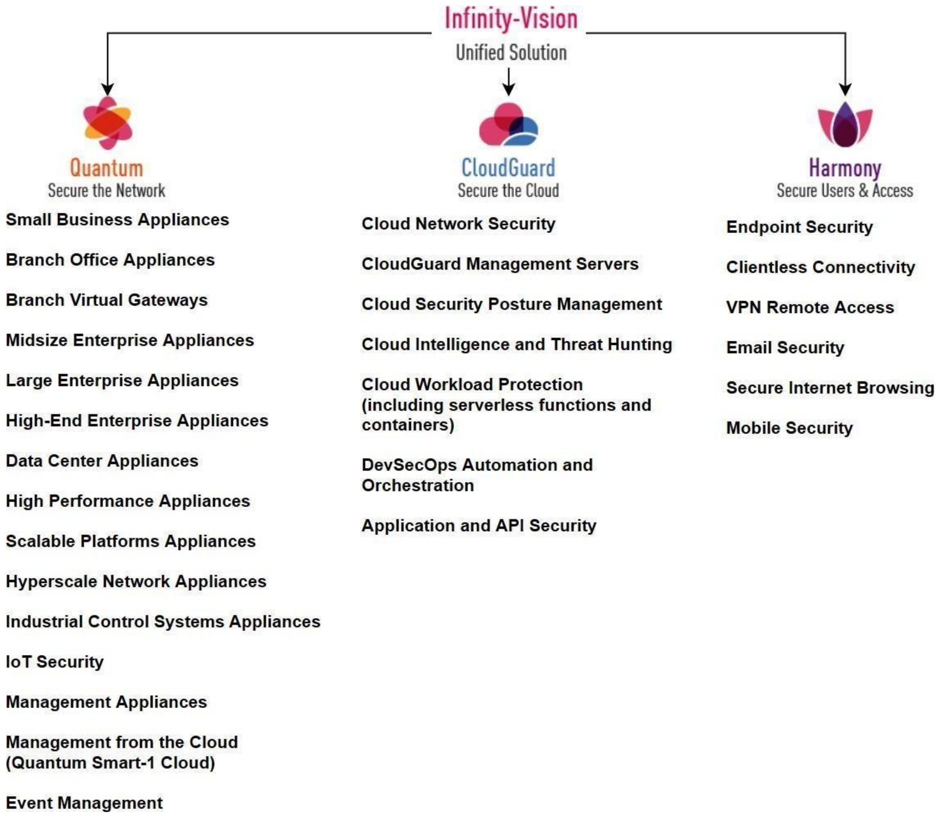
Chapter 1: Introduction to Check Point Firewalls and Threat Prevention Products



Infinity-Vision
Unified Solution

Quantum
Secure the Network

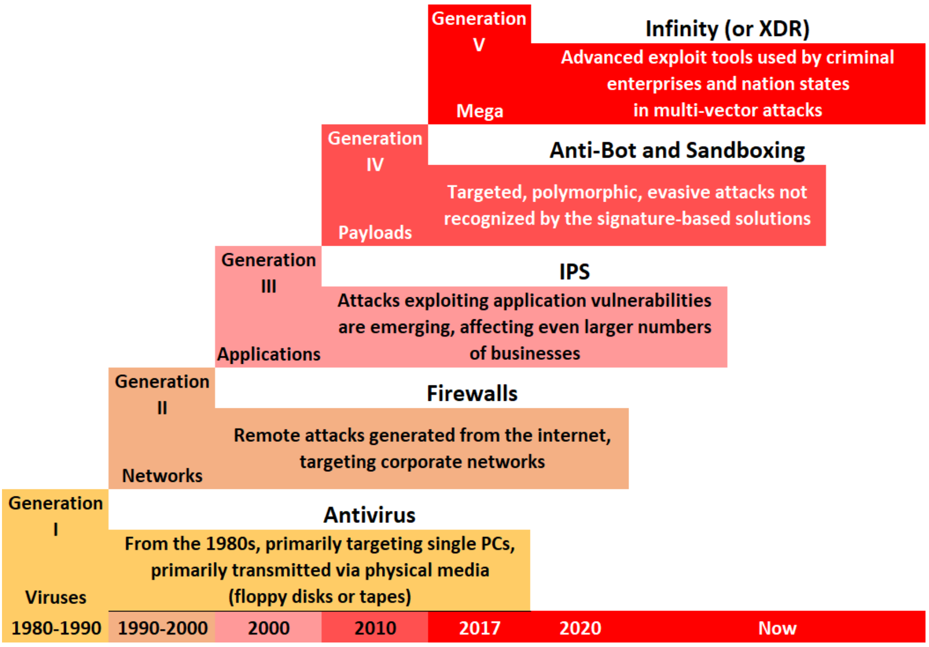
- Small Business Appliances
- Branch Office Appliances
- Branch Virtual Gateways
- Midsize Enterprise Appliances
- Large Enterprise Appliances
- High-End Enterprise Appliances
- Data Center Appliances
- High Performance Appliances
- Scalable Platforms Appliances
- Hyperscale Network Appliances
- Industrial Control Systems Appliances
- IoT Security
- Management Appliances
- Management from the Cloud (Quantum Smart-1 Cloud)
- Event Management

CloudGuard
Secure the Cloud

- Cloud Network Security
- CloudGuard Management Servers
- Cloud Security Posture Management
- Cloud Intelligence and Threat Hunting
- Cloud Workload Protection (including serverless functions and containers)
- DevSecOps Automation and Orchestration
- Application and API Security

Harmony
Secure Users & Access

- Endpoint Security
- Clientless Connectivity
- VPN Remote Access
- Email Security
- Secure Internet Browsing
- Mobile Security



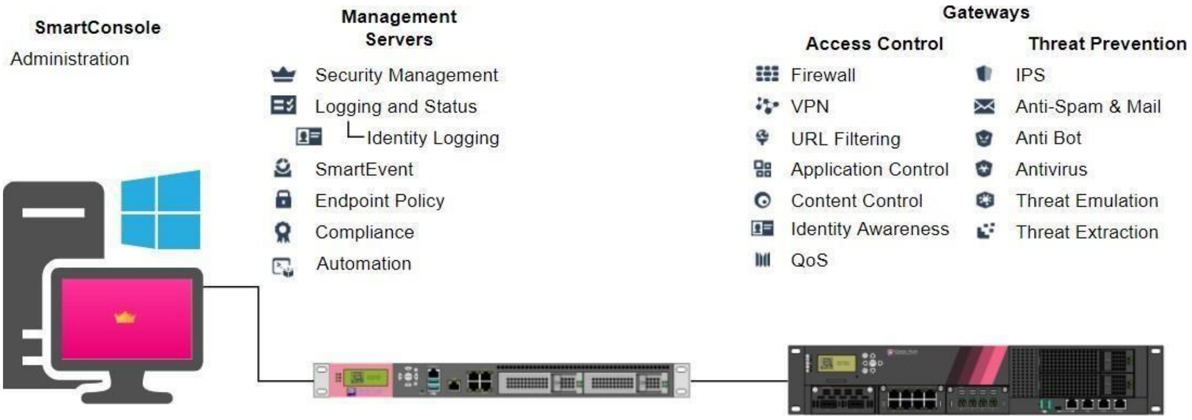
Generation V
Mega
Infinity (or XDR)
Advanced exploit tools used by criminal enterprises and nation states in multi-vector attacks

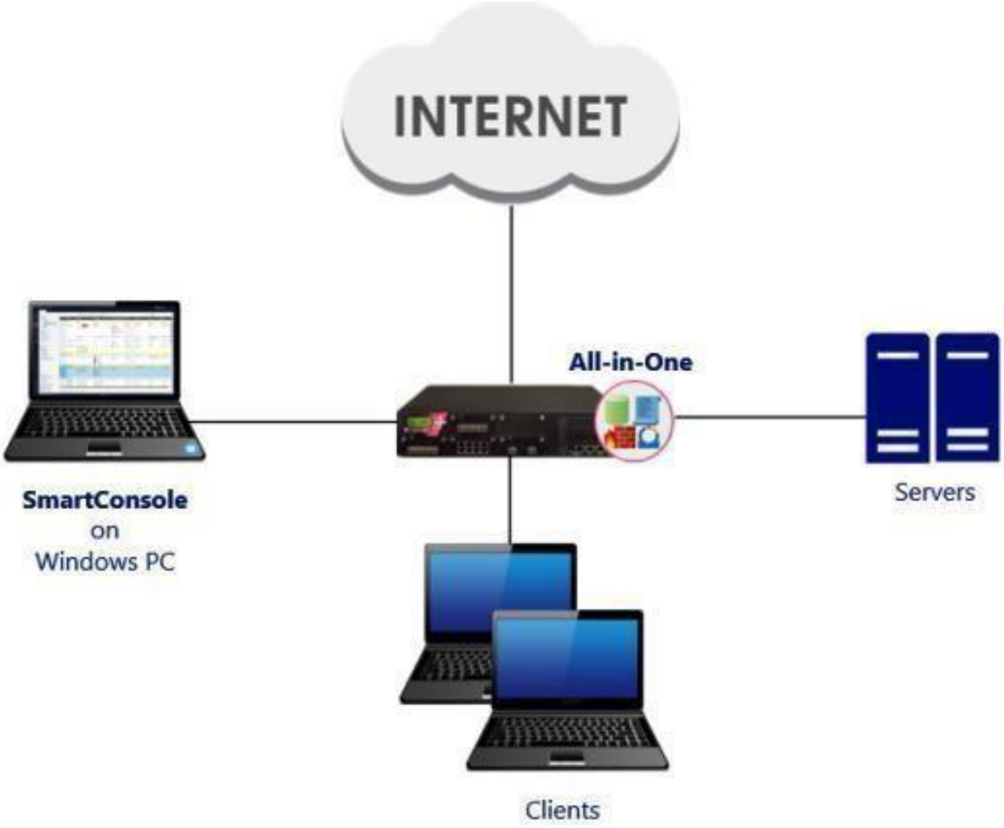
Generation IV
Payloads
Anti-Bot and Sandboxing
Targeted, polymorphic, evasive attacks not recognized by the signature-based solutions

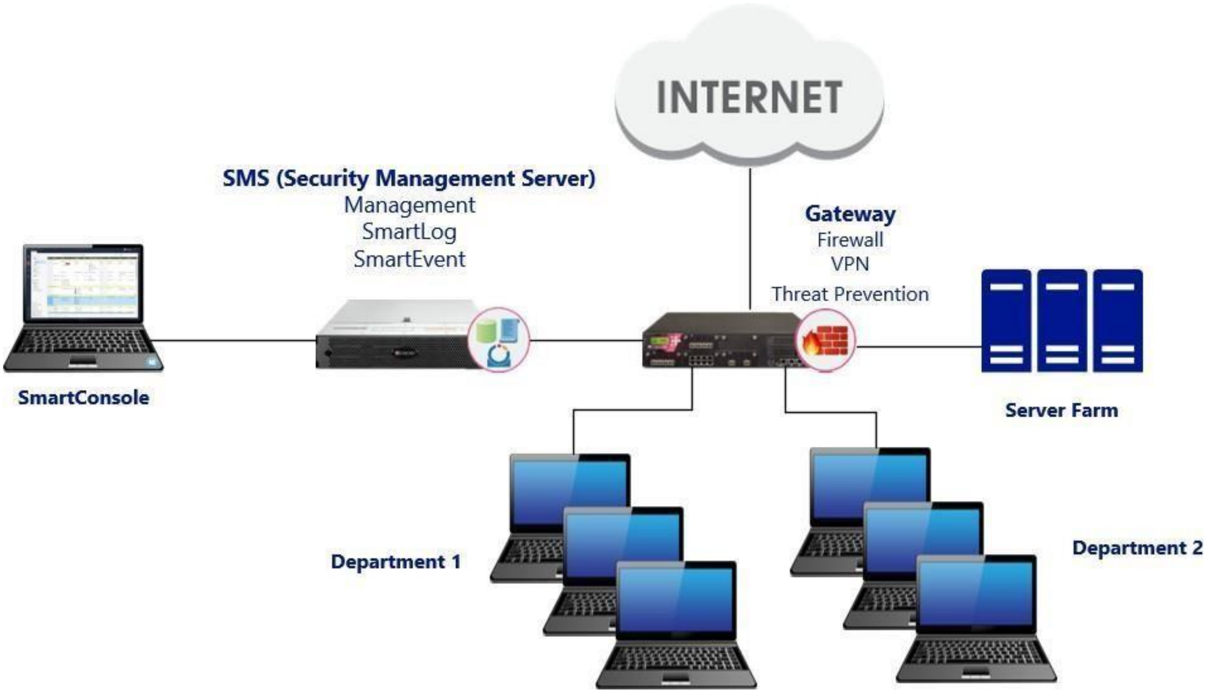
Generation III
Applications
IPS
Attacks exploiting application vulnerabilities are emerging, affecting even larger numbers of businesses

