, next step is to create gateway object in Management Server and connect to it using SmartConsole or API.

Open your Management Server SmartConsole:



Columns: General

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo
✓	ecs-mgmt	192.168.1.100	R80.40		Open server	2%	1 update available	N/A

ecs-mgmt

IPv4 Address:	192.168.1.100
OS:	Gaia
Version:	R80.40
License Status:	— N/A

Open server

CPU: 2%
Memory: 42%

Device Information...

Management Blades: Network Policy Management, Logging & Status

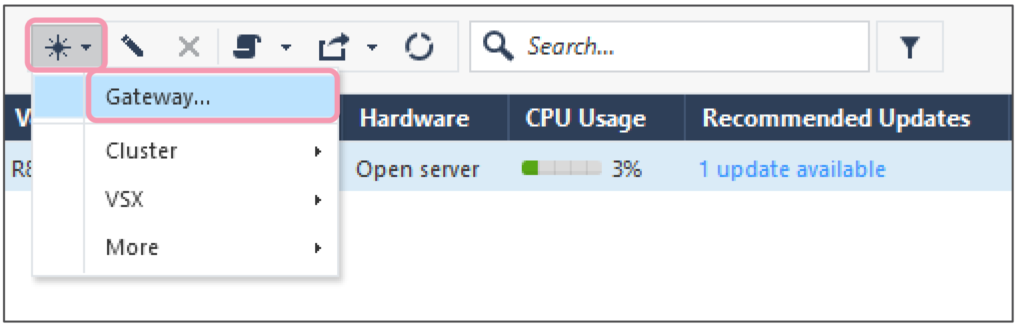
Activate Blades...

Object Categories

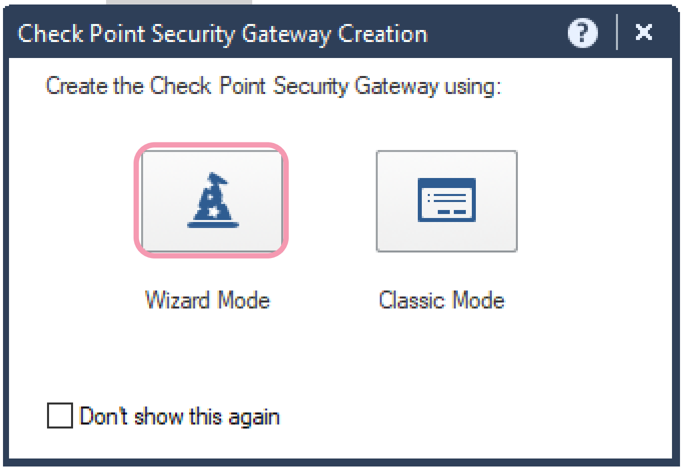
Network Objects	17
Services	514
Applications/Categories	7508
VPN Communities	2
Data Types	62
Users	1
Servers	1
Time Objects	3
UserCheck Interactions	13
Limit	4

No tasks in progress
90.84.199.177
No changes
admin

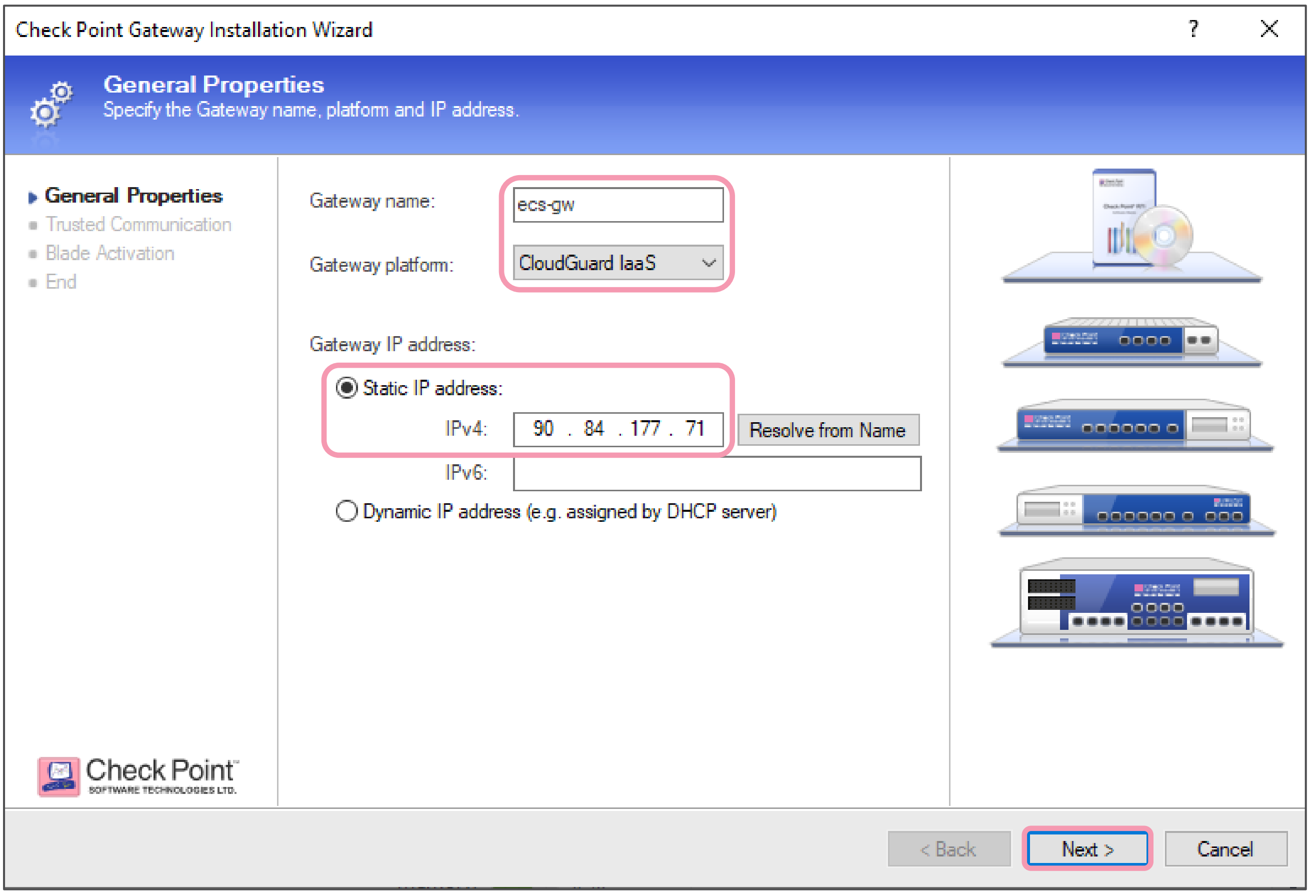
Click on ✳▾ button then Gateway... button:



Click on Wizard Mode button


Check Point Security Gateway Creation
Create the Check Point Security Gateway using:
Wizard Mode
Classic Mode
□ Don't show this again

Fill Gateway name and select Cloudguard IaaS as Gateway platform. Fill the IP adress of the EIP (Elastic IP) public IP adress of your Elastic Cloud Server Security Gateway instance. Click Next button.



Check Point Gateway Installation Wizard

General Properties
Specify the Gateway name, platform and IP address.

- General Properties
- Trusted Communication
- Blade Activation
- End

Gateway name: ecs-gw

Gateway platform: CloudGuard IaaS

Gateway IP address:

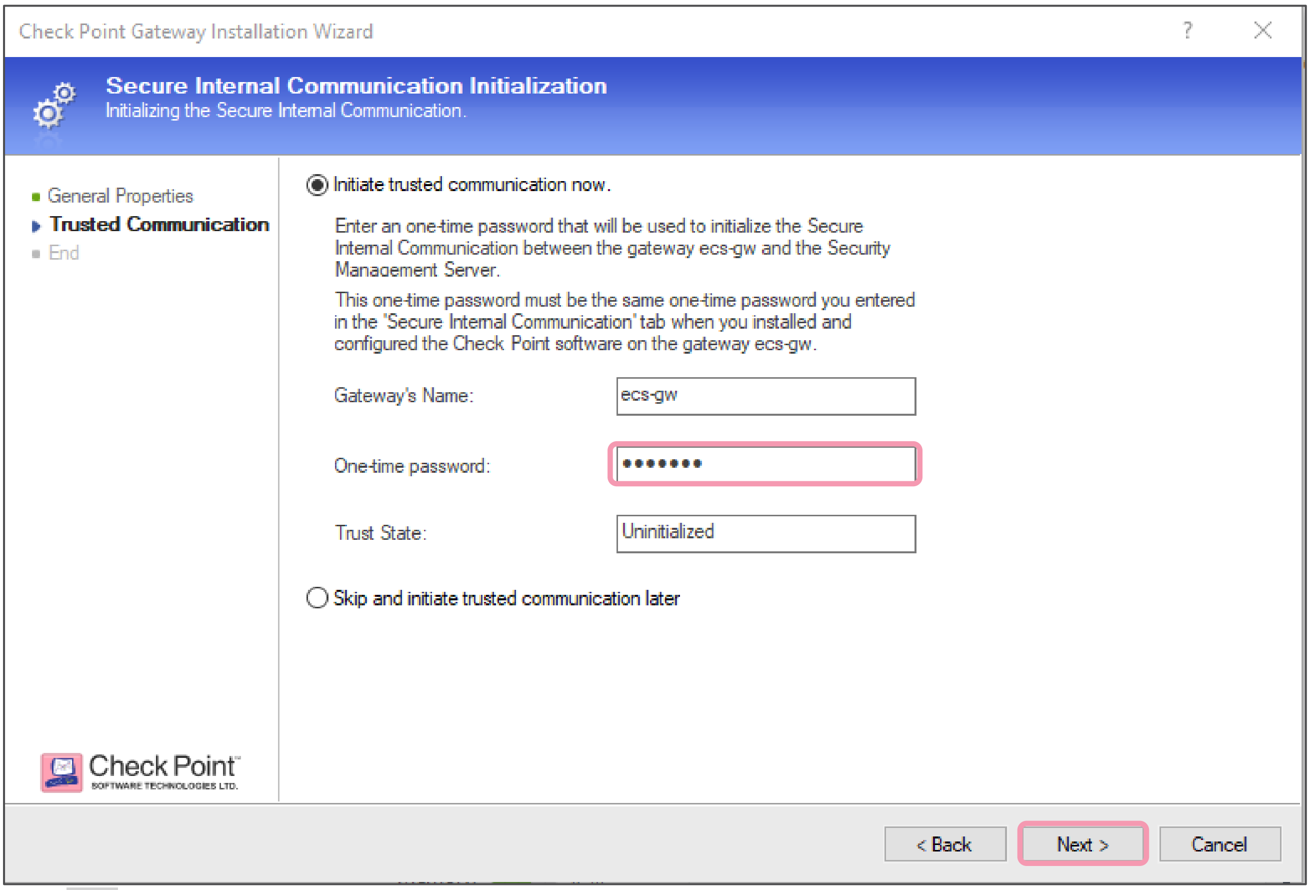
● Static IP address:

IPv4: 90 . 84 . 177 . 71

IPv6:

○ Dynamic IP address (e.g. assigned by DHCP server)

Type SIC (Secure Internal Communication) One-time password created during Security Gateway wizard phase to create the trust between Management Server and Security Gateway.



Check Point Gateway Installation Wizard

Secure Internal Communication Initialization
Initializing the Secure Internal Communication.

- General Properties
- Trusted Communication
- End

● Initiate trusted communication now.

Enter an one-time password that will be used to initialize the Secure Internal Communication between the gateway ecs-gw and the Security Management Server.

This one-time password must be the same one-time password you entered in the 'Secure Internal Communication' tab when you installed and configured the Check Point software on the gateway ecs-gw.

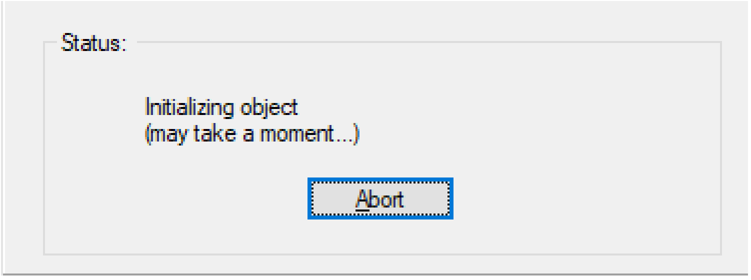
Gateway's Name: ecs-gw

One-time password: •••••••

Trust State: Uninitialized

○ Skip and initiate trusted communication later

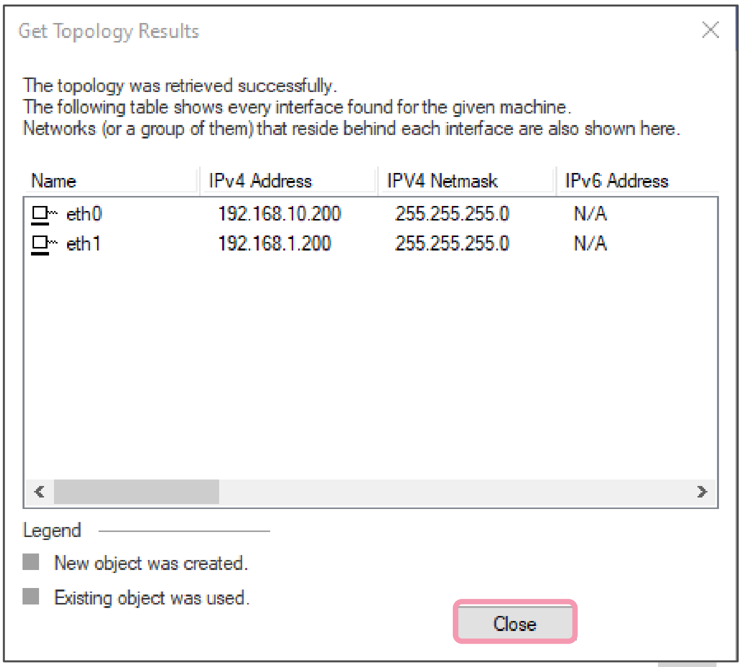
Click Next button.



Status:

Initializing object
(may take a moment...)

Wait few seconds until process complete.



Get Topology Results

The topology was retrieved successfully.
The following table shows every interface found for the given machine.
Networks (or a group of them) that reside behind each interface are also shown here.

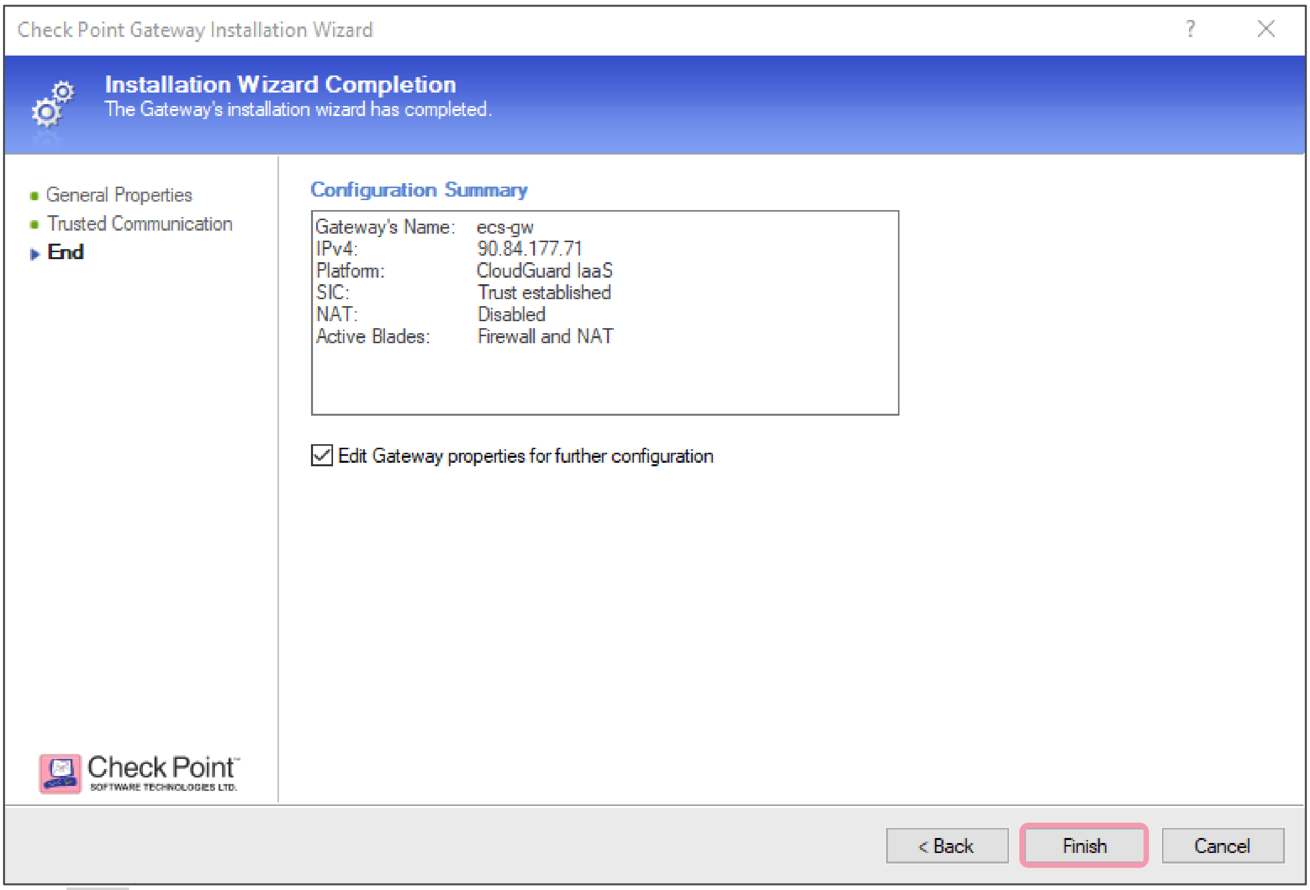
Name	IPv4 Address	IPV4 Netmask	IPv6 Address
eth0	192.168.10.200	255.255.255.0	N/A
eth1	192.168.1.200	255.255.255.0	N/A

Legend

▨ New object was created.

▨ Existing object was used.

Once complete, you will obtain the Security Gateway network topology. Click Close button.



Check Point Gateway Installation Wizard

Installation Wizard Completion
The Gateway's installation wizard has completed.

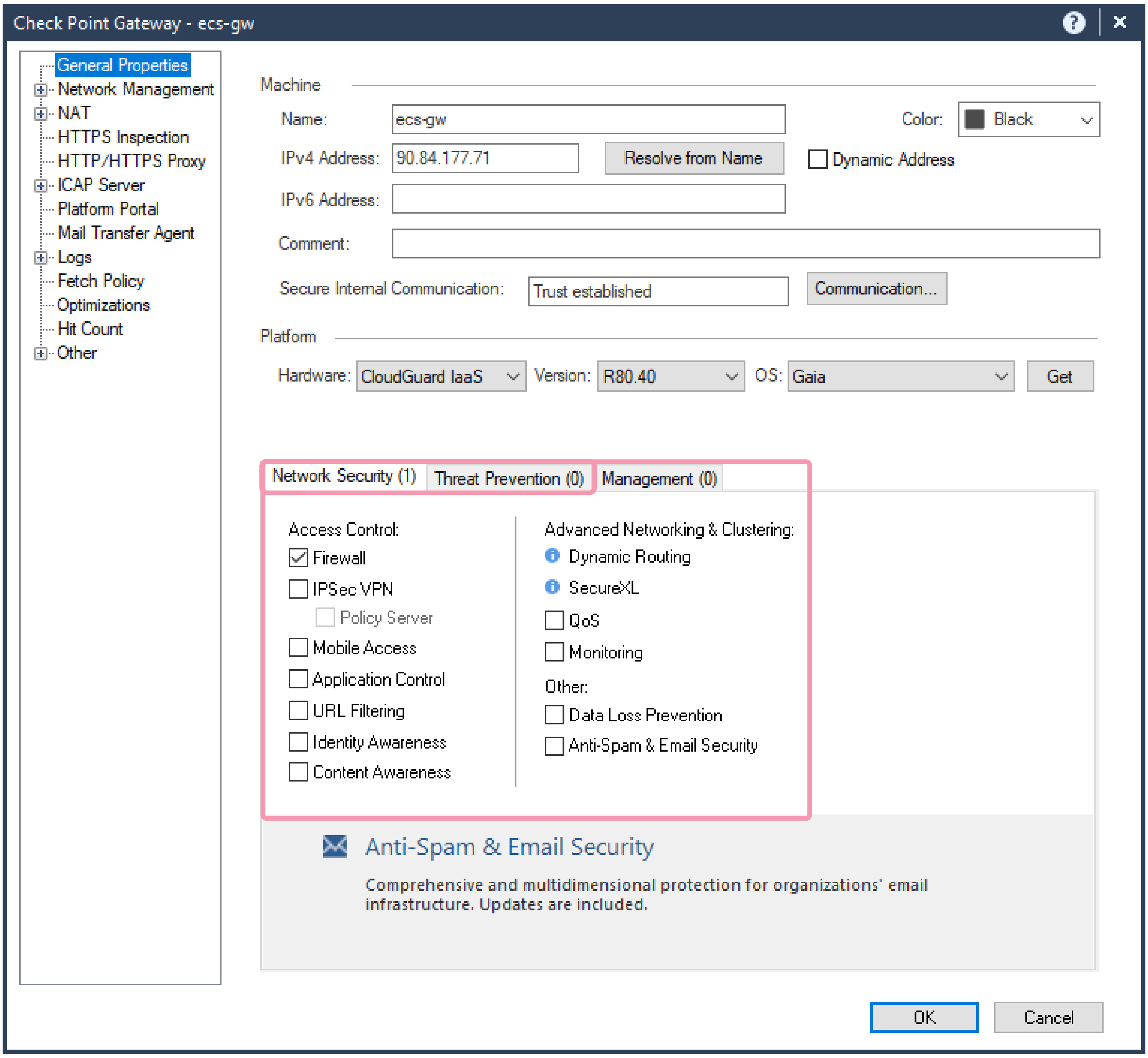
Configuration Summary

Gateway's Name:	ecs-gw
IPv4:	90.84.177.71
Platform:	CloudGuard IaaS
SIC:	Trust established
NAT:	Disabled
Active Blades:	Firewall and NAT

☑ Edit Gateway properties for further configuration

Click Finish button.

Configure the Network Security and Threat Prevention Blades you are willing to use (by example, Application Control, IPS, Antivirus, Anti-Bot,...)



Check Point Gateway - ecs-gw

Machine

Name: ecs-gw

Color: Black

IPv4 Address: 90.84.177.71 Resolve from Name □ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established Communication...

Platform

Hardware: CloudGuard IaaS Version: R80.40 OS: Gaia Get

Network Security (1) | Threat Prevention (0) | Management (0)

Access Control:
- ☑ Firewall
- □ IPSec VPN
- □ Policy Server
- □ Mobile Access
- □ Application Control
- □ URL Filtering
- □ Identity Awareness
- □ Content Awareness

Advanced Networking & Clustering:
- ● Dynamic Routing
- ● SecureXL
- □ QoS
- □ Monitoring

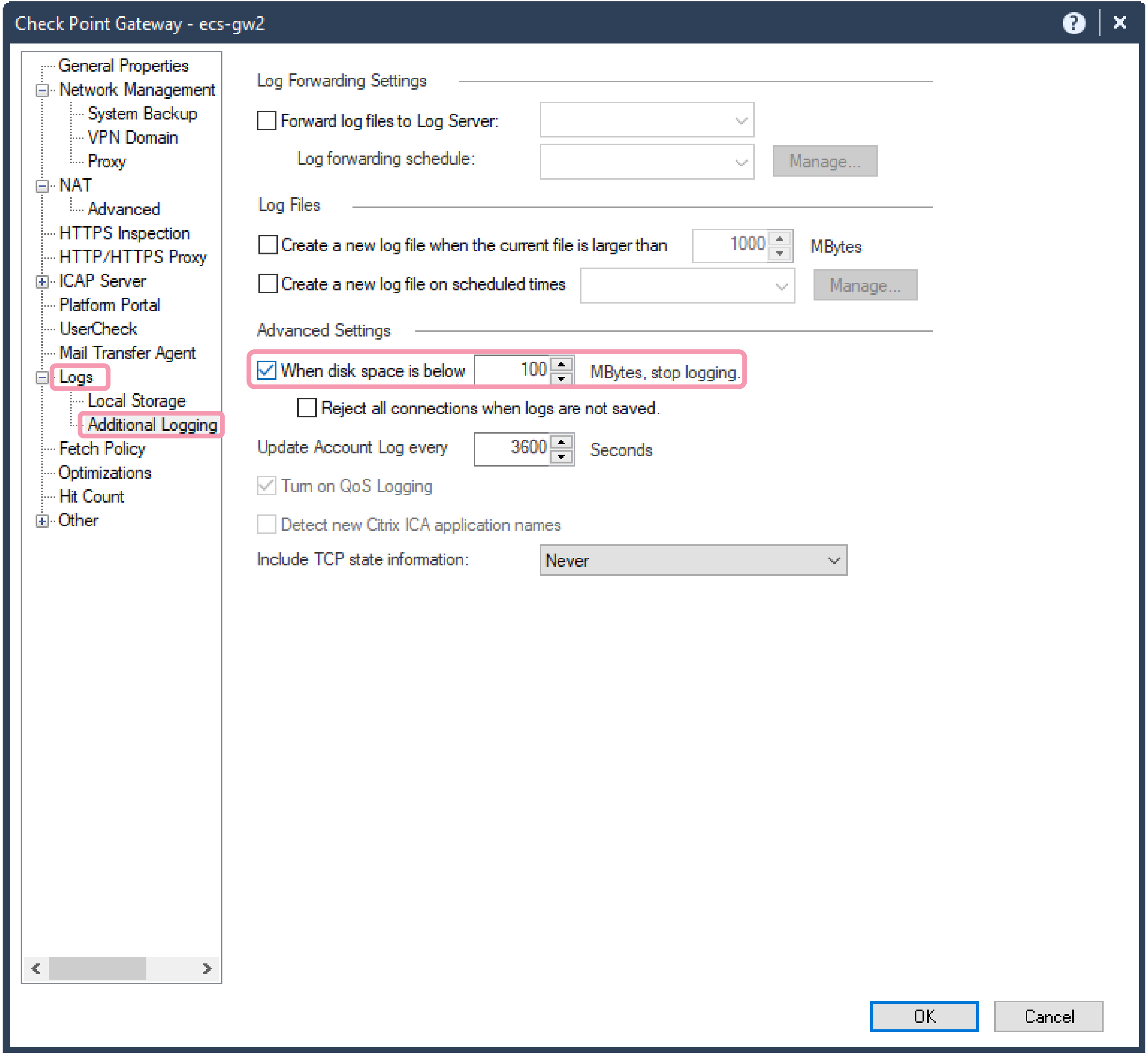
Other:
- □ Data Loss Prevention
- □ Anti-Spam & Email Security

Anti-Spam & Email Security

Comprehensive and multidimensional protection for organizations' email infrastructure. Updates are included.

As best practices, you can change the following parameters to your security gateway.

Please go to Logs → Additional Logging menu and select When disk space is below 100 Mbytes, stop logging. option. In case very long no connectivity from Gateway to Management Server / Log Server, local logging will not impact production.



Check Point Gateway - ecs-gw2

Log Forwarding Settings

□ Forward log files to Log Server:

Log forwarding schedule:

Log Files

□ Create a new log file when the current file is larger than 1000 MBytes

□ Create a new log file on scheduled times

Advanced Settings

☑ When disk space is below 100 MBytes, stop logging.