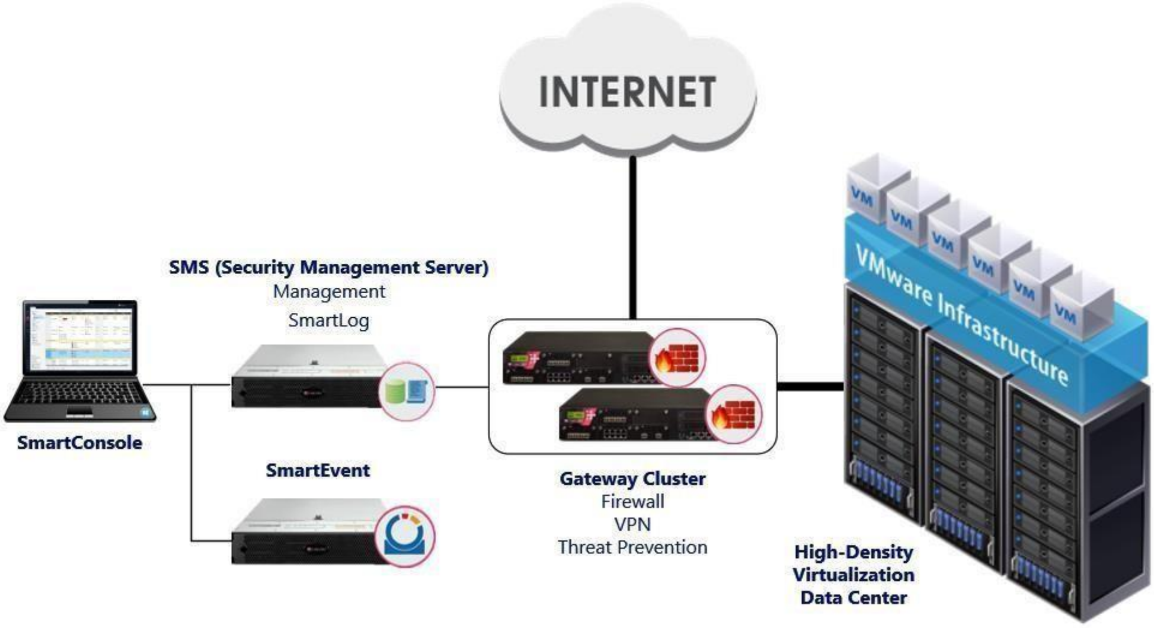
Generation II
Networks
Firewalls
Remote attacks generated from the internet, targeting corporate networks

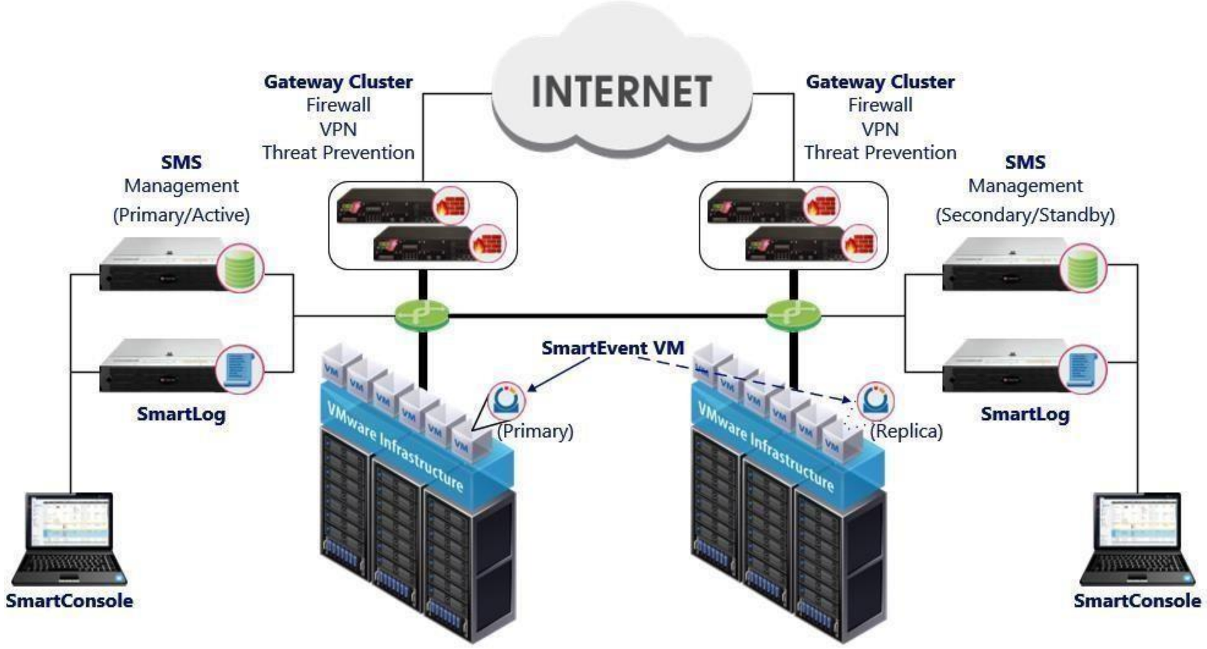
Generation I
Viruses
Antivirus
From the 1980s, primarily targeting single PCs, primarily transmitted via physical media (floppy disks or tapes)

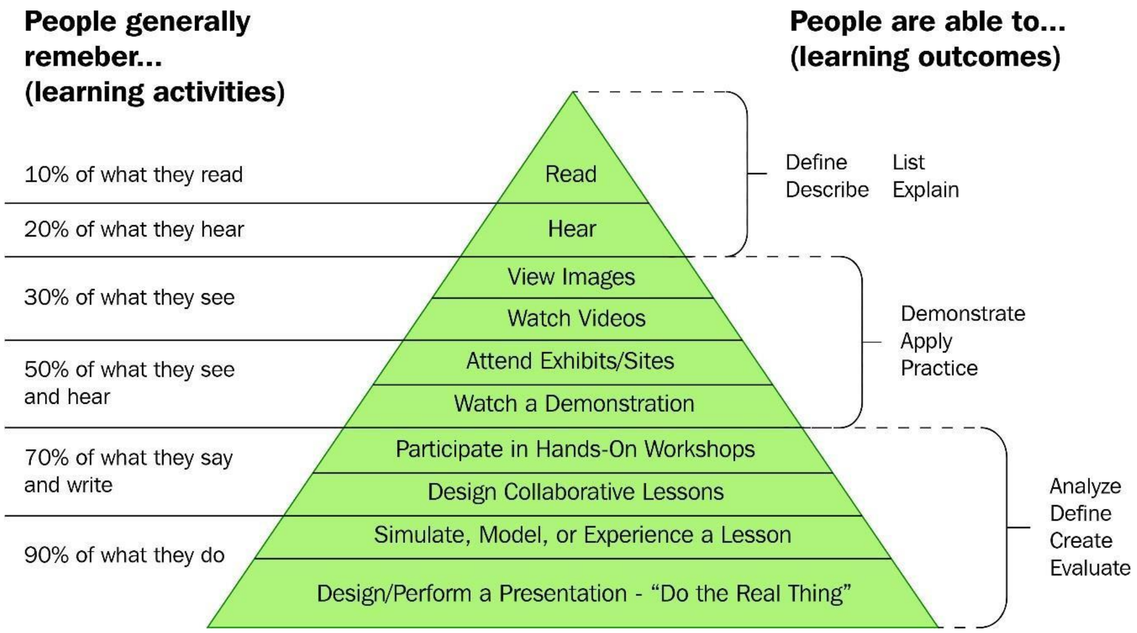

SmartConsole
Administration
Management Servers
Security Management
Logging and Status
Identity Logging
SmartEvent
Endpoint Policy
Compliance
Automation
Gateways
Access Control
Firewall
VPN
URL Filtering
Application Control
Content Control
Identity Awareness
QoS
Threat Prevention
IPS
Anti-Spam & Mail
Anti Bot
Antivirus
Threat Emulation
Threat Extraction


INTERNET
All-in-One
SmartConsole
on
Windows PC
Servers
Clients


INTERNET
SMS (Security Management Server)
Management
SmartLog
SmartEvent
Gateway
Firewall
VPN
Threat Prevention
SmartConsole
Server Farm
Department 1
Department 2


INTERNET
SMS (Security Management Server)
Management
SmartLog
SmartConsole
SmartEvent
Gateway Cluster
Firewall
VPN
Threat Prevention
VM
VMware Infrastructure
High-Density
Virtualization
Data Center





People generally remeber... (learning activities)

People are able to... (learning outcomes)