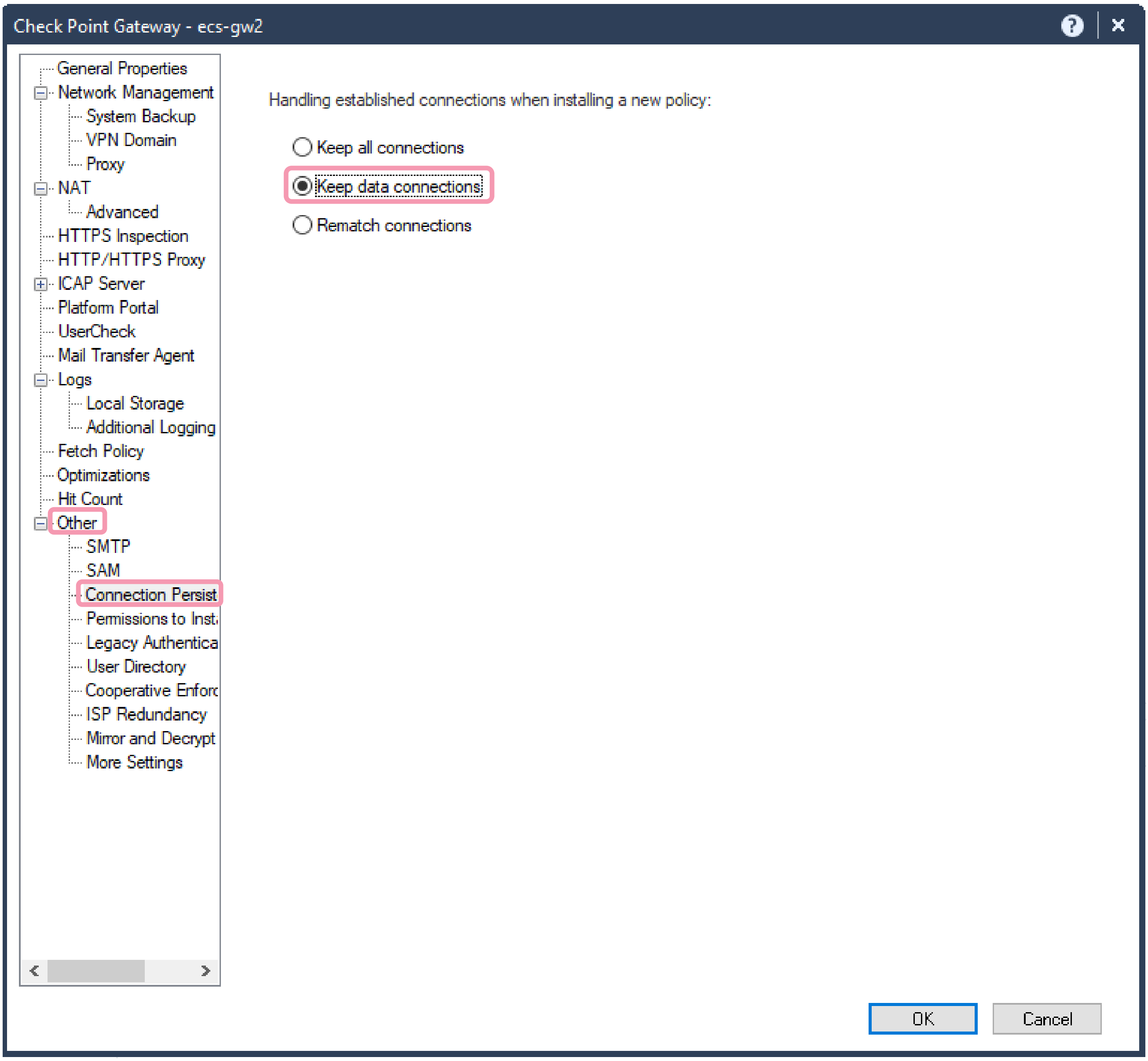
□ Reject all connections when logs are not saved.

Update Account Log every 3600 Seconds

☑ Turn on QoS Logging

□ Detect new Citrix ICA application names

Include TCP state information: Never



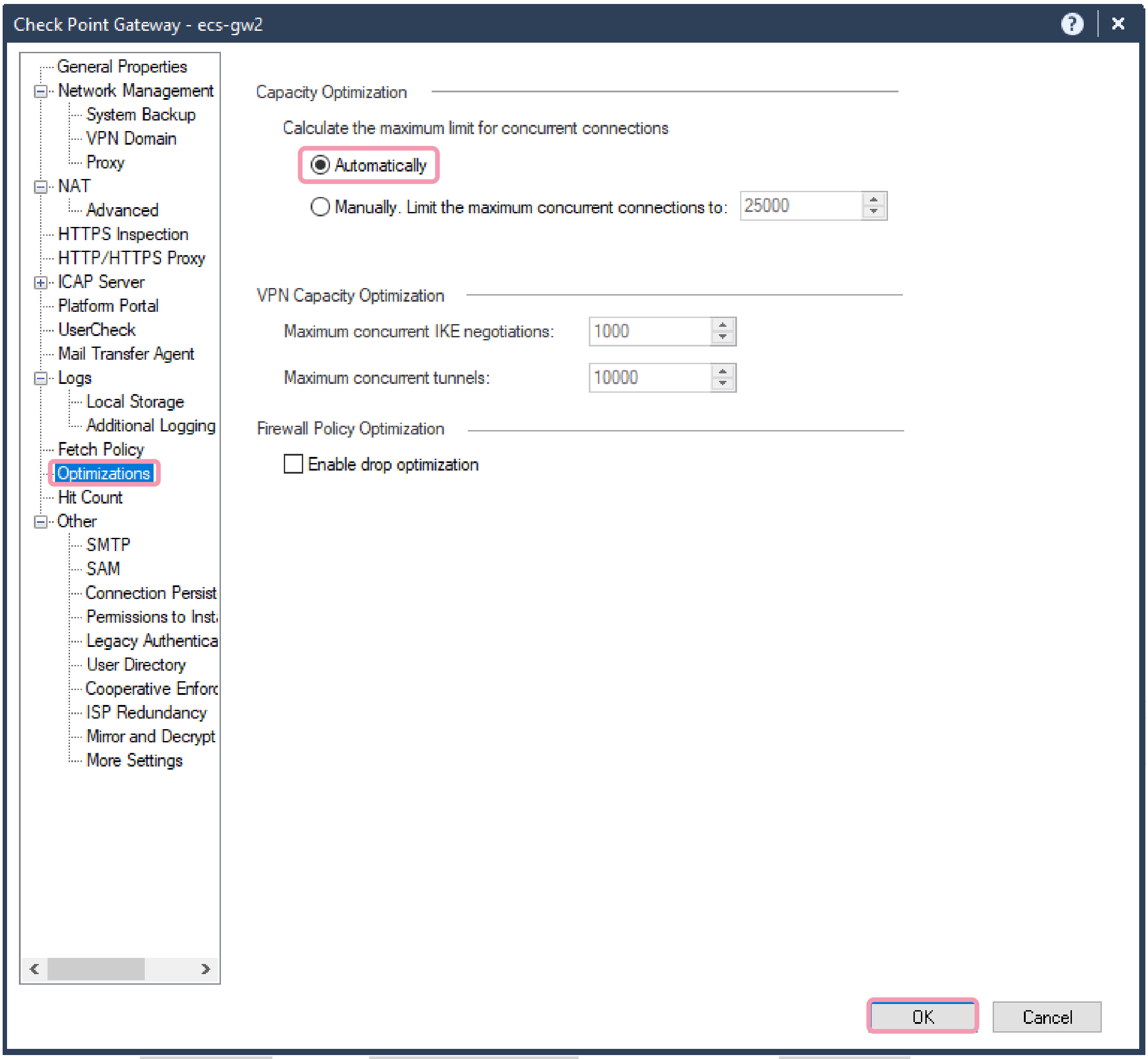
Handling established connections when installing a new policy:

○ Keep all connections

● Keep data connections

○ Rematch connections

Please go to Other → Connection Persistency menu and select Keep data connections option. In case of policy push, data connections will be not be rematch after new policy push avoiding cut in on-going data traffic previously authorized but new traffic only.



Capacity Optimization

Calculate the maximum limit for concurrent connections

● Automatically

○ Manually. Limit the maximum concurrent connections to: 25000

VPN Capacity Optimization

Maximum concurrent IKE negotiations: 1000

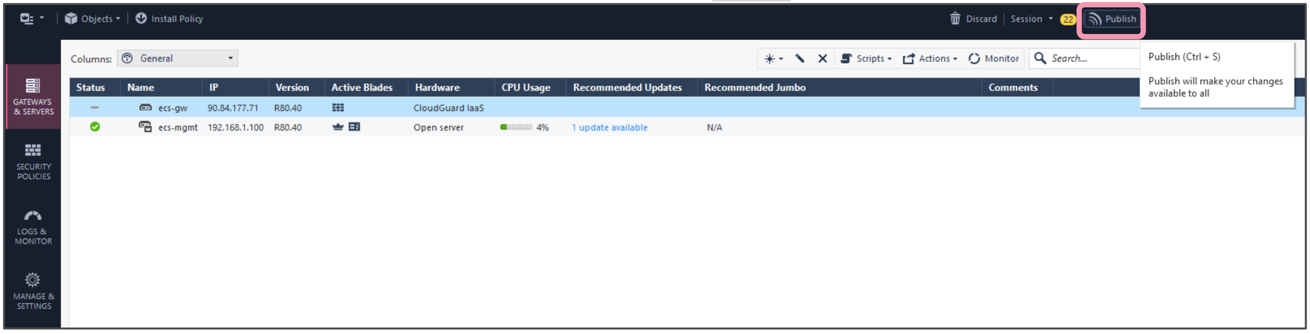
Maximum concurrent tunnels: 10000

Firewall Policy Optimization

□ Enable drop optimization

Please go to Optimizations menu in Capacity Optimization section and select Automatically option to calculate the maximum limit for concurrent connections. Click OK button to finalize the gateway object configuration.

Once all necessary changes are done, please make sure to Publish them to the Management Server.



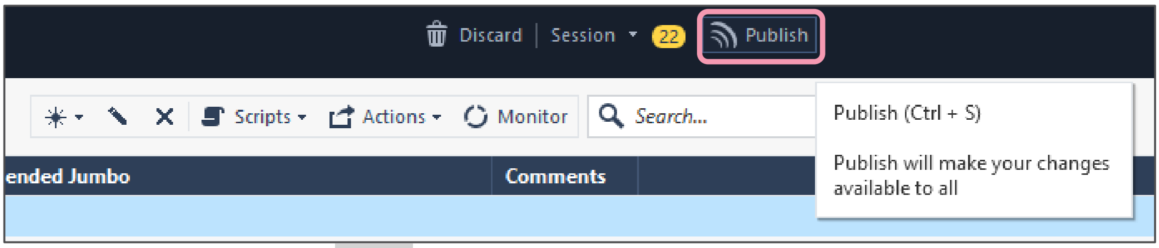
Columns: General

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo	Comments
–	ecs-gw	90.84.177.71	R80.40		CloudGuard IaaS				
✓	ecs-mgmt	192.168.1.100	R80.40		Open server	4%	1 update available	N/A	

Publish (Ctrl + S)

Publish will make your changes available to all

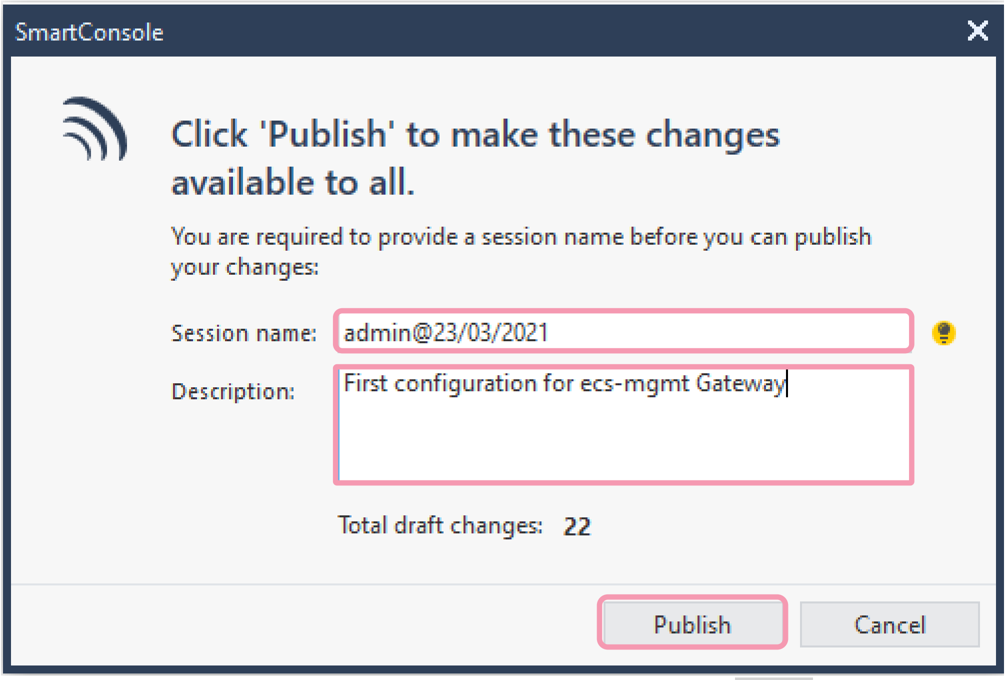
Zoomed view



Publish (Ctrl + S)

Publish will make your changes available to all

Click Publish top right button on SmartConsole client.



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

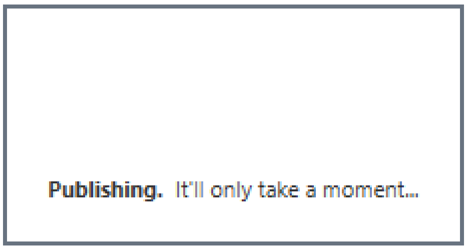
You are required to provide a session name before you can publish your changes:

Session name: admin@23/03/2021

Description: First configuration for ecs-mgmt Gateway

Total draft changes: 22

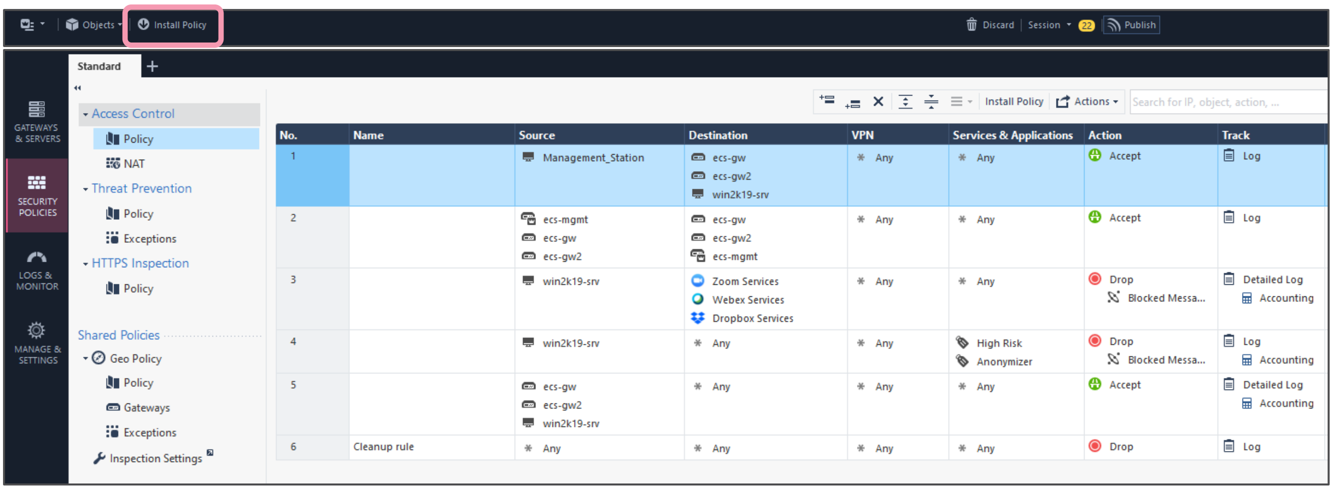
Indicates a Session Name and Description then click Publish button.



Publishing. It'll only take a moment...

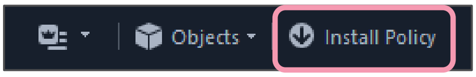
Wait few seconds to make it effective.