10% of what they read — Read

20% of what they hear — Hear

Define List Describe Explain

30% of what they see — View Images, Watch Videos

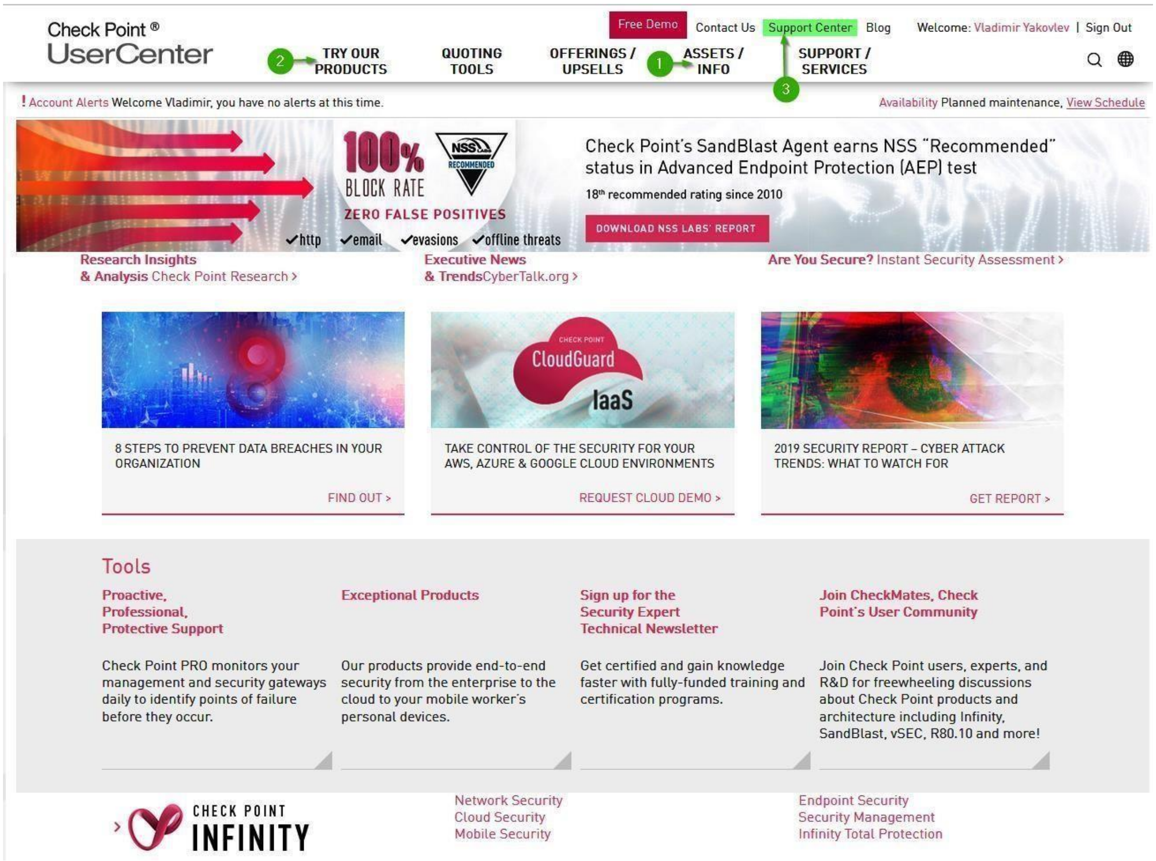
50% of what they see and hear — Attend Exhibits/Sites, Watch a Demonstration

Demonstrate Apply Practice

70% of what they say and write — Participate in Hands-On Workshops, Design Collaborative Lessons

90% of what they do — Simulate, Model, or Experience a Lesson, Design/Perform a Presentation - “Do the Real Thing”

Analyze Define Create Evaluate



! Account Alerts Welcome Vladimir, you have no alerts at this time.

Availability Planned maintenance, View Schedule

Check Point's SandBlast Agent earns NSS "Recommended" status in Advanced Endpoint Protection (AEP) test

18th recommended rating since 2010

Research Insights & Analysis Check Point Research >

Executive News & Trends CyberTalk.org >

Are You Secure? Instant Security Assessment >

8 STEPS TO PREVENT DATA BREACHES IN YOUR ORGANIZATION

TAKE CONTROL OF THE SECURITY FOR YOUR AWS, AZURE & GOOGLE CLOUD ENVIRONMENTS

2019 SECURITY REPORT – CYBER ATTACK TRENDS: WHAT TO WATCH FOR

Tools

Proactive, Professional, Protective Support

Check Point PRO monitors your management and security gateways daily to identify points of failure before they occur.

Exceptional Products

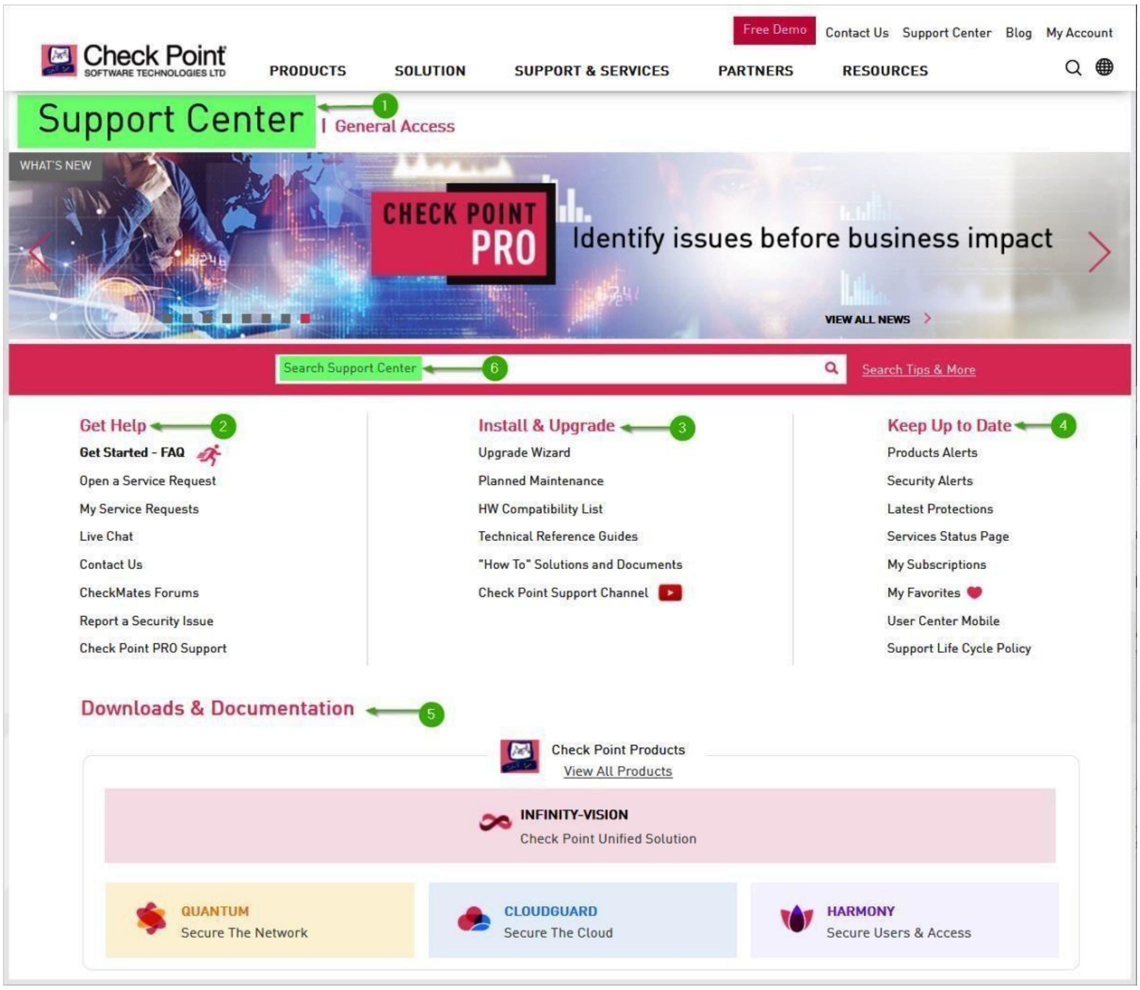
Our products provide end-to-end security from the enterprise to the cloud to your mobile worker's personal devices.

Sign up for the Security Expert Technical Newsletter

Get certified and gain knowledge faster with fully-funded training and certification programs.

Join CheckMates, Check Point's User Community

Join Check Point users, experts, and R&D for freewheeling discussions about Check Point products and architecture including Infinity, SandBlast, vSEC, R80.10 and more!



Free Demo Contact Us Support Center Blog My Account

Check Point SOFTWARE TECHNOLOGIES LTD

PRODUCTS SOLUTION SUPPORT & SERVICES PARTNERS RESOURCES

Support Center 1 | General Access

WHAT'S NEW

CHECK POINT PRO Identify issues before business impact

VIEW ALL NEWS

Search Support Center 6 Search Tips & More

Get Help 2
- Get Started - FAQ
- Open a Service Request
- My Service Requests
- Live Chat
- Contact Us
- CheckMates Forums
- Report a Security Issue
- Check Point PRO Support

Install & Upgrade 3
- Upgrade Wizard
- Planned Maintenance
- HW Compatibility List
- Technical Reference Guides
- "How To" Solutions and Documents
- Check Point Support Channel

Keep Up to Date 4
- Products Alerts
- Security Alerts
- Latest Protections
- Services Status Page
- My Subscriptions
- My Favorites
- User Center Mobile
- Support Life Cycle Policy