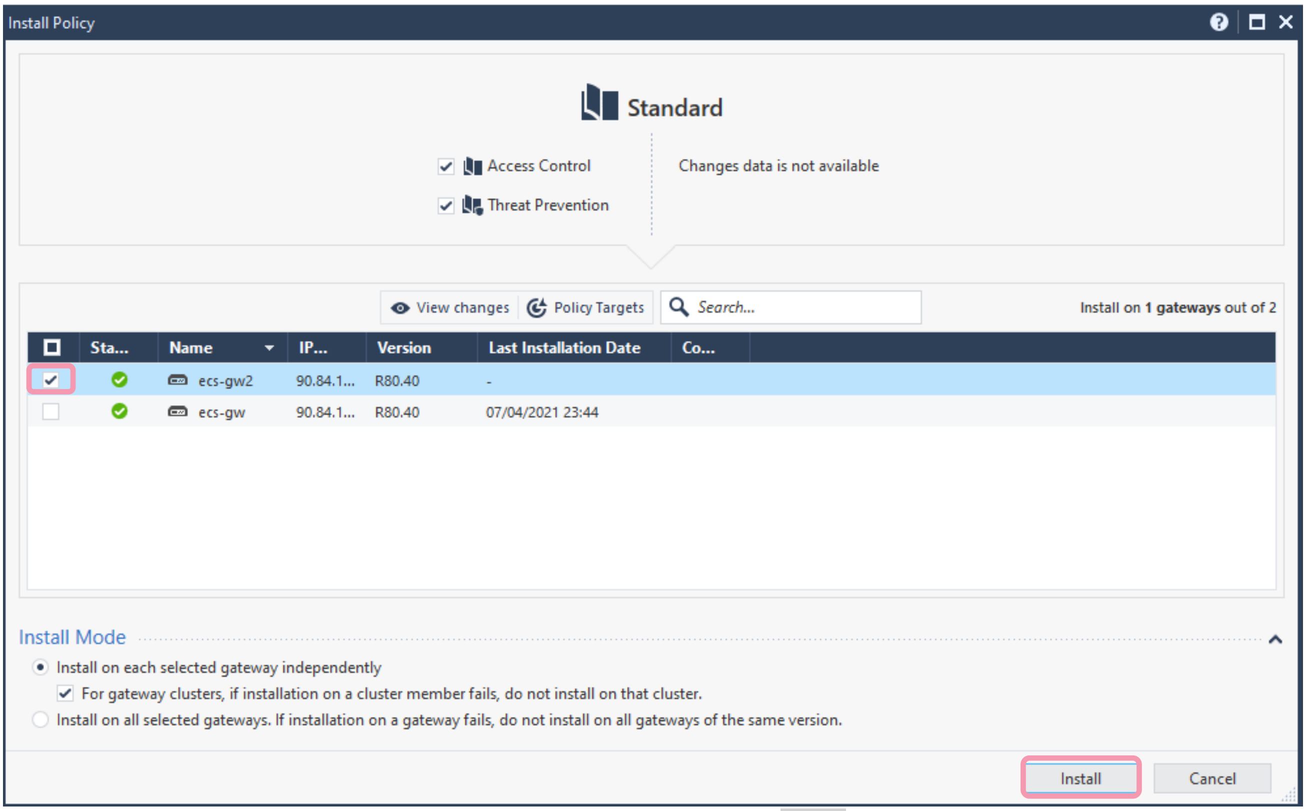
Prepare a Security Policy you will push to the Security Gateway. Click Install Policy top left button on SmartConsole.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1		Management_Station	ecs-gw ecs-gw2 win2k19-srv	Any	Any	Accept	Log
2		ecs-mgmt ecs-gw ecs-gw2	ecs-gw ecs-gw2 ecs-mgmt	Any	Any	Accept	Log
3		win2k19-srv	Zoom Services Webex Services Dropbox Services	Any	Any	Drop Blocked Messa...	Detailed Log Accounting
4		win2k19-srv	Any	Any	High Risk Anonymizer	Drop Blocked Messa...	Log Accounting
5		ecs-gw ecs-gw2 win2k19-srv	Any	Any	Any	Accept	Detailed Log Accounting
6	Cleanup rule	Any	Any	Any	Any	Drop	Log

Zoomed view





Install Policy

Standard

☑ Access Control
☑ Threat Prevention

Changes data is not available

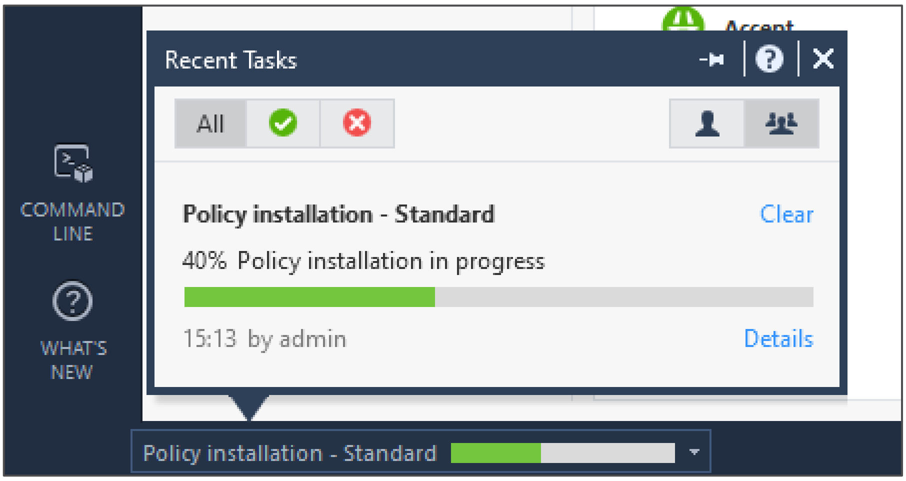
Install on 1 gateways out of 2

☐	Sta...	Name	IP...	Version	Last Installation Date	Co...
☑	✓	ecs-gw2	90.84.1...	R80.40	-	
☐	✓	ecs-gw	90.84.1...	R80.40	07/04/2021 23:44	

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.

Select the target Security Gateway for policy installation and click Install button.
Then wait a moment until policy installation is complete.



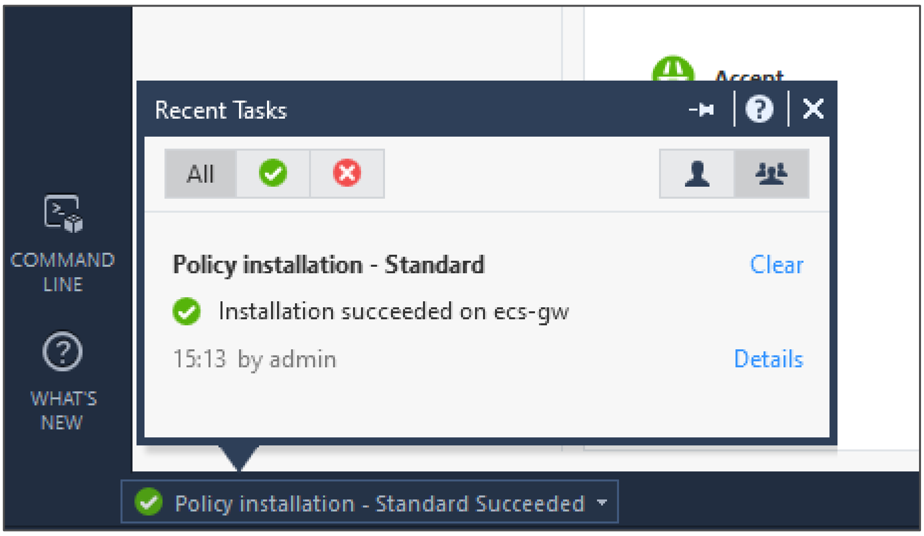
Recent Tasks

Policy installation - Standard

40% Policy installation in progress

15:13 by admin

Policy installation - Standard



Recent Tasks

Policy installation - Standard

Installation succeeded on ecs-gw

15:13 by admin

Policy installation - Standard Succeeded

GATEWAY LICENSING

A security gateway comes with 15 days embedded evaluation licenses to leave you time to install definitive license (process described at next page). The below information give you all you need to know about Cloudguard Network Security licensing model.

Description
CloudGuard Network Security Gateway provides advanced threat prevention and automated cloud network security through a virtual security gateway, with unified security management across all your public cloud and private cloud environments

Service Specifications
Includes Advance threat preventions – IPS, Identity Awareness, App Control, Anti-Virus, Anti-Bot, URL Filtering, VPN, threat emulation*, and threat extraction*, Zero-Day* and ThreatCloud.
*with NGTX subscription.

References
CloudGuard Network is licensed by the number of virtual cores (vCores) assigned to the virtual machine running it. The license supports CloudGuard Network gateways running on a wide variety of public and private cloud vendors.

- NGTP SKU: CPSG-VSEC-NSX-BUN-NGTP-XY where X is the number of years of services
- NGTX SKU: CPSG-VSEC-NSX-BUN-NGTX-XY where X is the number of years of services

Example:

- 1 x CPSG-VSEC-NSX-BUN-NGTP-3Y = 1 x CloudGuard Network virtual core for VMware ESXi, Hyper-V, KVM Gateway. Annual subscription for 3 years.

Licensing instructions for CloudGuard Network Security:

- CloudGuard Network Gateway is licensed by the number of virtual cores (vCores) assigned to the virtual machine running it.
- The License supports CloudGuard Network Gateways running on public and private cloud.
- Public Cloud: Amazon Web Services (AWS); Microsoft Azure; Google Cloud; Oracle Cloud Infrastructure; Alibaba Cloud; IBM cloud; Huawei; Yandex; and more.
- Private Cloud / SDN: VMware - Esxi; VMware – NSX; Nutanix.
- Check Point CloudGuard Network Gateway license is pool based (sk109713):
- You can add additional licenses to the pool
- The license pool is deployed on Check Point management server and will be automatically assigned to CloudGuard Network Security gateways

Renewal:

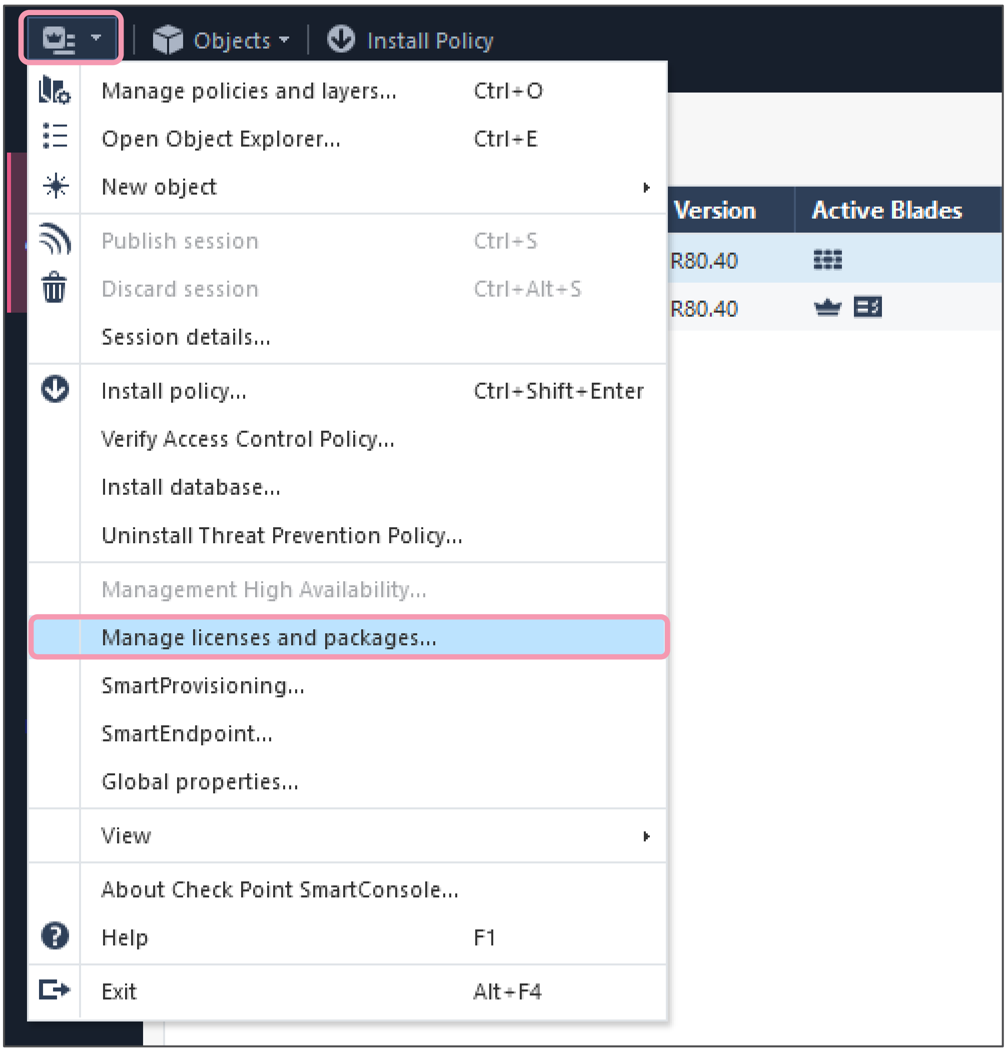
- The renewal subscription license should match the number of vCores in the subscription license

More licensing data:

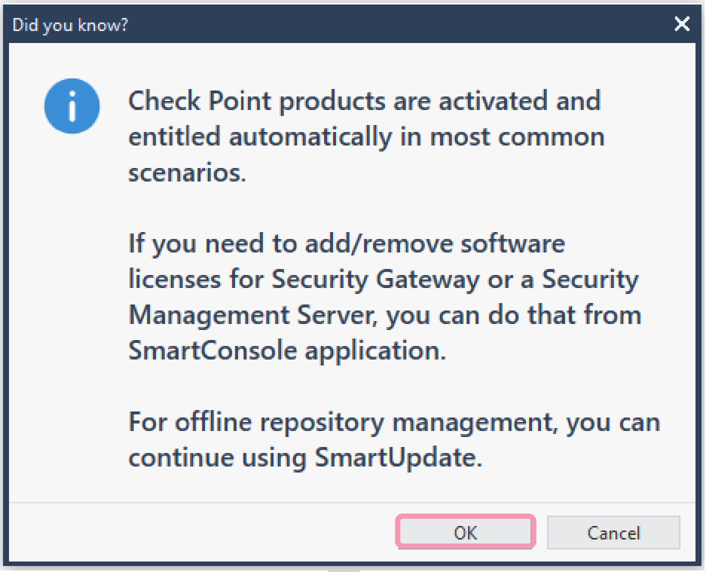
- Customer can purchase addition software blades and deploy them on specific CloudGuard Network Gateways
- Multi-Domain-Management (MDM) - every license pool should be issued with the CMA IP and will be attached to the CloudGuard Network Security gateways which are managed by that CMA
- NGTX cloud inspection quota is 10 000 files/vCore/month

Note: Please make sure to update your Service Contract on your management following the integration of new Security Gateway.

- What is a Service Contract File?
- Download Contract File


Objects
Install Policy
Manage policies and layers... Ctrl+O
Open Object Explorer... Ctrl+E
New object
Publish session Ctrl+S
Discard session Ctrl+Alt+S
Session details...
Install policy... Ctrl+Shift+Enter
Verify Access Control Policy...
Install database...
Uninstall Threat Prevention Policy...
Management High Availability...
Manage licenses and packages...
SmartProvisioning...
SmartEndpoint...
Global properties...
View
About Check Point SmartConsole...
Help F1
Exit Alt+F4
Version
Active Blades
R80.40
R80.40

To install definitive license on your Security Gateway instance, please connect to your Management Server using SmartConsole client. Go to menu → Manage licenses and packages…

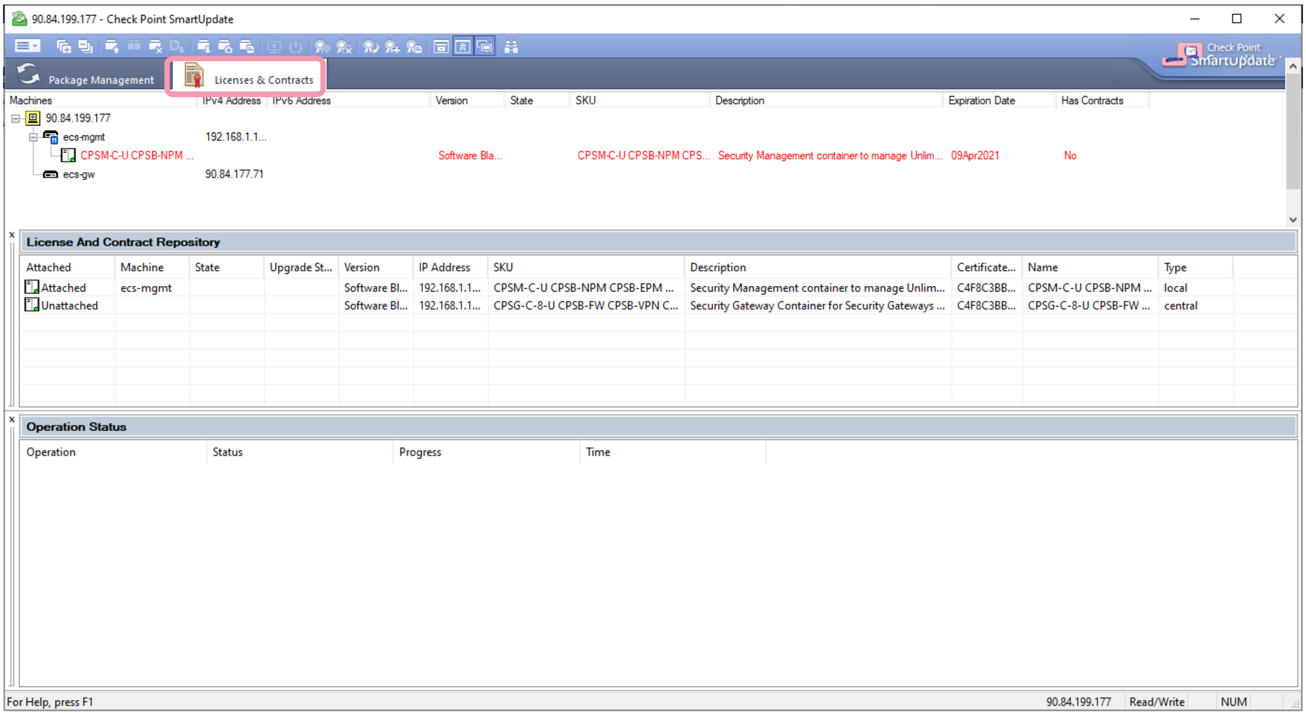

Did you know?

Check Point products are activated and entitled automatically in most common scenarios.

If you need to add/remove software licenses for Security Gateway or a Security Management Server, you can do that from SmartConsole application.

For offline repository management, you can continue using SmartUpdate.

Click OK button



90.84.199.177 - Check Point SmartUpdate

Machines	IPv4 Address	IPv6 Address	Version	State	SKU	Description	Expiration Date	Has Contracts
90.84.199.177								
ecs-mgmt	192.168.1.1...							
CPSM-C-U CPSB-NPM ...			Software Bla...		CPSM-C-U CPSB-NPM CPS...	Security Management container to manage Unlim...	09Apr2021	No
ecs-gw	90.84.177.71							

License And Contract Repository

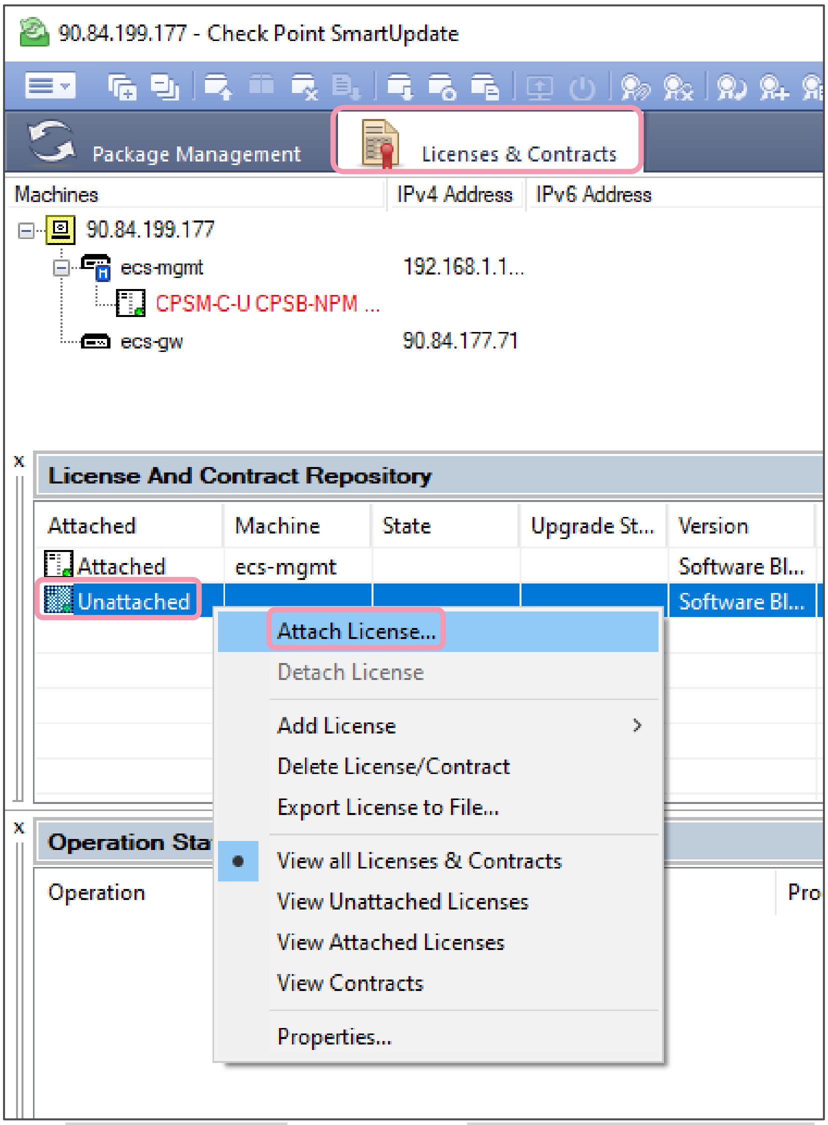
Attached	Machine	State	Upgrade St...	Version	IP Address	SKU	Description	Certificate...	Name	Type
Attached	ecs-mgmt			Software Bl...	192.168.1.1...	CPSM-C-U CPSB-NPM CPSB-EPM ...	Security Management container to manage Unlim...	C4F8C3BB...	CPSM-C-U CPSB-NPM ...	local
Unattached				Software Bl...	192.168.1.1...	CPSG-C-8-U CPSB-FW CPSB-VPN C...	Security Gateway Container for Security Gateways ...	C4F8C3BB...	CPSG-C-8-U CPSB-FW ...	central

Operation Status

Operation	Status	Progress	Time

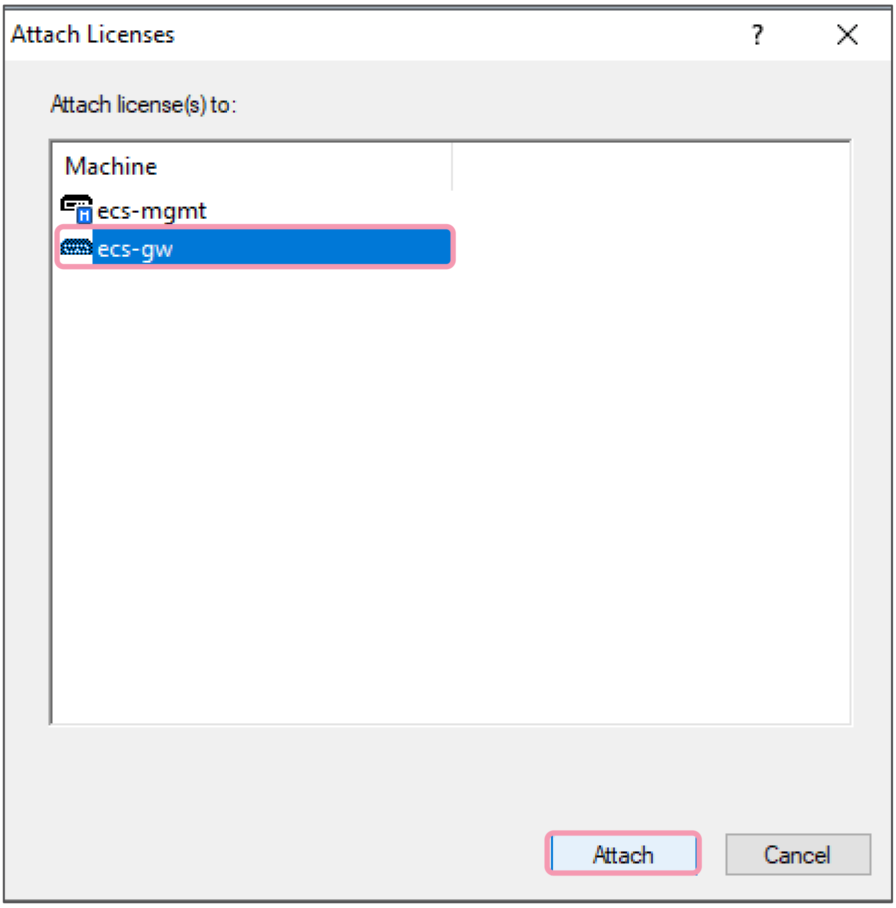
For Help, press F1 90.84.199.177 Read/Write NUM

Zoomed view



90.84.199.177 - Check Point SmartUpdate

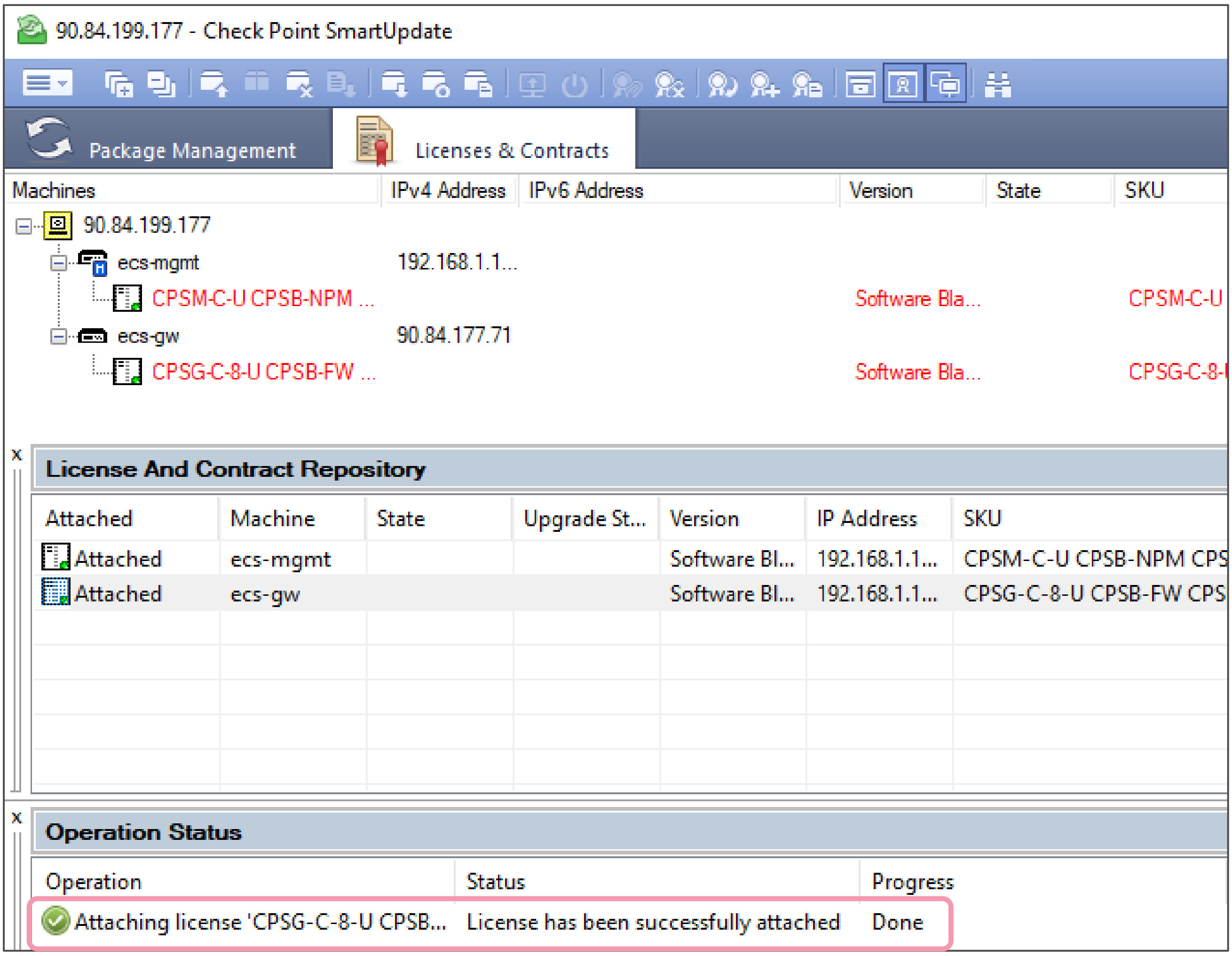
Click Licenses & Contracts tab, then go to License And Contract Repository section. Select the proper Unattached license, right click on it then select Attach License... contextual menu.