Downloads & Documentation 5

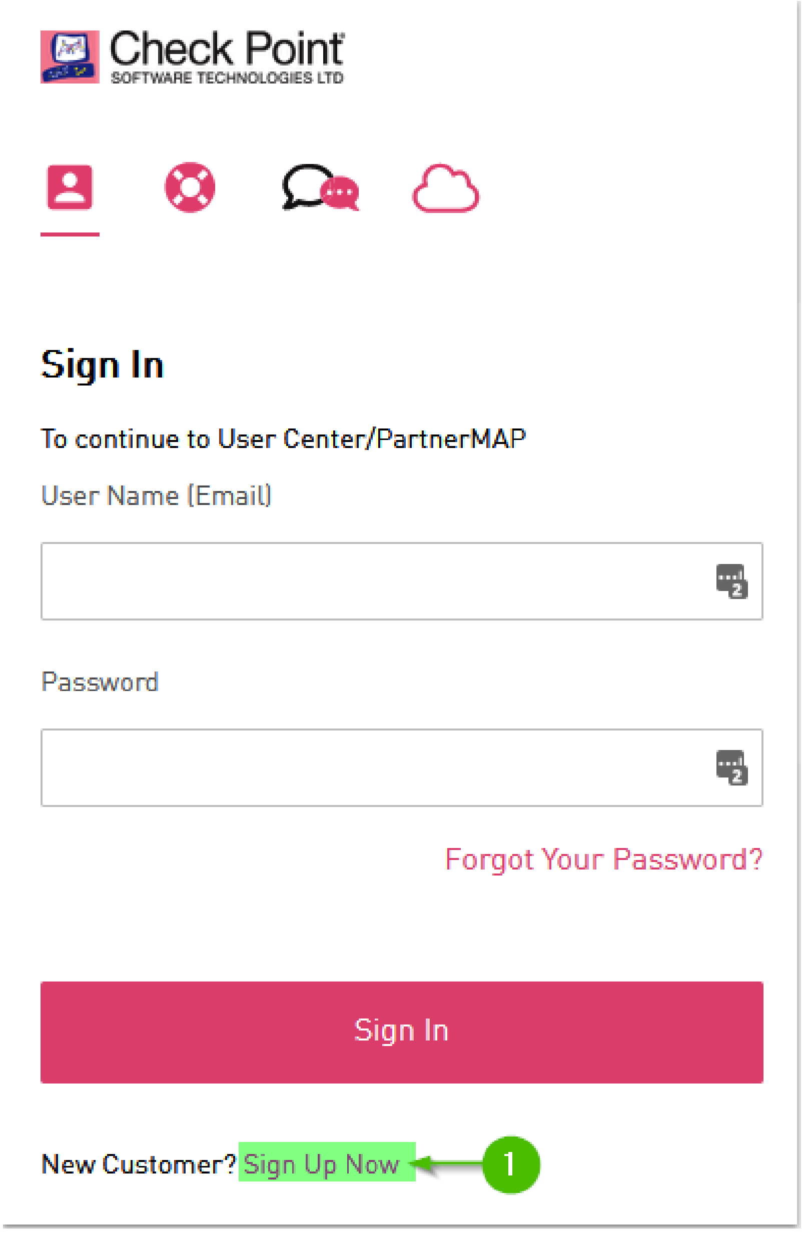
Check Point Products
View All Products

INFINITY-VISION
Check Point Unified Solution

QUANTUM
Secure The Network

CLOUDGUARD
Secure The Cloud

HARMONY
Secure Users & Access



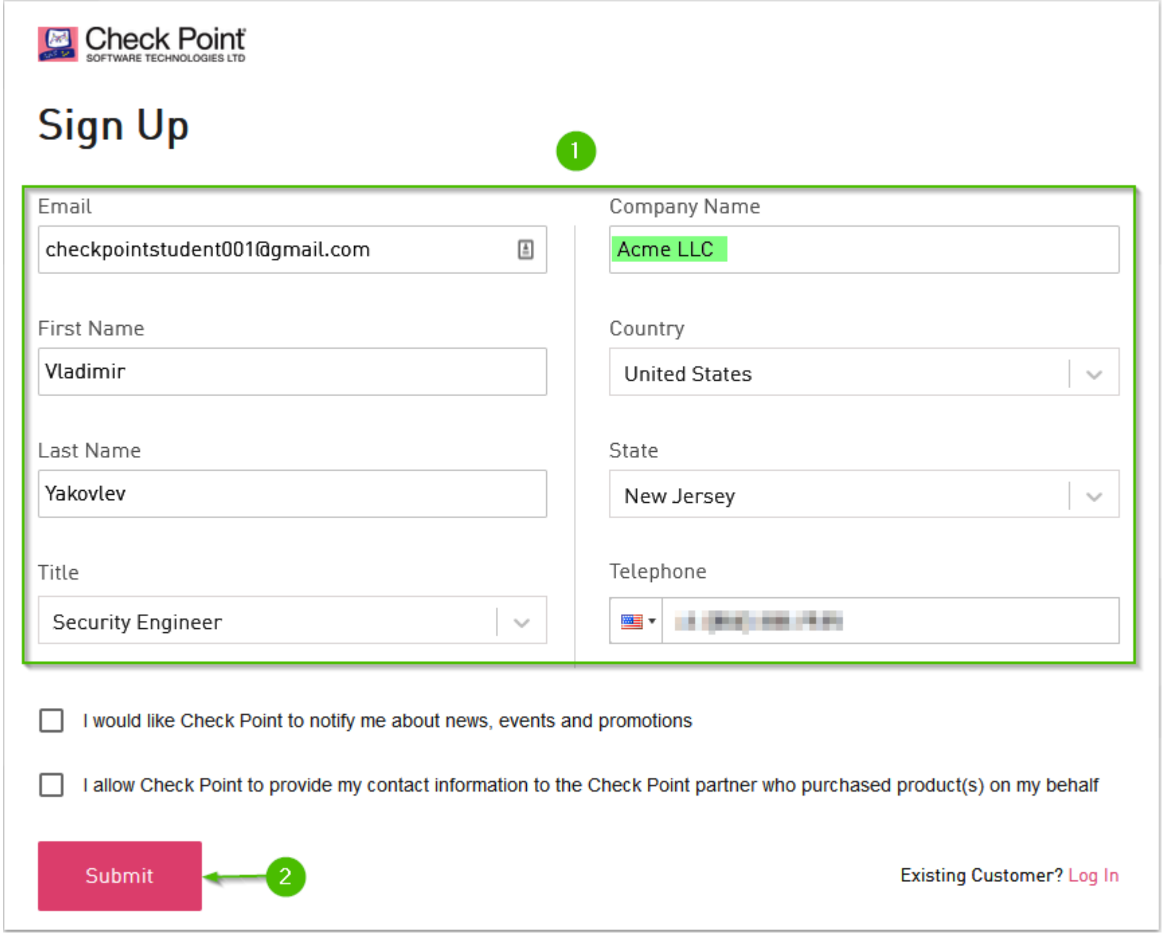
Sign In

To continue to User Center/PartnerMAP

User Name (Email)

Password

New Customer? Sign Up Now



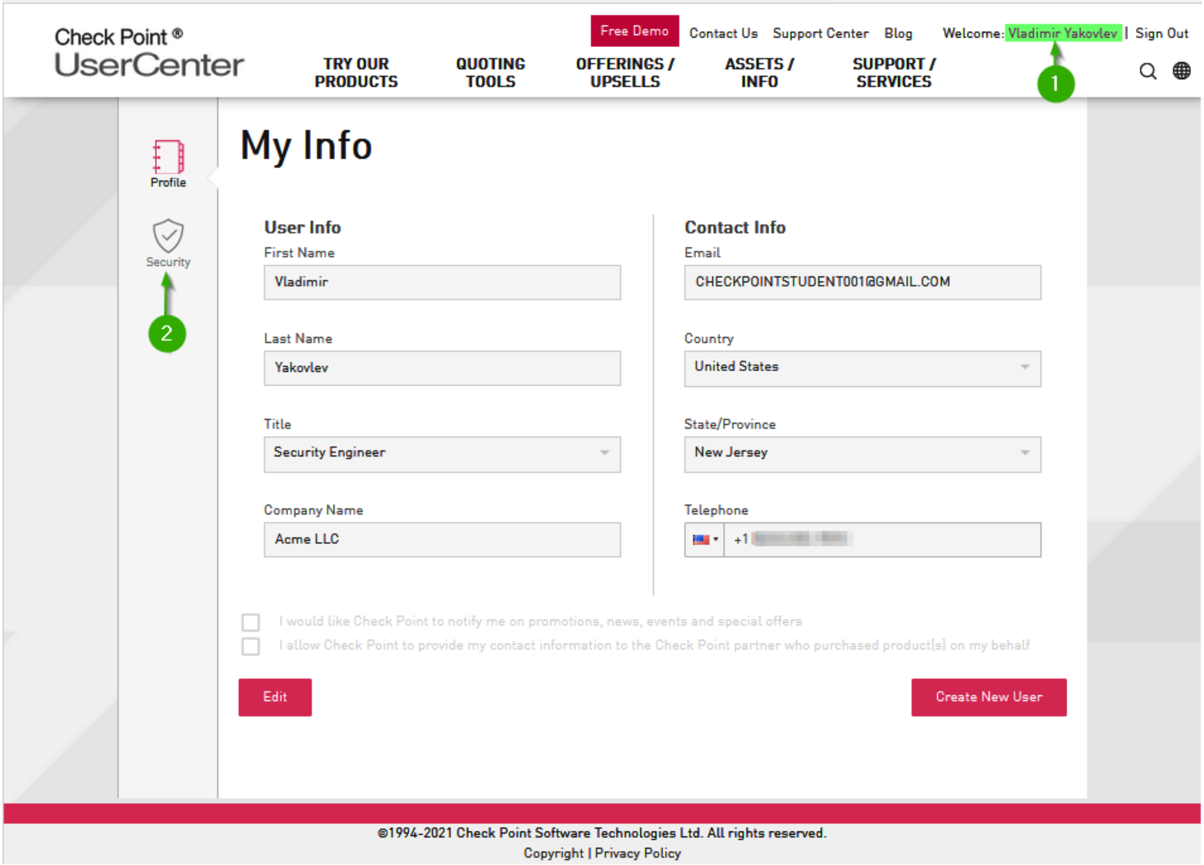
Check Point
SOFTWARE TECHNOLOGIES LTD

Sign Up

Email	Company Name
checkpointstudent001@gmail.com	Acme LLC
First Name	Country
Vladimir	United States
Last Name	State
Yakovlev	New Jersey
Title	Telephone
Security Engineer	[redacted]

☐ I would like Check Point to notify me about news, events and promotions

☐ I allow Check Point to provide my contact information to the Check Point partner who purchased product(s) on my behalf



My Info

User Info

First Name: Vladimir

Last Name: Yakovlev

Title: Security Engineer

Company Name: Acme LLC

Contact Info

Email: CHECKPOINTSTUDENT001@GMAIL.COM

Country: United States

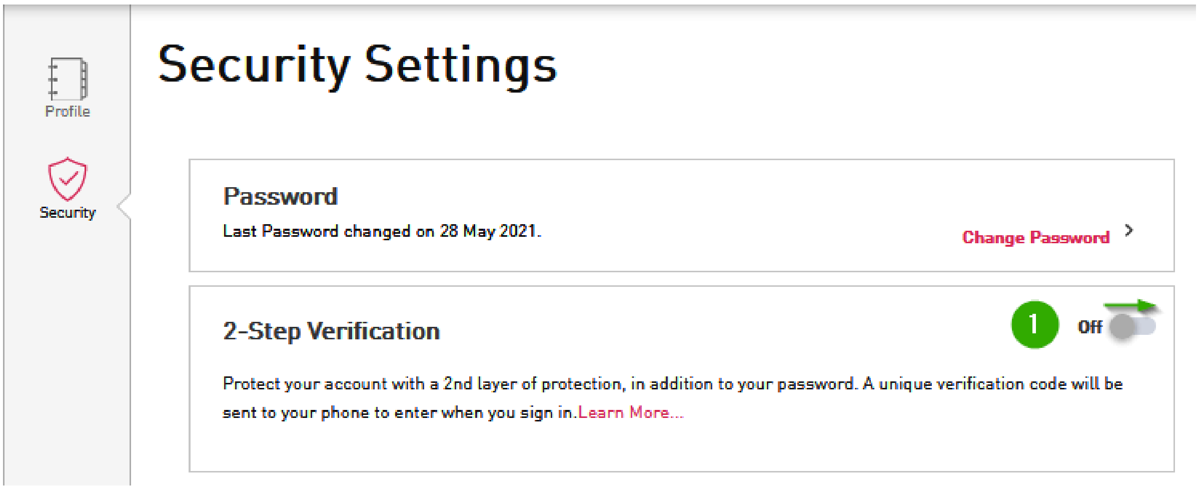
State/Province: New Jersey

Telephone: +1 [redacted]

□ I would like Check Point to notify me on promotions, news, events and special offers

□ I allow Check Point to provide my contact information to the Check Point partner who purchased product(s) on my behalf

©1994-2021 Check Point Software Technologies Ltd. All rights reserved.
Copyright | Privacy Policy



Security Settings

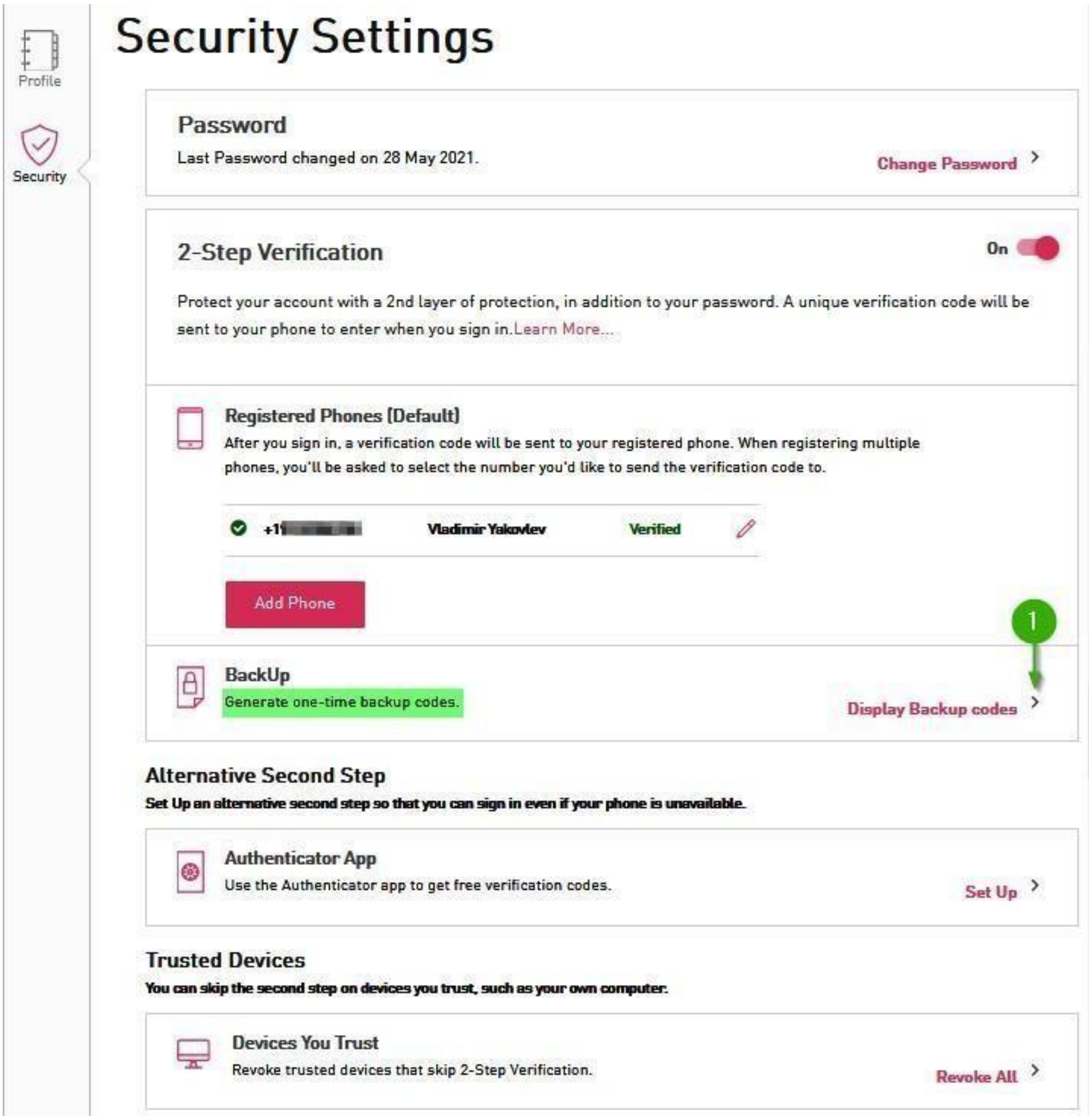
Password

Last Password changed on 28 May 2021.

2-Step Verification

Off

Protect your account with a 2nd layer of protection, in addition to your password. A unique verification code will be sent to your phone to enter when you sign in.Learn More...



Security Settings

Password

Last Password changed on 28 May 2021.

Change Password >

2-Step Verification

On

Protect your account with a 2nd layer of protection, in addition to your password. A unique verification code will be sent to your phone to enter when you sign in.Learn More...

Registered Phones (Default)

After you sign in, a verification code will be sent to your registered phone. When registering multiple phones, you'll be asked to select the number you'd like to send the verification code to.

✓ +1[redacted]	Vladimir Yakovlev	Verified	✎

Add Phone

BackUp

Generate one-time backup codes.

Display Backup codes >

Alternative Second Step

Set Up an alternative second step so that you can sign in even if your phone is unavailable.

Authenticator App

Use the Authenticator app to get free verification codes.

Set Up >

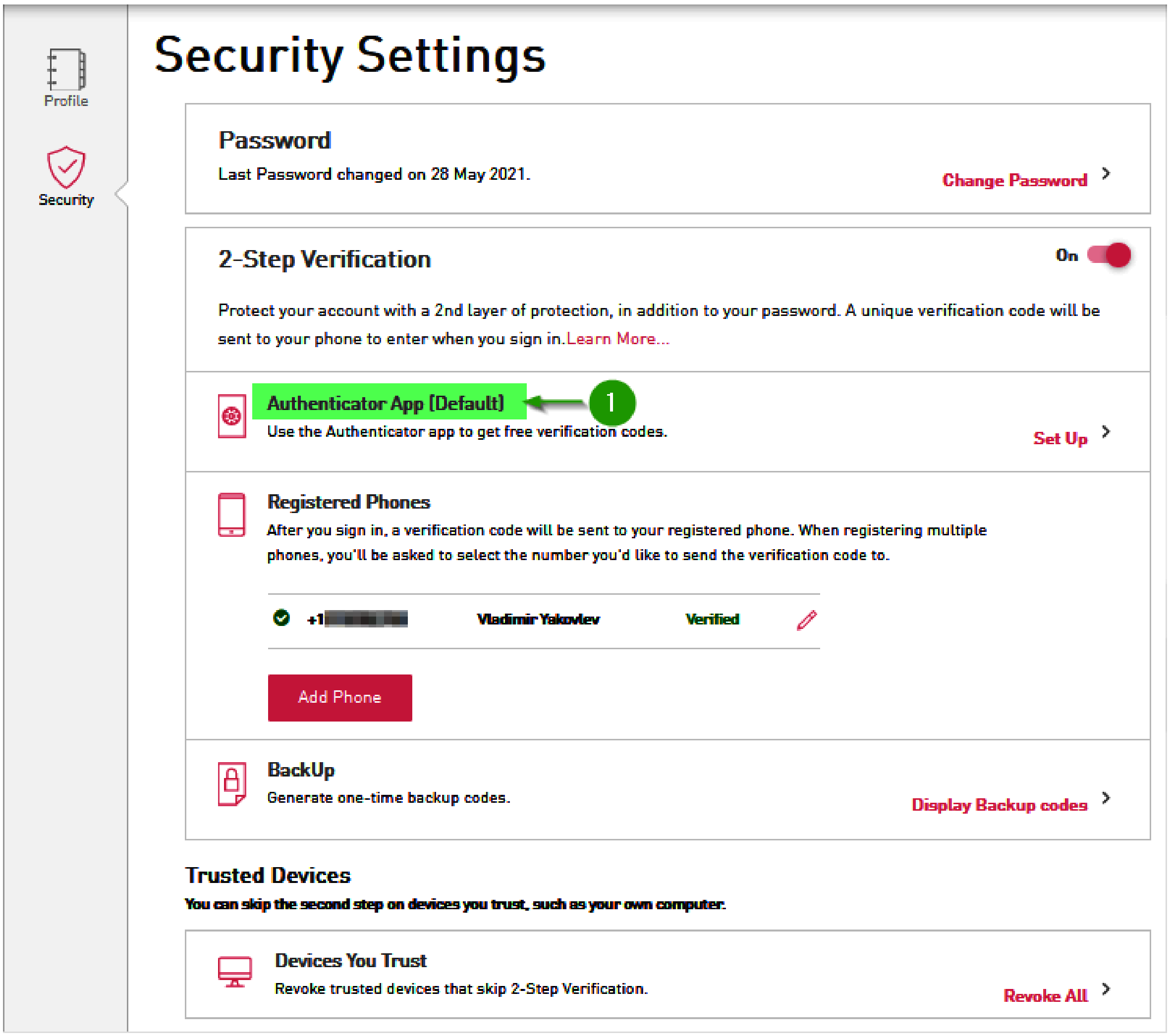
Trusted Devices

You can skip the second step on devices you trust, such as your own computer.

Devices You Trust

Revoke trusted devices that skip 2-Step Verification.

Revoke All >



Security Settings

Password

Last Password changed on 28 May 2021.

Change Password >

2-Step Verification

On

Protect your account with a 2nd layer of protection, in addition to your password. A unique verification code will be sent to your phone to enter when you sign in.Learn More...

Authenticator App (Default)

Use the Authenticator app to get free verification codes.

Set Up >

Registered Phones

After you sign in, a verification code will be sent to your registered phone. When registering multiple phones, you'll be asked to select the number you'd like to send the verification code to.

✓ +1[redacted]	Vladimir Yakovlev	Verified	✎

Add Phone

BackUp

Generate one-time backup codes.

Display Backup codes >

Trusted Devices

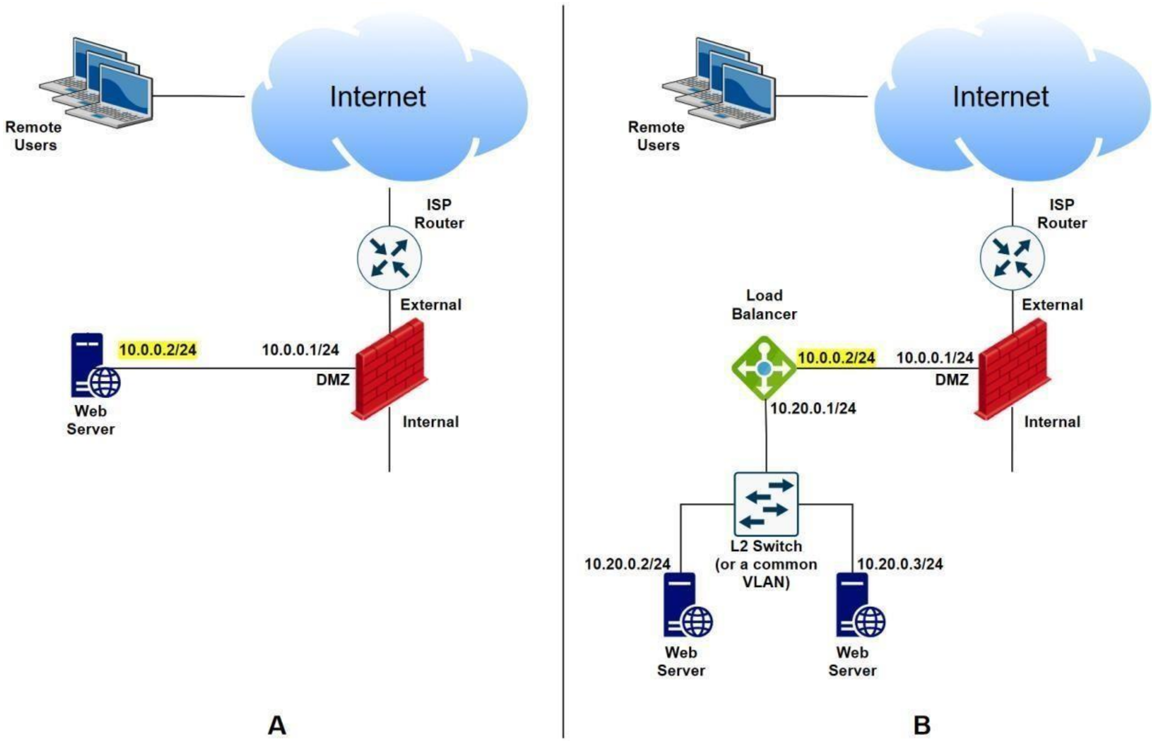
You can skip the second step on devices you trust, such as your own computer.