Attach Licenses

Attach license(s) to:

Machine
ecs-mgmt
ecs-gw



90.84.199.177 - Check Point SmartUpdate

Machines	IPv4 Address	IPv6 Address	Version	State	SKU
90.84.199.177					
ecs-mgmt	192.168.1.1...				
CPSM-C-U CPSB-NPM ...			Software Bla...		CPSM-C-U
ecs-gw	90.84.177.71				
CPSG-C-8-U CPSB-FW ...			Software Bla...		CPSG-C-8-

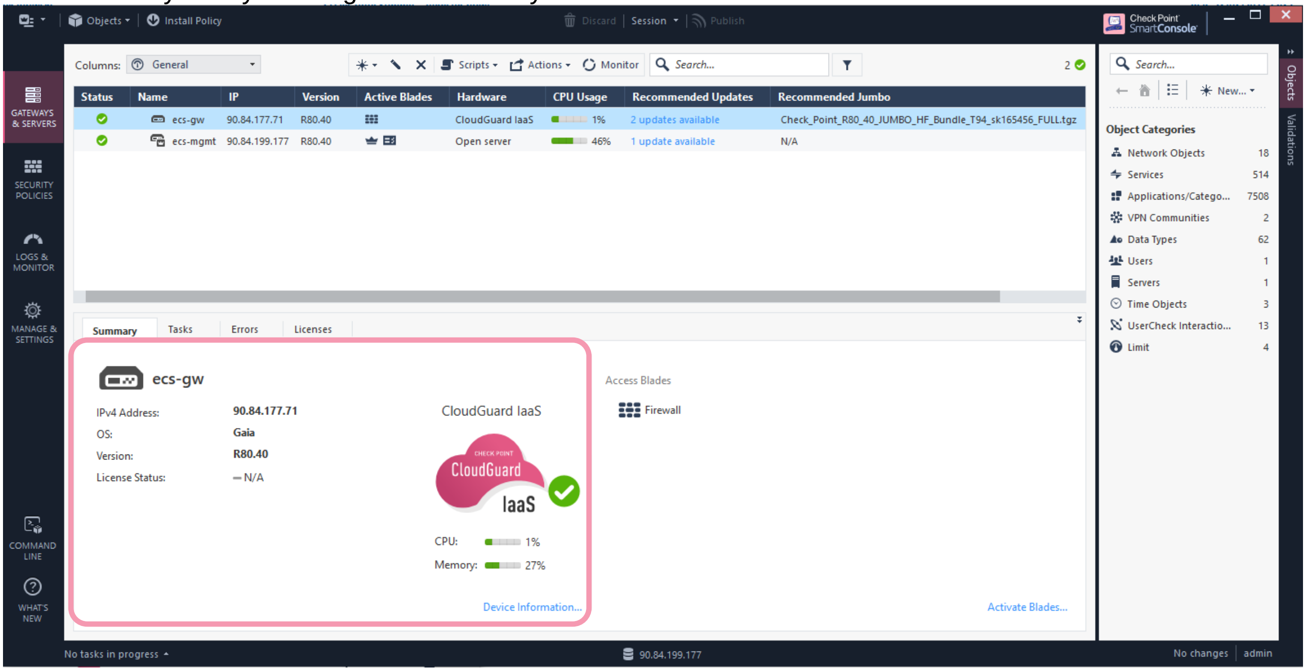
License And Contract Repository

Attached	Machine	State	Upgrade St...	Version	IP Address	SKU
Attached	ecs-mgmt			Software Bl...	192.168.1.1...	CPSM-C-U CPSB-NPM CPS
Attached	ecs-gw			Software Bl...	192.168.1.1...	CPSG-C-8-U CPSB-FW CPS

Operation Status

Operation	Status	Progress
Attaching license 'CPSG-C-8-U CPSB...	License has been successfully attached	Done

Install Security Policy once again and check your instance status as below.



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo
✓	ecs-gw	90.84.177.71	R80.40		CloudGuard IaaS	1%	2 updates available	Check_Point_R80_40_JUMBO_HF_Bundle_T94_sk165456_FULL.tgz
✓	ecs-mgmt	90.84.199.177	R80.40		Open server	46%	1 update available	N/A

ecs-gw

IPv4 Address:	90.84.177.71
OS:	Gaia
Version:	R80.40
License Status:	— N/A

CloudGuard IaaS

CPU: 1%

Memory: 27%

Device Information...

Access Blades

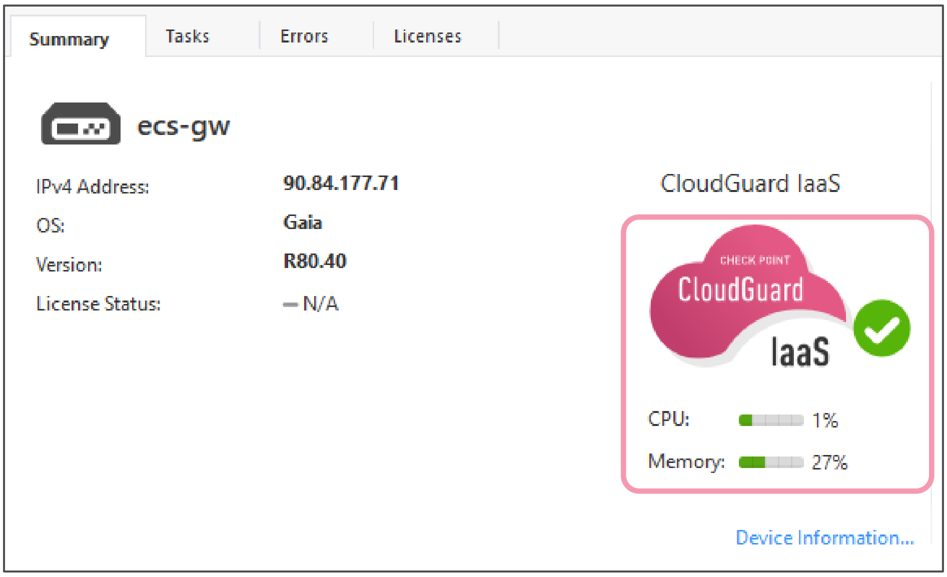
Firewall

Activate Blades...

Object Categories

Network Objects	18
Services	514
Applications/Catego...	7508
VPN Communities	2
Data Types	62
Users	1
Servers	1
Time Objects	3
UserCheck Interactio...	13
Limit	4

Zoomed view



ecs-gw

IPv4 Address:	90.84.177.71
OS:	Gaia
Version:	R80.40
License Status:	— N/A

CloudGuard IaaS

CPU: 1%

Memory: 27%

Device Information...

POST INSTALLATION OPERATIONS & JUMBO HOTFIX UPDATE

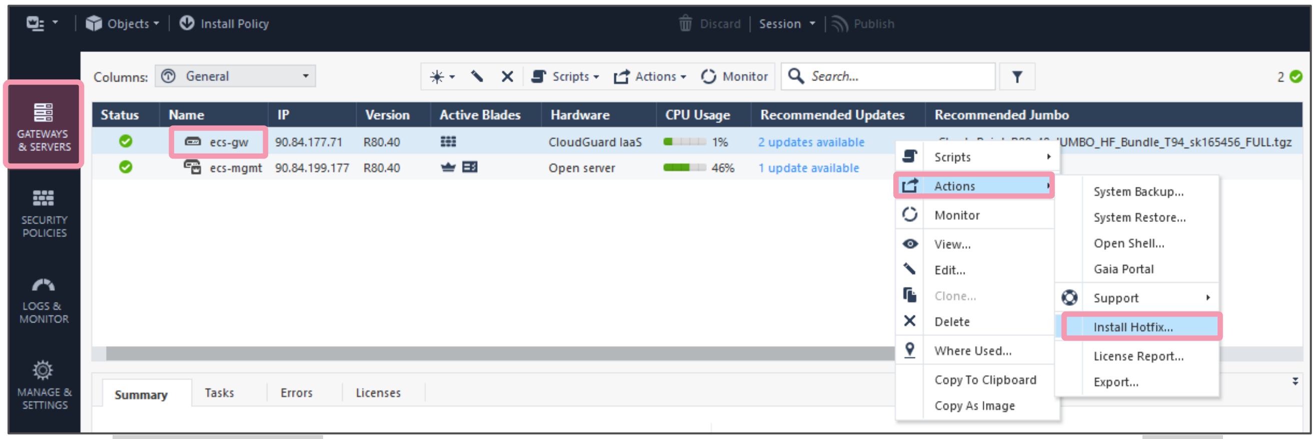
Once definitive license has been applied to the Security Gateway, you'll be able to update to the latest General Availability Jumbo Hotfix that is mandatory to apply after first installation and most recommended to apply every time a new GA release is available.

As reminder, Supported Version is R80.40 GA Take 294 plus Jumbo HF Take_94 or above Jumbo HF GA releases.

File Name: **Check_Point_R80_40_JUMBO_HF_Bundle_T94_sk165456_FULL.tgz**
Release Date: **07-Mar-2021**

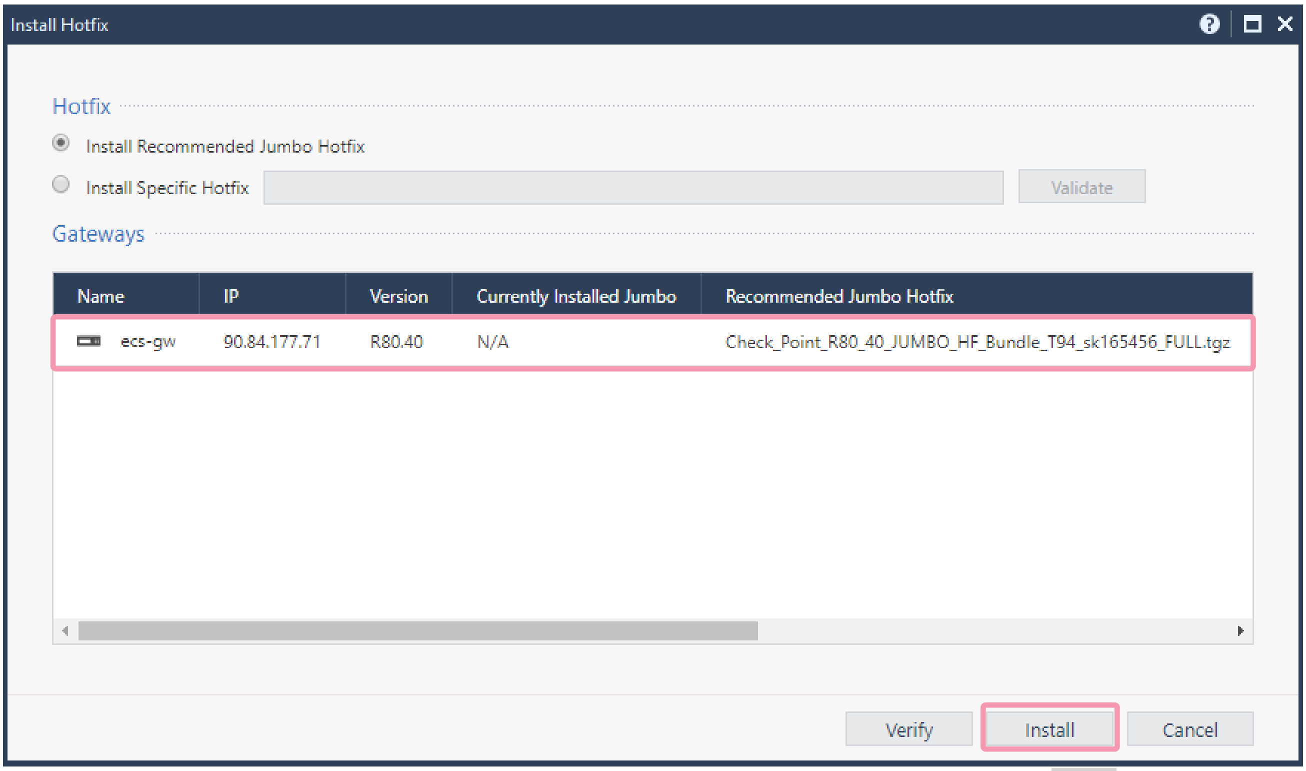
For more information about Jumbo Hotfix Accumulator for R80.40, please refer to solution ID: sk165456

To install Jumbo Hotfix on your Security Gateway, please connect to your Security Management Server using your SmartConsole to have a central deployment (or using Gaia WebUI directly on your Security Gateway).



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo
✓	ecs-gw	90.84.177.71	R80.40		CloudGuard IaaS	1%	2 updates available	UMBO_HF_Bundle_T94_sk165456_FULL.tgz
✓	ecs-mgmt	90.84.199.177	R80.40		Open server	46%	1 update available	

Click on Gateway & Servers tab. Click on the target Security Gateway then right click → select Actions → Install Hotfix... on contextual menu.



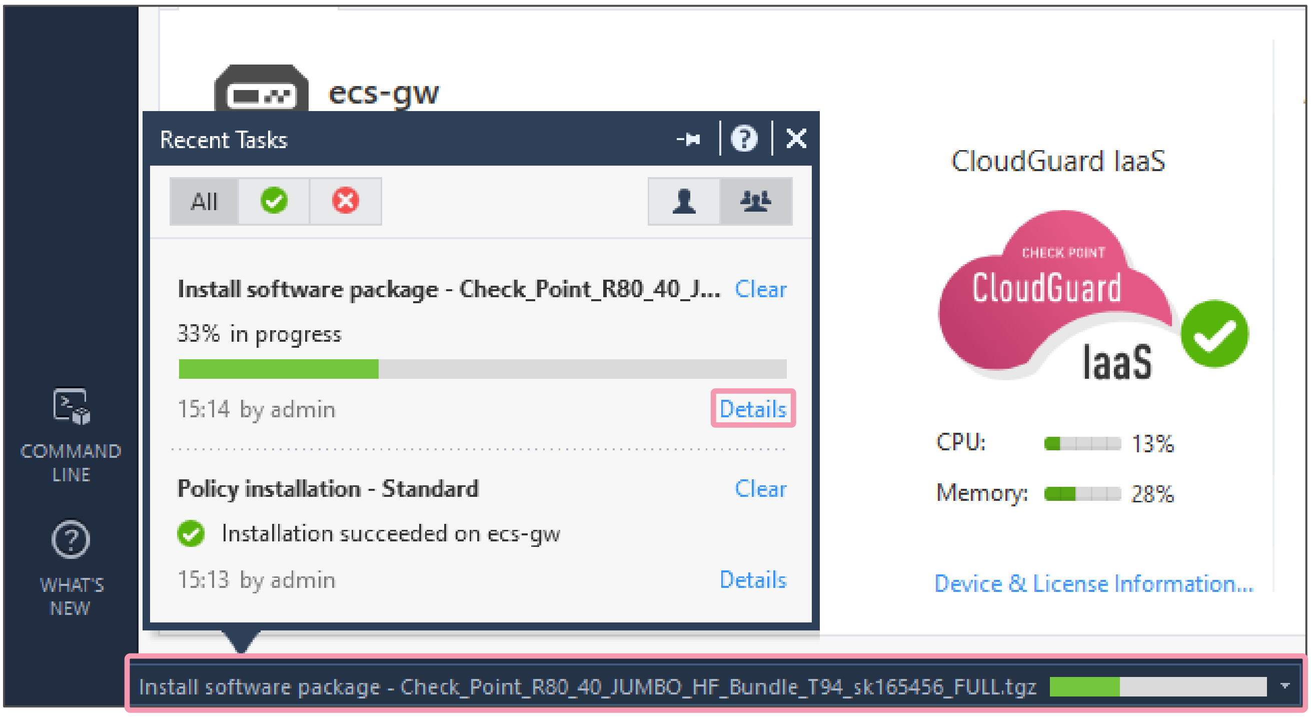
● Install Recommended Jumbo Hotfix

○ Install Specific Hotfix

Name	IP	Version	Currently Installed Jumbo	Recommended Jumbo Hotfix
ecs-gw	90.84.177.71	R80.40	N/A	Check_Point_R80_40_JUMBO_HF_Bundle_T94_sk165456_FULL.tgz

Select the target Security Gateway with target Recommended Jumbo Hotfix and click on Install button.