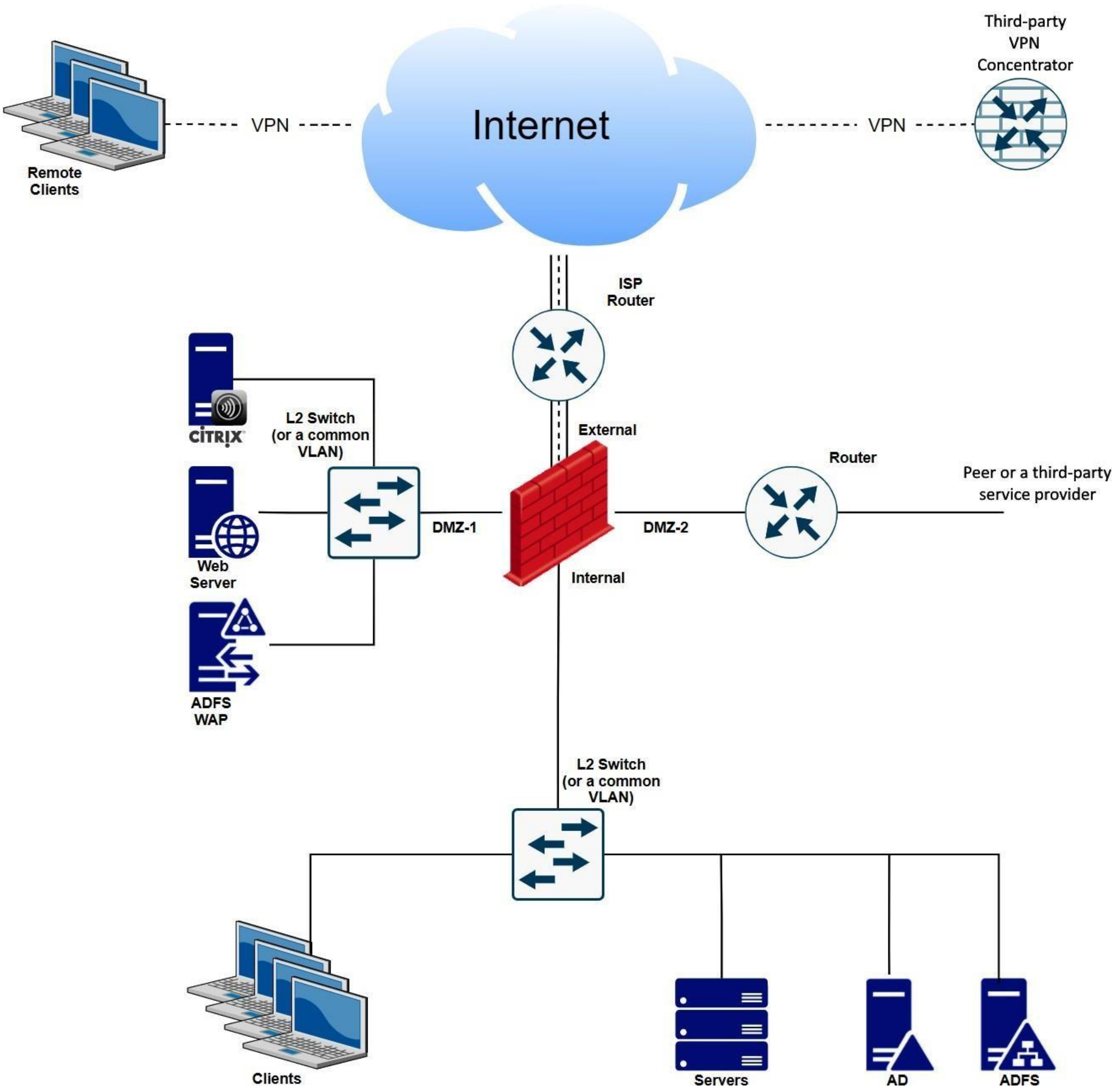
Devices You Trust

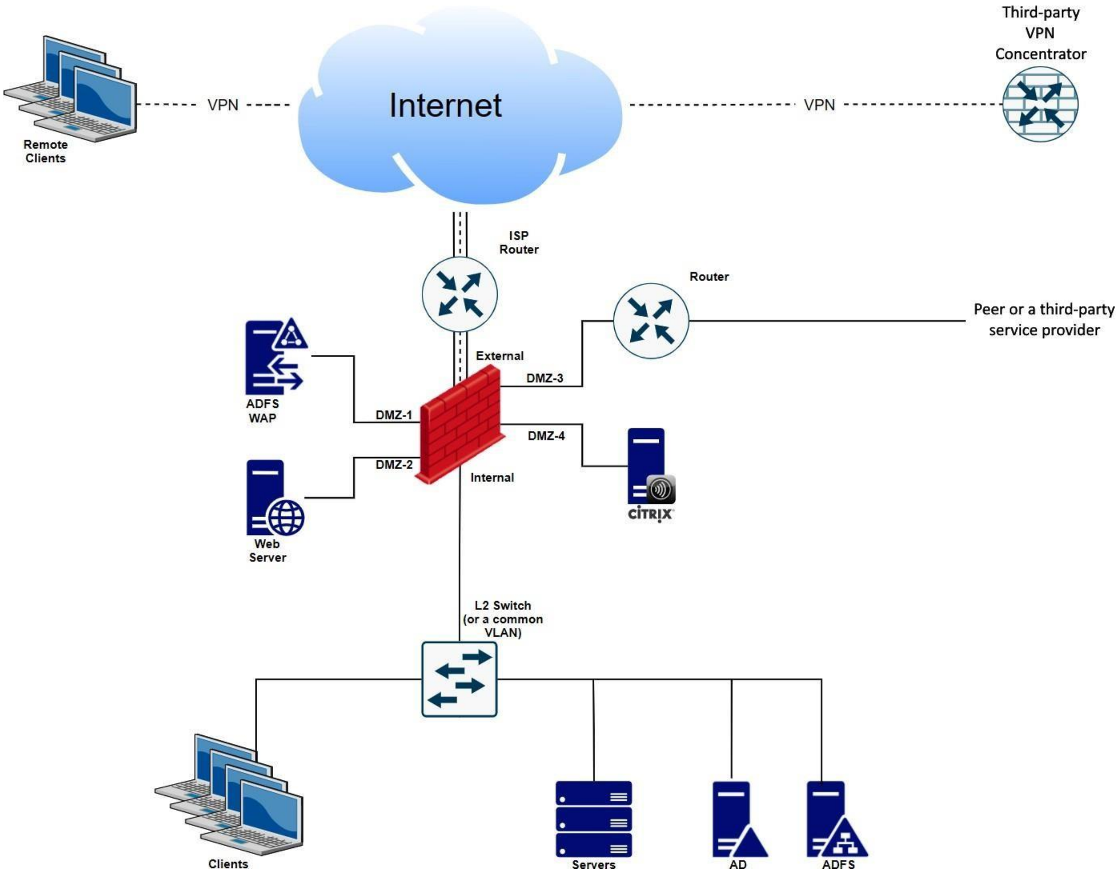
Revoke trusted devices that skip 2-Step Verification.

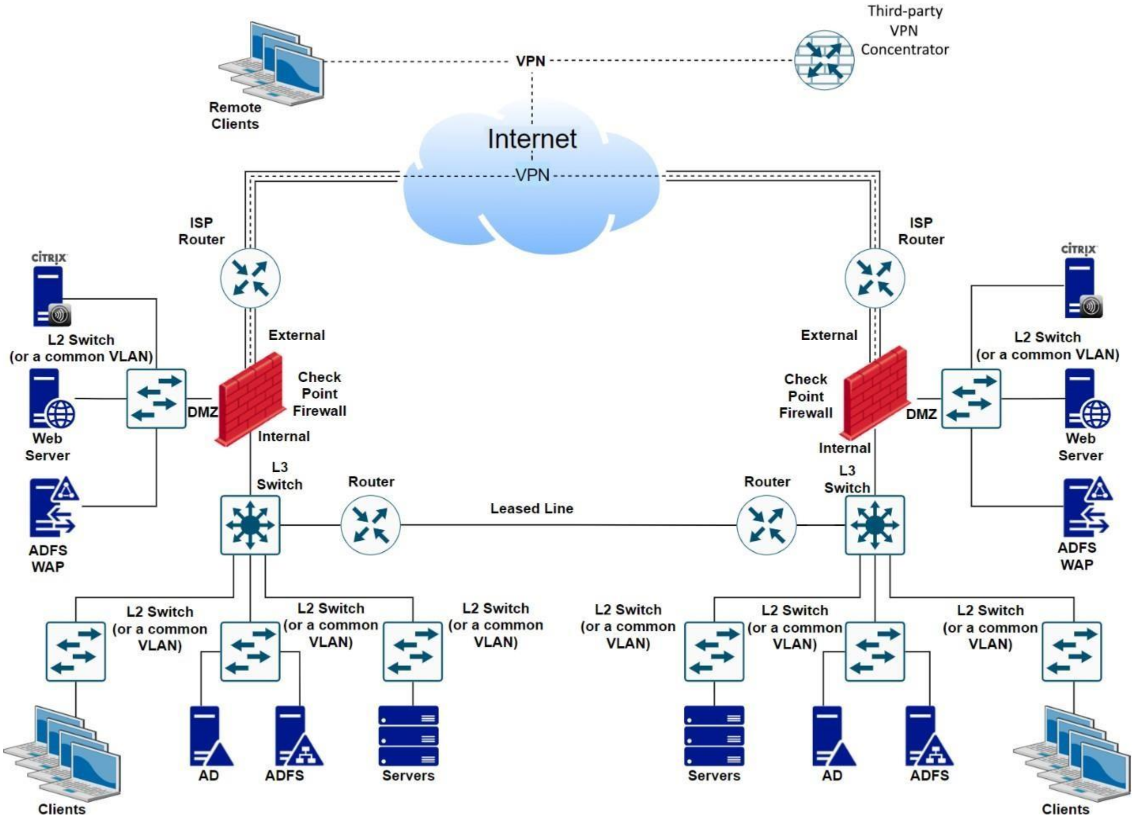
Revoke All >

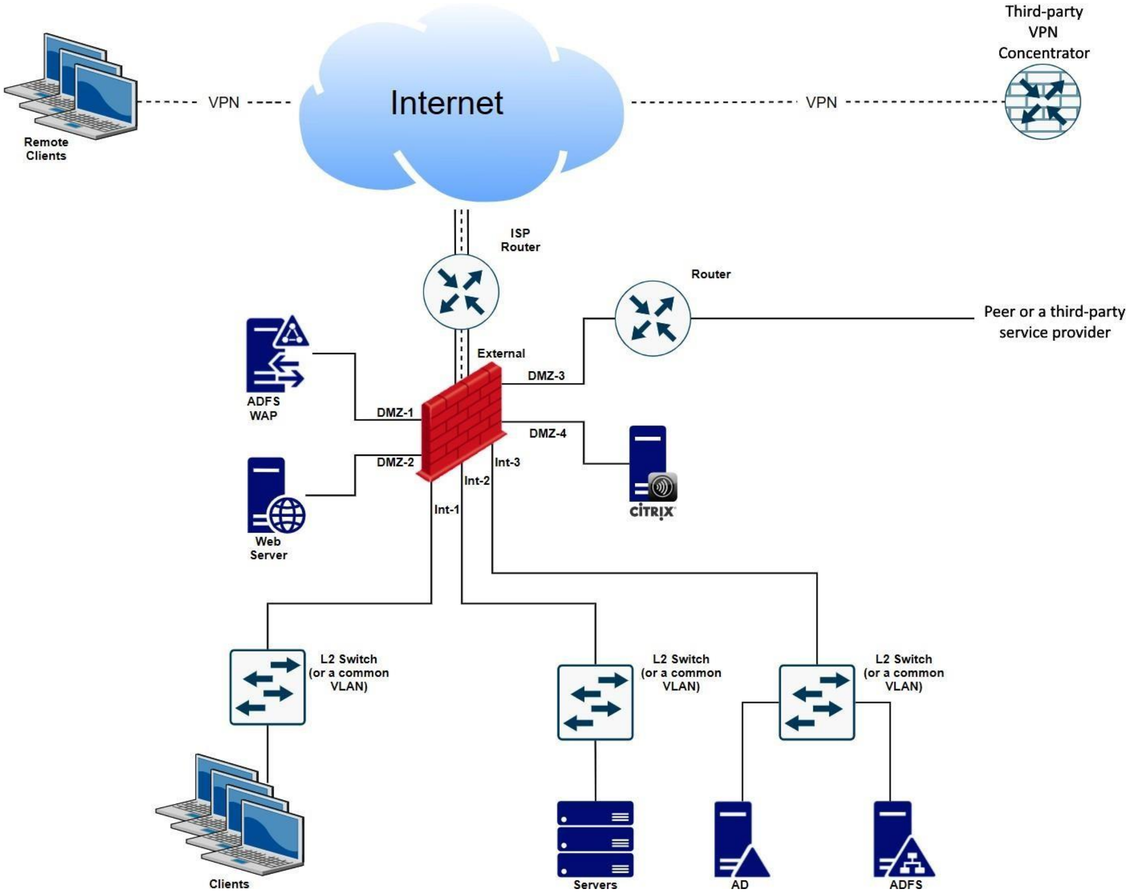
Chapter 2: Common Deployment Scenarios and Network Segmentation

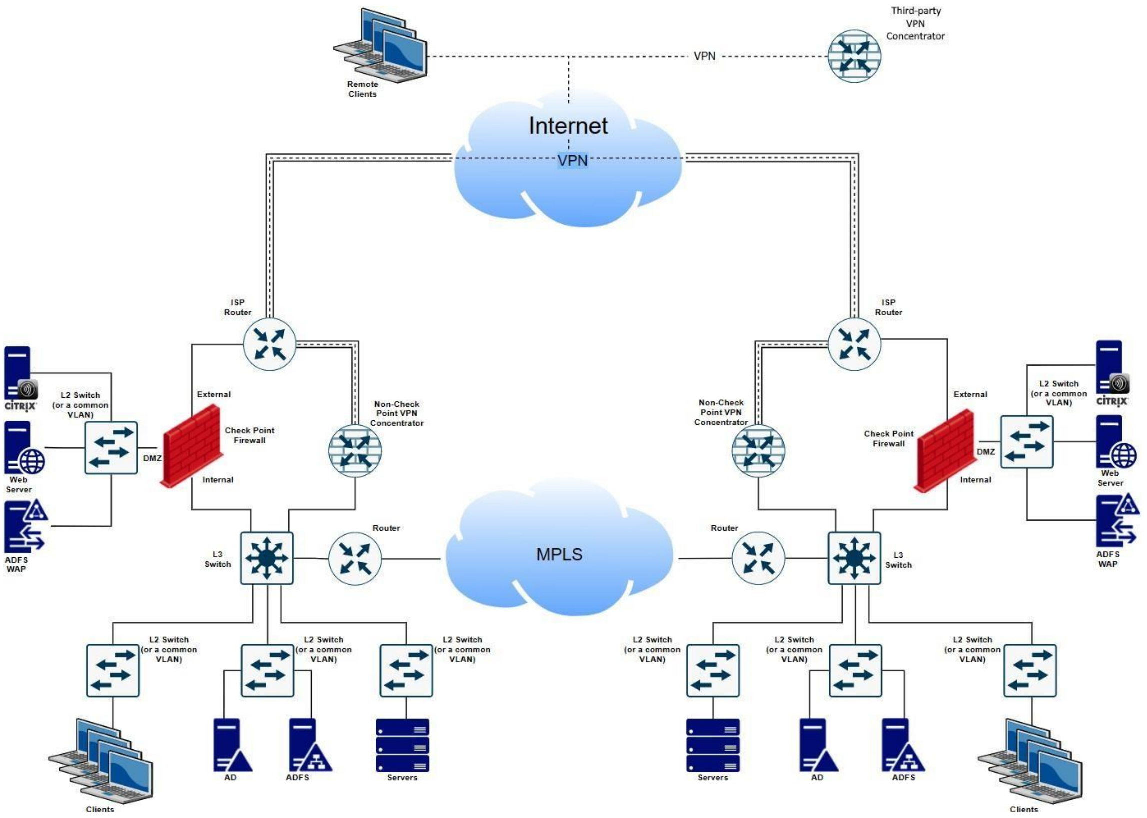


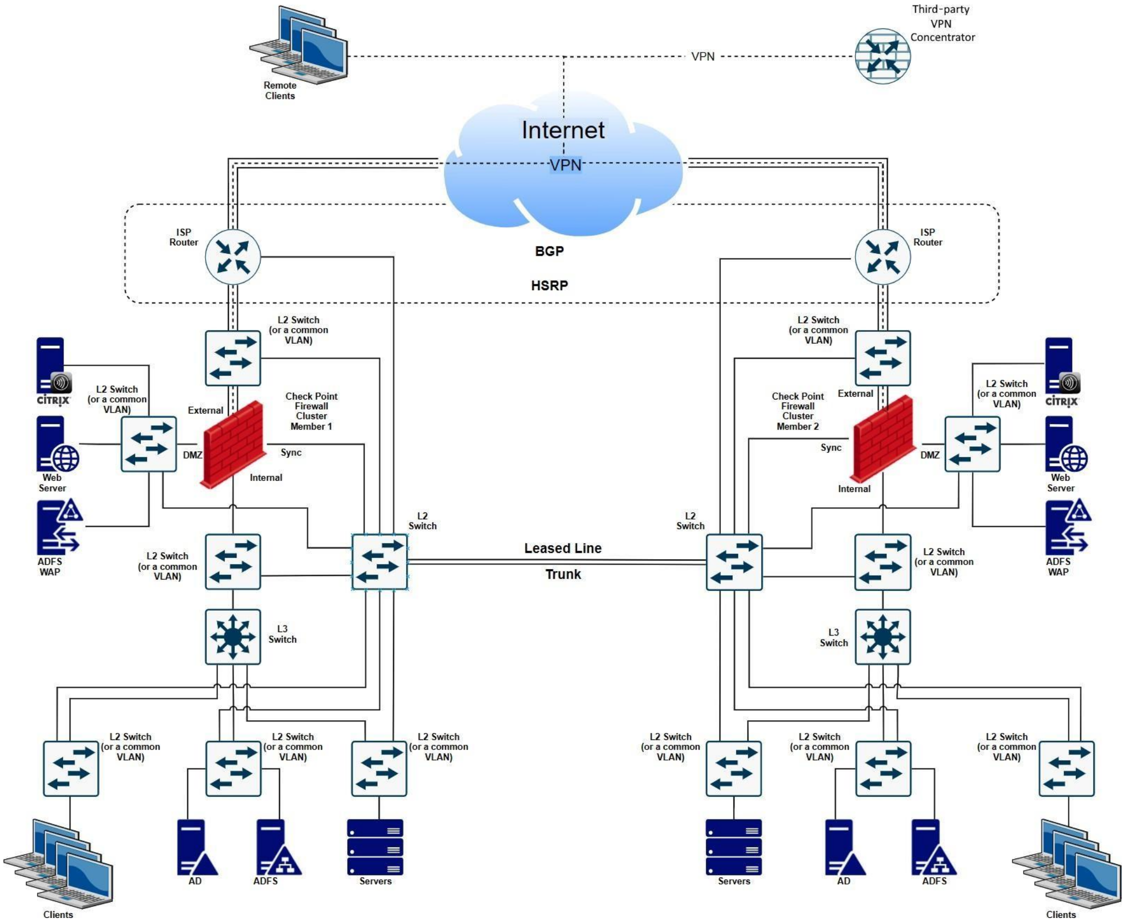

Remote Clients
VPN
Internet
VPN
Third-party VPN Concentrator
ISP Router
CITRIX
L2 Switch (or a common VLAN)
External
Router
Peer or a third-party service provider
Web Server
DMZ-1
DMZ-2
Internal
ADFS WAP
L2 Switch (or a common VLAN)
Clients
Servers
AD
ADFS

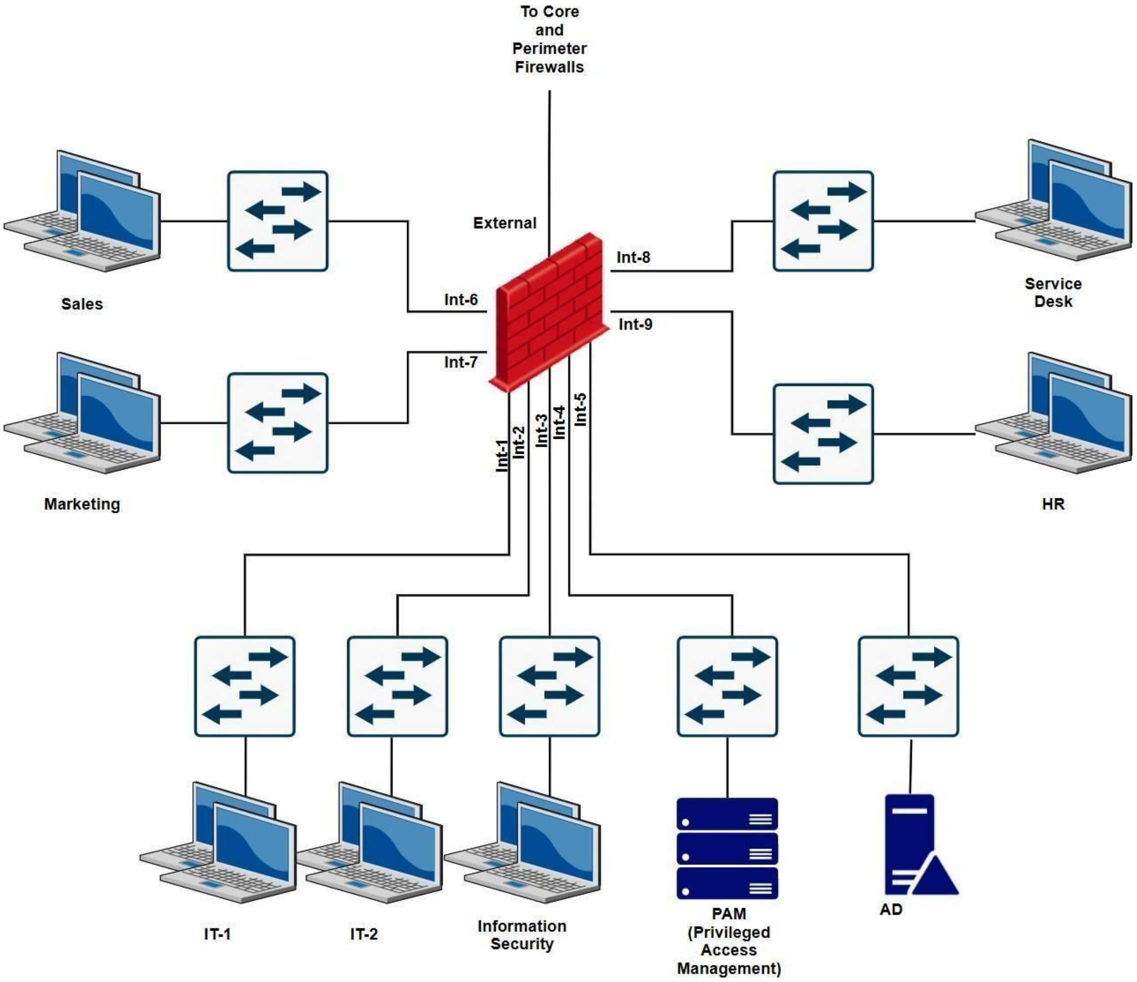

Internet
Remote Clients
VPN
VPN
Third-party VPN Concentrator
ISP Router
Router
Peer or a third-party service provider
External
DMZ-3
ADFS WAP
DMZ-1
DMZ-2
DMZ-4
Internal
Web Server
CITRIX
L2 Switch (or a common VLAN)
Clients
Servers
AD
ADFS