Zoomed view



ecs-gw

Recent Tasks

All

Install software package - Check_Point_R80_40_J... Clear

33% in progress

15:14 by admin Details

Policy installation - Standard Clear

✓ Installation succeeded on ecs-gw

15:13 by admin Details

COMMAND LINE

WHAT'S NEW

CloudGuard IaaS

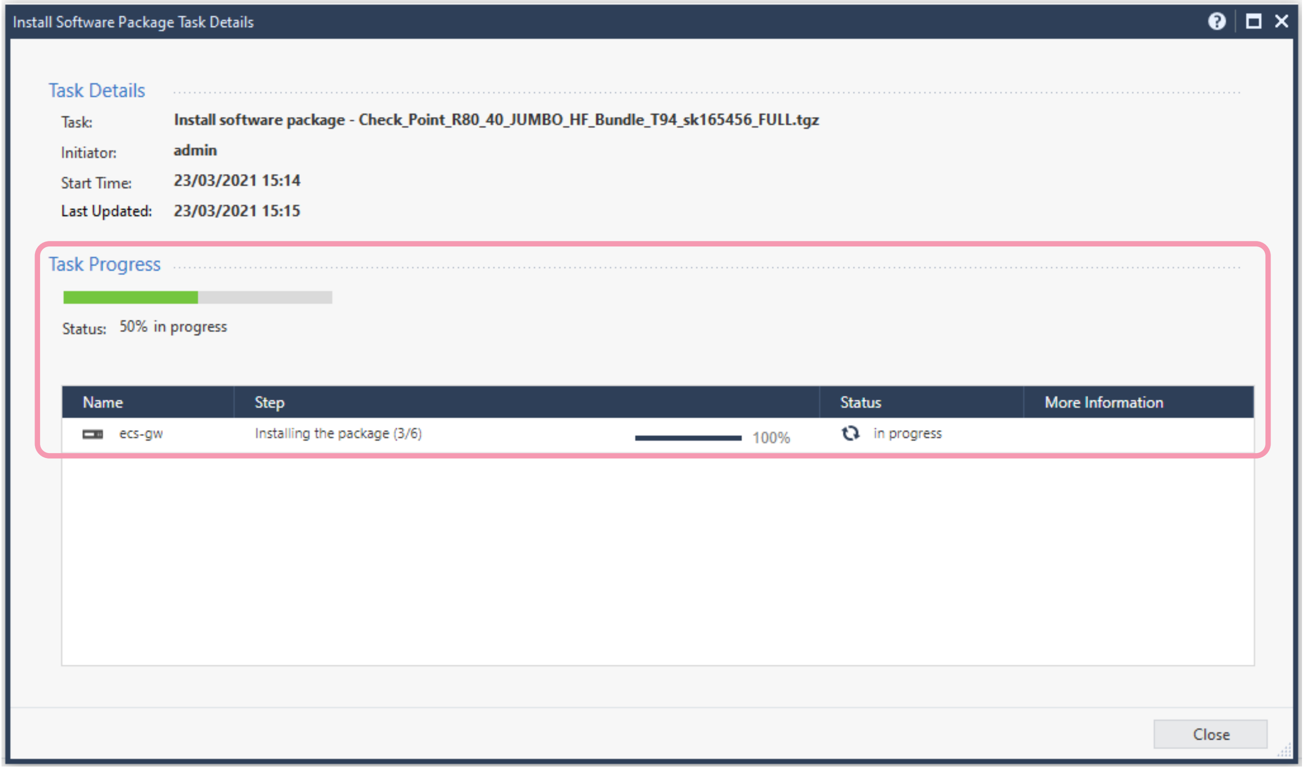
CPU: 13%

Memory: 28%

Device & License Information...

Install software package - Check_Point_R80_40_JUMBO_HF_Bundle_T94_sk165456_FULL.tgz

On bottom right of the SmartConsole client, click on the installation task to have more details about progress and full details (as below) clicking on Details button.



Install Software Package Task Details

Task Details

Task: Install software package - Check_Point_R80_40_JUMBO_HF_Bundle_T94_sk165456_FULL.tgz

Initiator: admin

Start Time: 23/03/2021 15:14

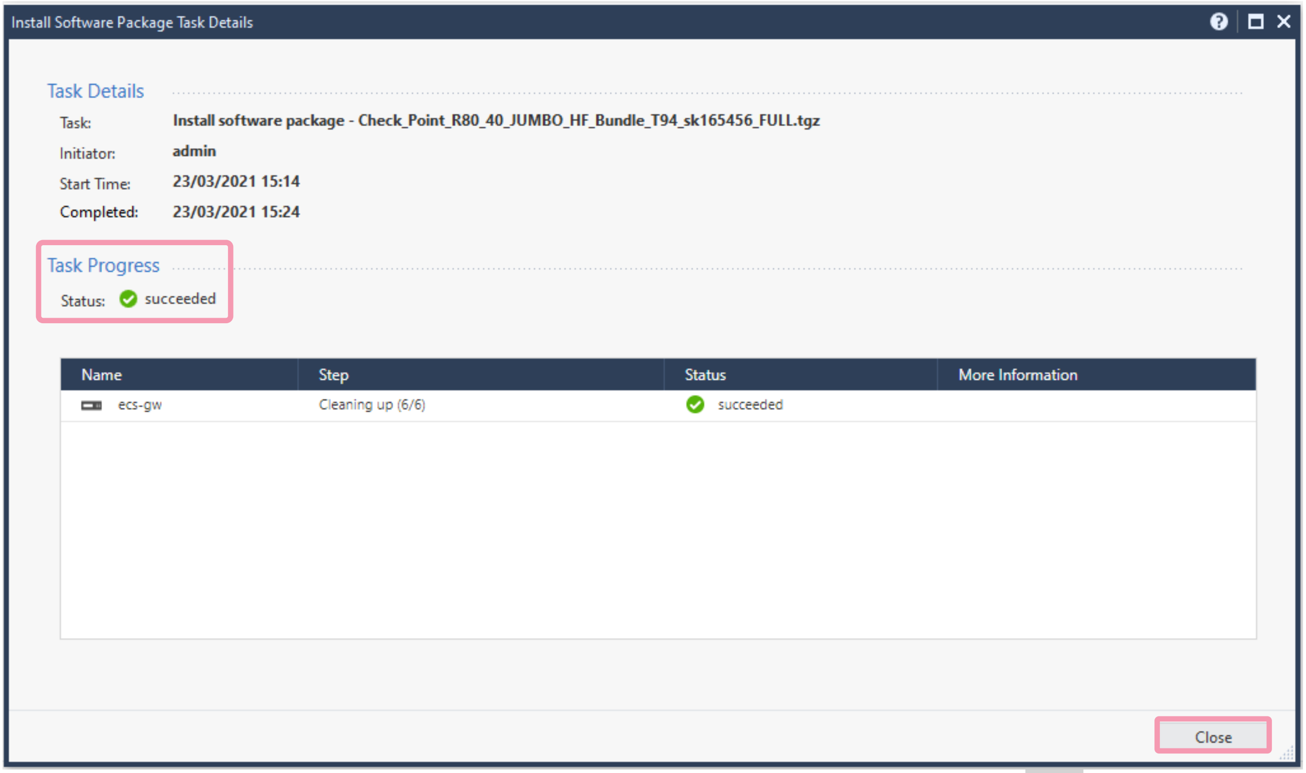
Last Updated: 23/03/2021 15:15

Task Progress

Status: 50% in progress

Name	Step	Status	More Information
ecs-gw	Installing the package (3/6) 100%	in progress	

Close



Install Software Package Task Details

Task Details

Task:	Install software package - Check_Point_R80_40_JUMBO_HF_Bundle_T94_sk165456_FULL.tgz
Initiator:	admin
Start Time:	23/03/2021 15:14
Completed:	23/03/2021 15:24

Task Progress

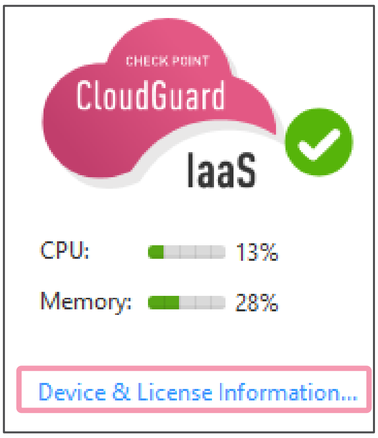
Status: ✓ succeeded

Name	Step	Status	More Information
ecs-gw	Cleaning up (6/6)	✓ succeeded	

Once finalized, succeed and you do not want check detailed status anymore, just click Close button.

MONITORING CHECKS

After Hotfix installation, you can check that Security Gateway instance is operating correctly using Monitoring view. To get access to that detailed information, click on Device & License Information... on the desired Security Gateway.

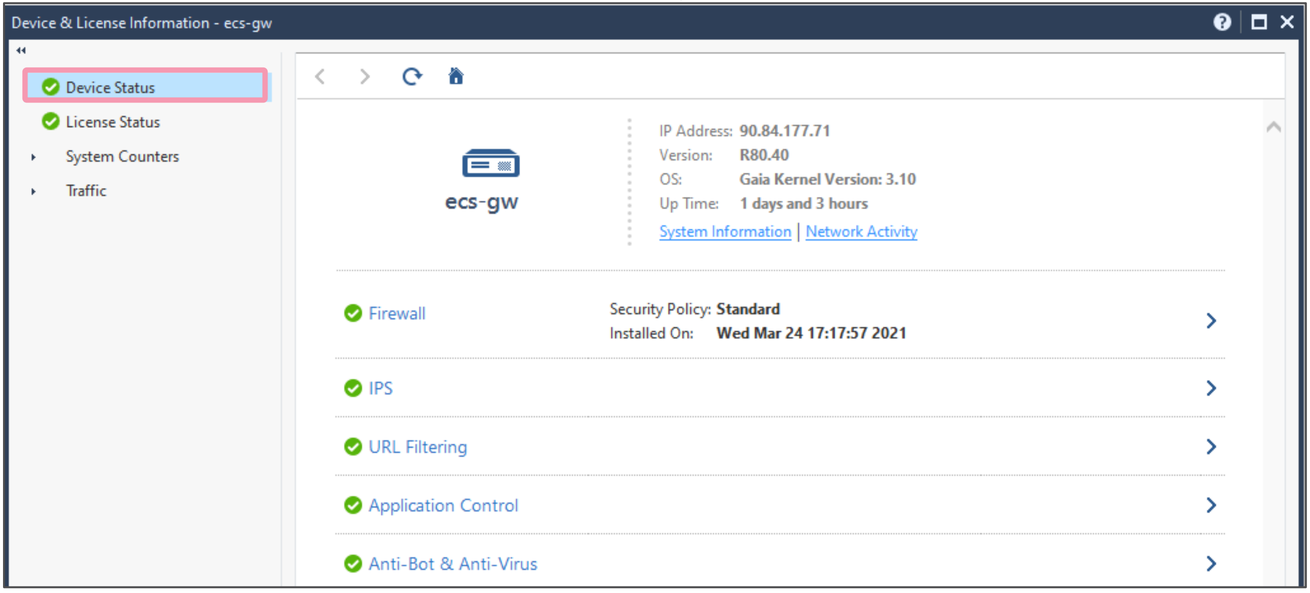


CPU: 13%

Memory: 28%

Device & License Information...

You can now review in more details its Device & Licensing information.



IP Address: 90.84.177.71
Version: R80.40
OS: Gaia Kernel Version: 3.10
Up Time: 1 days and 3 hours

System Information | Network Activity

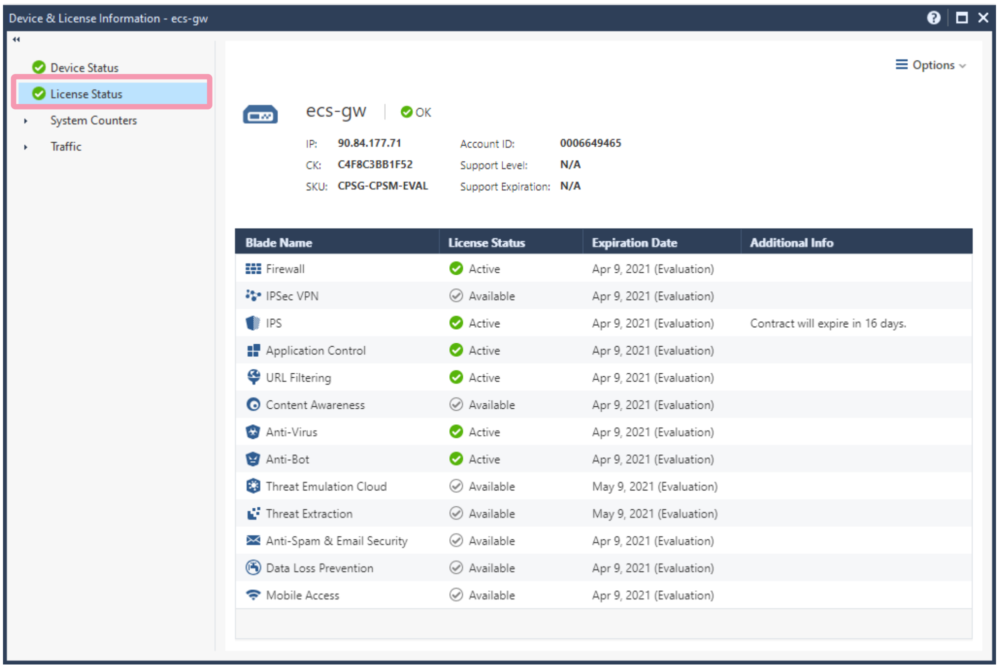
Firewall — Security Policy: Standard
Installed On: Wed Mar 24 17:17:57 2021

IPS

URL Filtering

Application Control

Anti-Bot & Anti-Virus

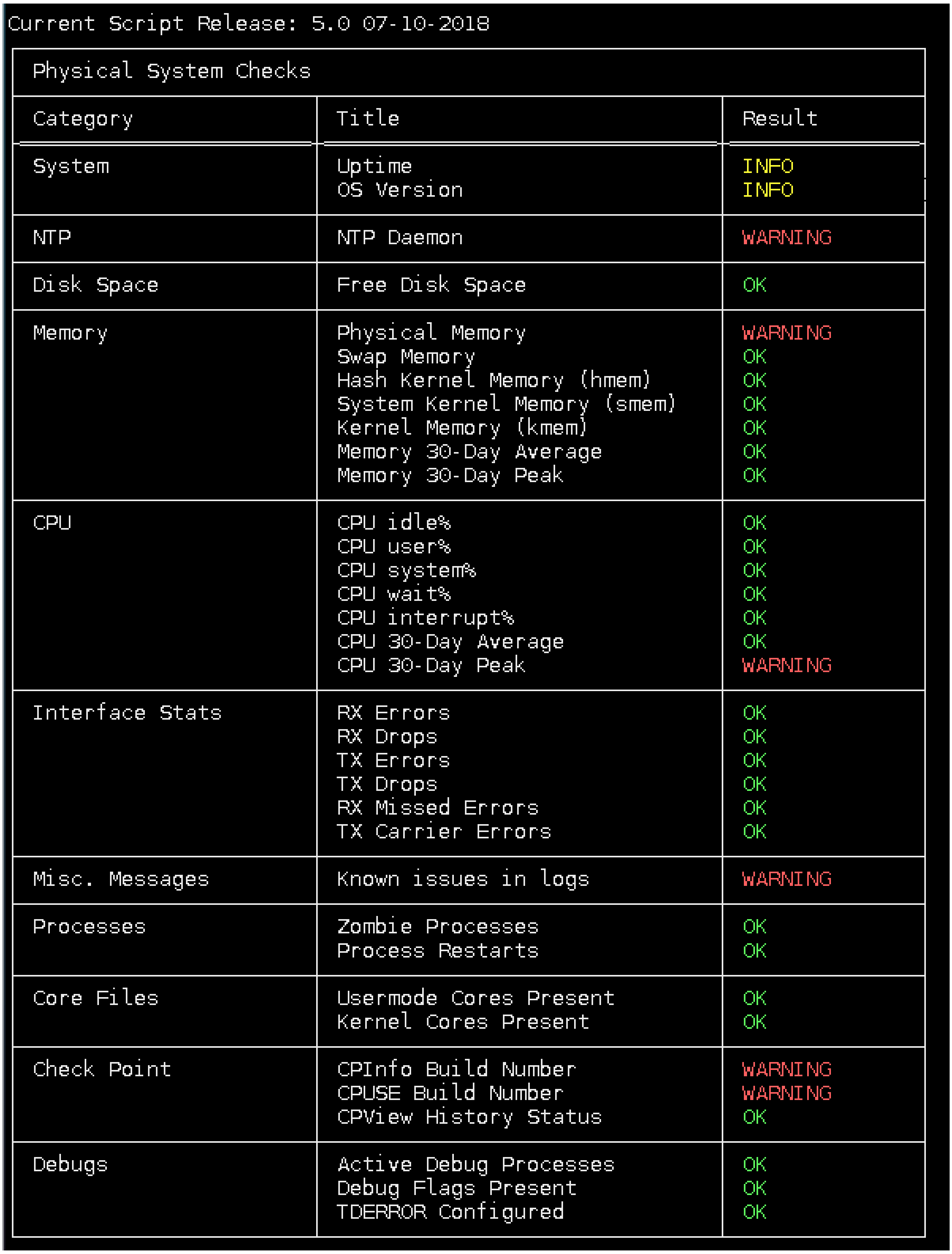


IP: 90.84.177.71
CK: C4F8C3BB1F52
SKU: CPSG-CPSM-EVAL
Account ID: 0006649465
Support Level: N/A
Support Expiration: N/A

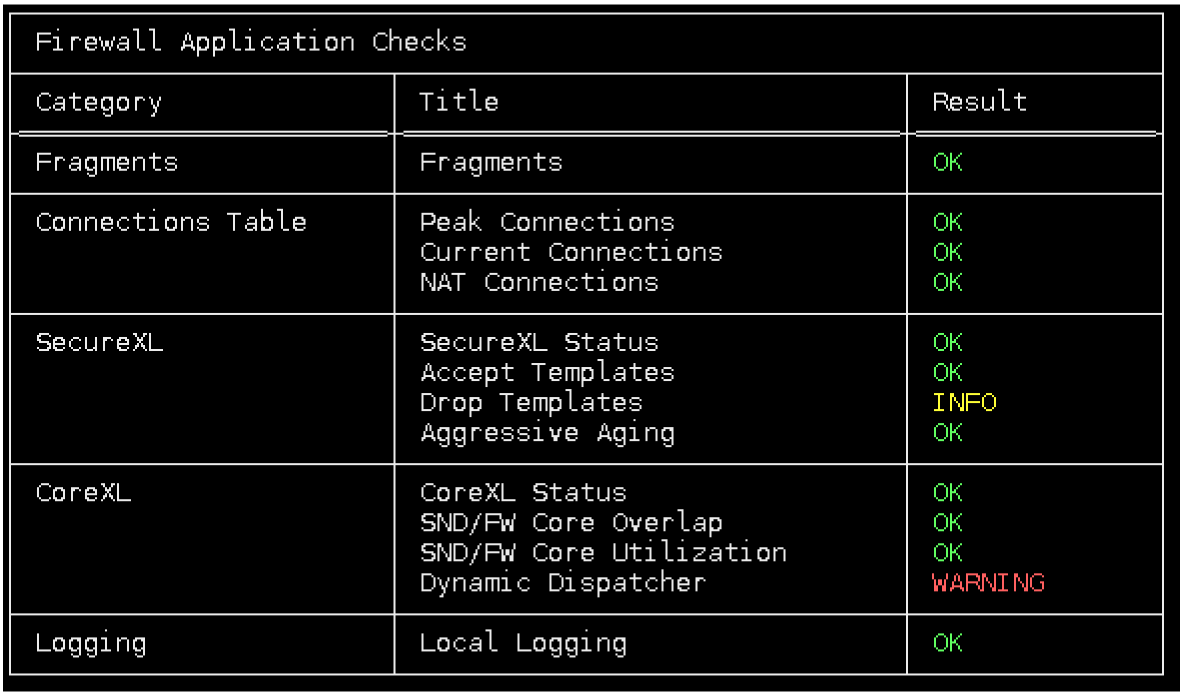
Blade Name	License Status	Expiration Date	Additional Info
Firewall	Active	Apr 9, 2021 (Evaluation)	
IPSec VPN	Available	Apr 9, 2021 (Evaluation)	
IPS	Active	Apr 9, 2021 (Evaluation)	Contract will expire in 16 days.
Application Control	Active	Apr 9, 2021 (Evaluation)	
URL Filtering	Active	Apr 9, 2021 (Evaluation)	
Content Awareness	Available	Apr 9, 2021 (Evaluation)	
Anti-Virus	Active	Apr 9, 2021 (Evaluation)	
Anti-Bot	Active	Apr 9, 2021 (Evaluation)	
Threat Emulation Cloud	Available	May 9, 2021 (Evaluation)	
Threat Extraction	Available	May 9, 2021 (Evaluation)	
Anti-Spam & Email Security	Available	Apr 9, 2021 (Evaluation)	
Data Loss Prevention	Available	Apr 9, 2021 (Evaluation)	
Mobile Access	Available	Apr 9, 2021 (Evaluation)	

In addition, if needed you can perform an automated health check of a Gaia OS based system Security Gateway please consult Solution ID: sk121447

Find some example of dashboard generated running the script.

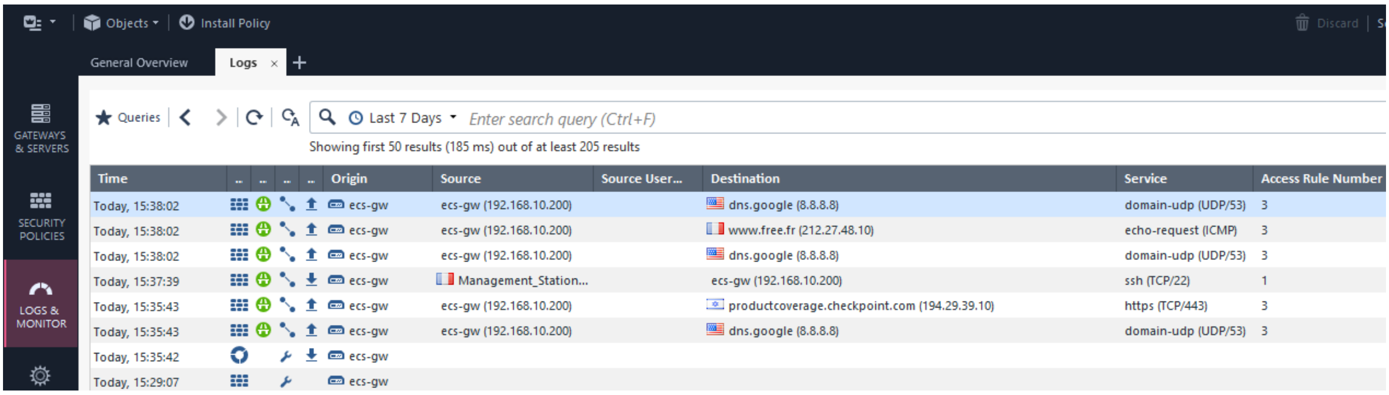


```
Current Script Release: 5.0 07-10-2018
+--------------------------------------------------------------------------+
| Physical System Checks                                                   |
+-----------------------+--------------------------------+-----------------+
| Category              | Title                          | Result          |
+=======================+================================+=================+
| System                | Uptime                         | INFO            |
|                       | OS Version                     | INFO            |
+-----------------------+--------------------------------+-----------------+
| NTP                   | NTP Daemon                     | WARNING         |
+-----------------------+--------------------------------+-----------------+
| Disk Space            | Free Disk Space                | OK              |
+-----------------------+--------------------------------+-----------------+
| Memory                | Physical Memory                | WARNING         |
|                       | Swap Memory                    | OK              |
|                       | Hash Kernel Memory (hmem)      | OK              |
|                       | System Kernel Memory (smem)    | OK              |
|                       | Kernel Memory (kmem)           | OK              |
|                       | Memory 30-Day Average          | OK              |
|                       | Memory 30-Day Peak             | OK              |
+-----------------------+--------------------------------+-----------------+
| CPU                   | CPU idle%                      | OK              |
|                       | CPU user%                      | OK              |
|                       | CPU system%                    | OK              |
|                       | CPU wait%                      | OK              |
|                       | CPU interrupt%                 | OK              |
|                       | CPU 30-Day Average             | OK              |
|                       | CPU 30-Day Peak                | WARNING         |
+-----------------------+--------------------------------+-----------------+
| Interface Stats       | RX Errors                      | OK              |
|                       | RX Drops                       | OK              |
|                       | TX Errors                      | OK              |
|                       | TX Drops                       | OK              |
|                       | RX Missed Errors               | OK              |
|                       | TX Carrier Errors              | OK              |
+-----------------------+--------------------------------+-----------------+
| Misc. Messages        | Known issues in logs           | WARNING         |
+-----------------------+--------------------------------+-----------------+
| Processes             | Zombie Processes               | OK              |
|                       | Process Restarts               | OK              |
+-----------------------+--------------------------------+-----------------+
| Core Files            | Usermode Cores Present         | OK              |
|                       | Kernel Cores Present           | OK              |
+-----------------------+--------------------------------+-----------------+
| Check Point           | CPInfo Build Number            | WARNING         |
|                       | CPUSE Build Number             | WARNING         |
|                       | CPView History Status          | OK              |
+-----------------------+--------------------------------+-----------------+
| Debugs                | Active Debug Processes         | OK              |
|                       | Debug Flags Present            | OK              |
|                       | TDERROR Configured             | OK              |
+-----------------------+--------------------------------+-----------------+
```



```
Firewall Application Checks
+--------------------+---------------------------+----------+
| Category           | Title                     | Result   |
+====================+===========================+==========+
| Fragments          | Fragments                 | OK       |
+--------------------+---------------------------+----------+
| Connections Table  | Peak Connections          | OK       |
|                    | Current Connections       | OK       |
|                    | NAT Connections           | OK       |
+--------------------+---------------------------+----------+
| SecureXL           | SecureXL Status           | OK       |
|                    | Accept Templates          | OK       |
|                    | Drop Templates            | INFO     |
|                    | Aggressive Aging          | OK       |
+--------------------+---------------------------+----------+
| CoreXL             | CoreXL Status             | OK       |
|                    | SND/FW Core Overlap       | OK       |
|                    | SND/FW Core Utilization   | OK       |
|                    | Dynamic Dispatcher        | WARNING  |
+--------------------+---------------------------+----------+
| Logging            | Local Logging             | OK       |
+--------------------+---------------------------+----------+
```

Finally yet importantly, make sure logs sent from Security Gateway are received from Management Server / Log Server. If it's not the case, most of time blocked connectivity is the root cause (don't forget to check Security Groups policy on Flexible Engine side).



Showing first 50 results (185 ms) out of at least 205 results

Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Access Rule Number
Today, 15:38:02					ecs-gw	ecs-gw (192.168.10.200)		dns.google (8.8.8.8)	domain-udp (UDP/53)	3
Today, 15:38:02					ecs-gw	ecs-gw (192.168.10.200)		www.free.fr (212.27.48.10)	echo-request (ICMP)	3
Today, 15:38:02					ecs-gw	ecs-gw (192.168.10.200)		dns.google (8.8.8.8)	domain-udp (UDP/53)	3
Today, 15:37:39					ecs-gw	Management_Station...		ecs-gw (192.168.10.200)	ssh (TCP/22)	1
Today, 15:35:43					ecs-gw	ecs-gw (192.168.10.200)		productcoverage.checkpoint.com (194.29.39.10)	https (TCP/443)	3
Today, 15:35:43					ecs-gw	ecs-gw (192.168.10.200)		dns.google (8.8.8.8)	domain-udp (UDP/53)	3
Today, 15:35:42					ecs-gw					
Today, 15:29:07					ecs-gw					

You can finalize the testing process by checking Check Point Threat Prevention configuration effectiveness using CheckMe Instant Security Check after configuring NGTP (Next Generation Threat Prevention) Blades in Prevent Mode (Application Control blocking High Risks and Anonymizers, IPS, Antivirus and Anti-Bot).

END OF THE DOCUMENT