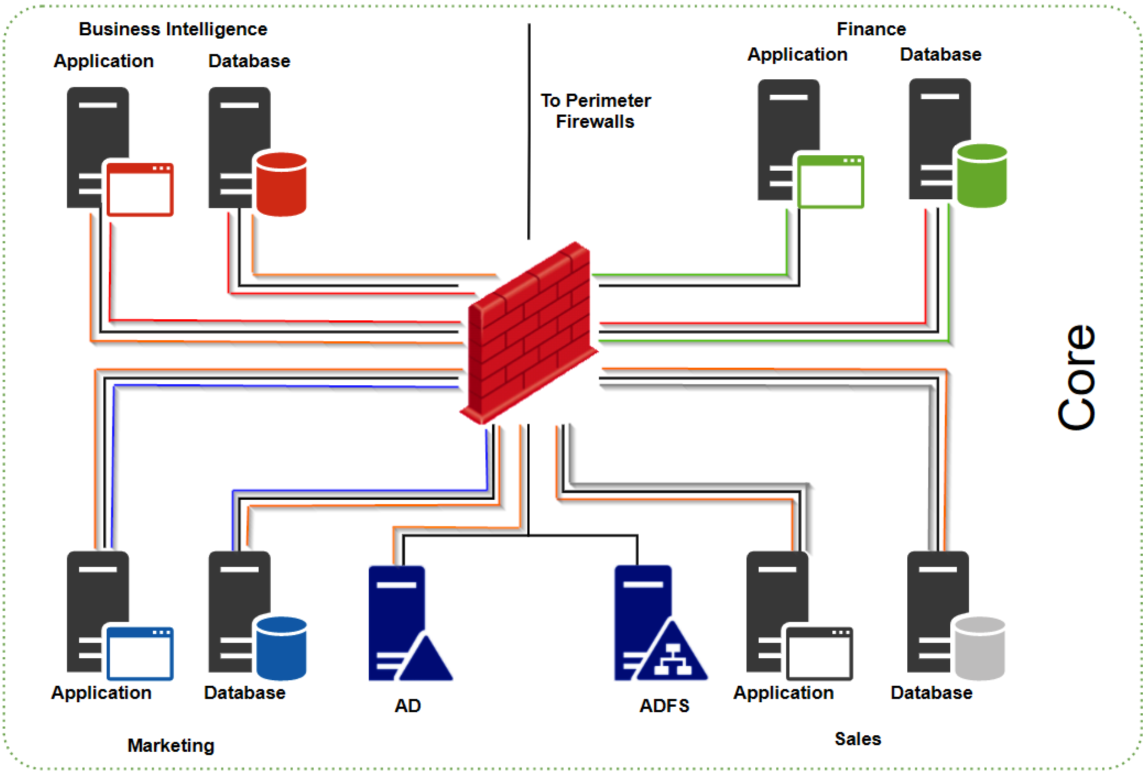

Third-party
VPN
Concentrator
VPN
Remote
Clients
Internet
VPN
ISP
Router
ISP
Router
External
Check
Point
Firewall
DMZ
Internal
L2 Switch
(or a common VLAN)
Web
Server
ADFS
WAP
L3
Switch
Router
Leased Line
Router
L3
Switch
External
Check
Point
Firewall
DMZ
Internal
L2 Switch
(or a common VLAN)
Web
Server
ADFS
WAP
L2 Switch
(or a common
VLAN)
L2 Switch
(or a common
VLAN)
L2 Switch
(or a common
VLAN)
L2 Switch
(or a common
VLAN)
L2 Switch
(or a common
VLAN)
L2 Switch
(or a common
VLAN)
Clients
AD
ADFS
Servers
Servers
AD
ADFS
Clients

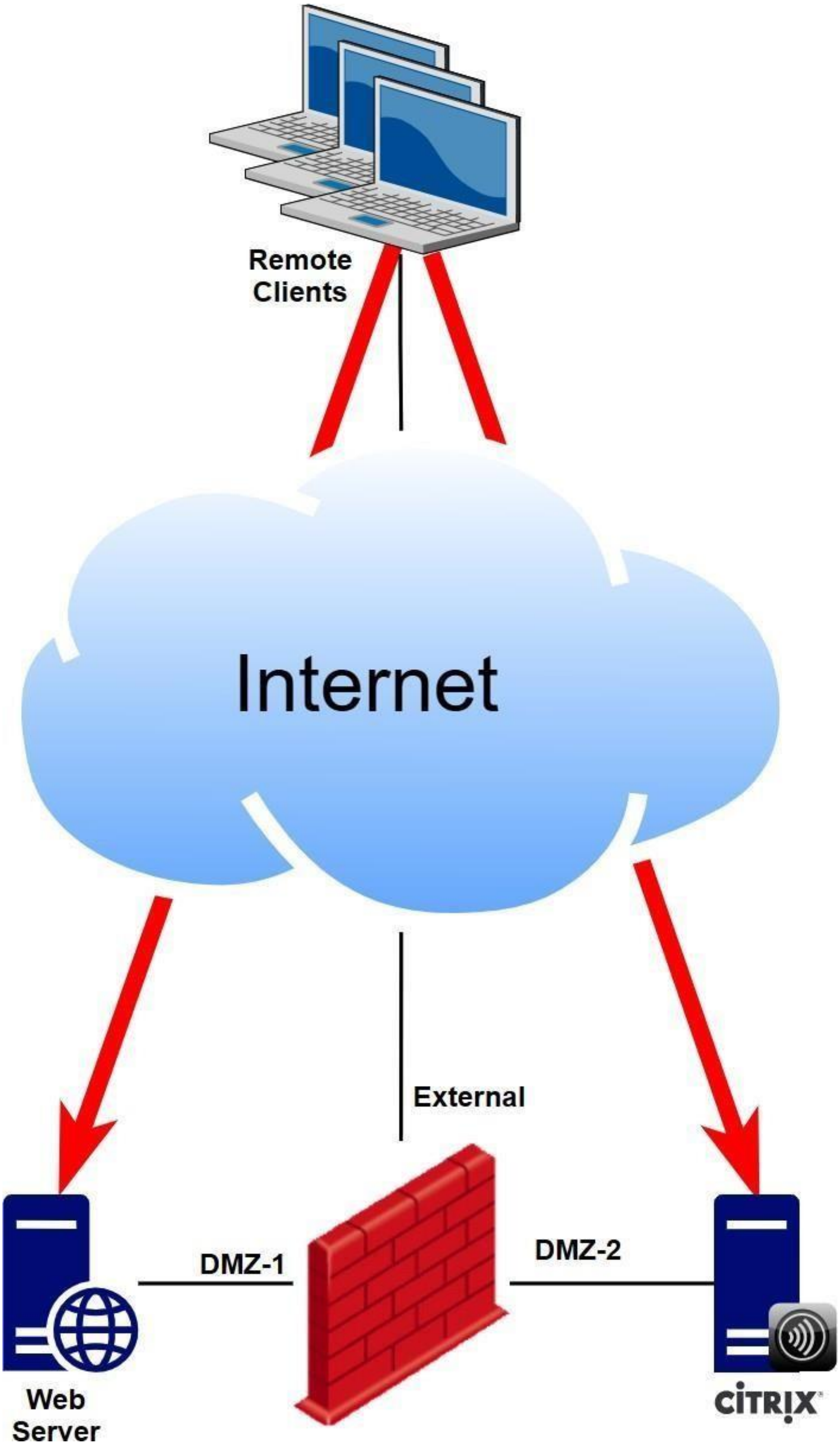

Third-party
VPN
Concentrator
Remote
Clients
VPN
Internet
VPN
ISP
Router
Router
Peer or a third-party
service provider
External
DMZ-3
ADFS
WAP
DMZ-1
DMZ-4
DMZ-2
Int-3
Int-2
Int-1
Web
Server
citrix
L2 Switch
(or a common
VLAN)
L2 Switch
(or a common
VLAN)
L2 Switch
(or a common
VLAN)
Clients
Servers
AD
ADFS

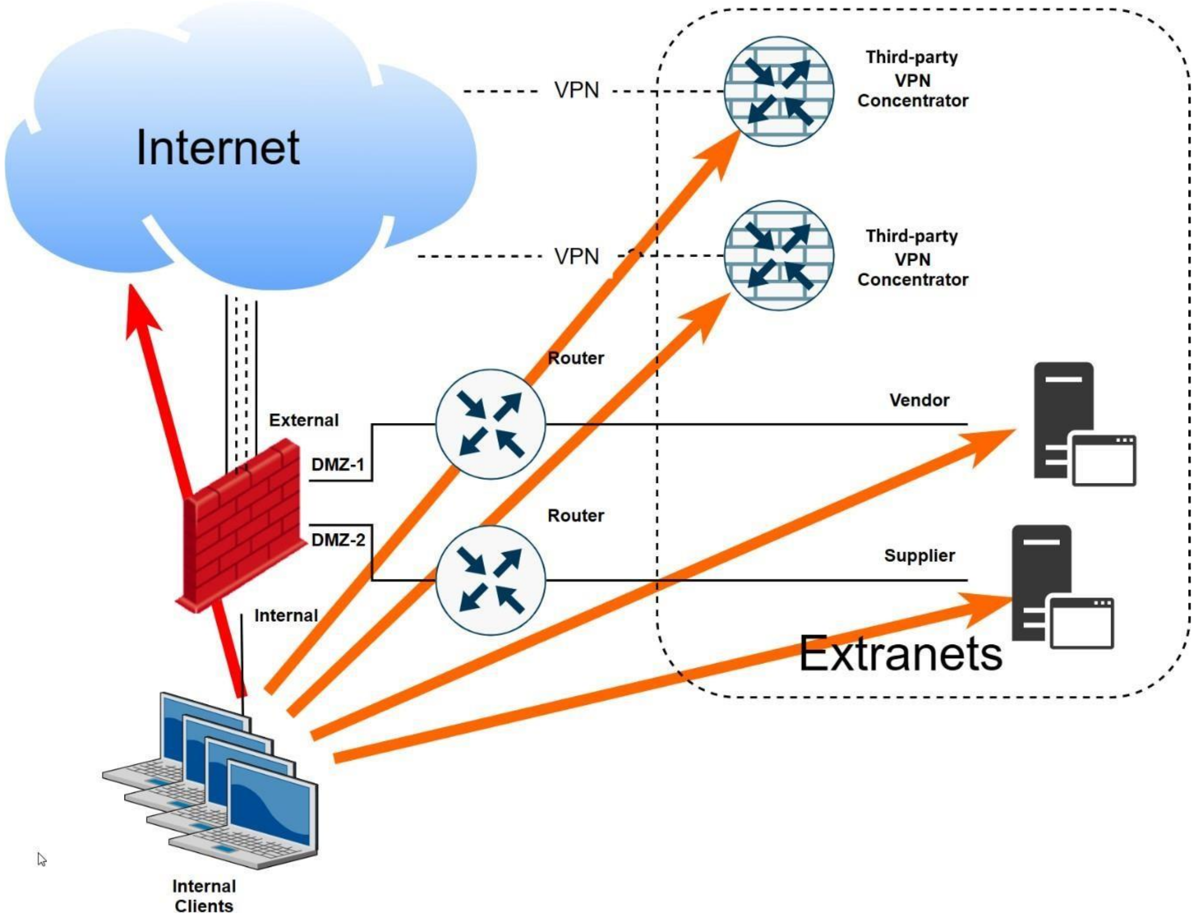

Remote Clients
VPN
Third-party VPN Concentrator
Internet
VPN
ISP Router
ISP Router
L2 Switch (or a common VLAN)
CITRIX
Web Server
ADFS WAP
DMZ
External
Check Point Firewall
Internal
Non-Check Point VPN Concentrator
Non-Check Point VPN Concentrator
External
Check Point Firewall
DMZ
Internal
L2 Switch (or a common VLAN)
CITRIX
Web Server
ADFS WAP
L3 Switch
Router
MPLS
Router
L3 Switch
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
Clients
AD
ADFS
Servers
Servers
AD
ADFS
Clients

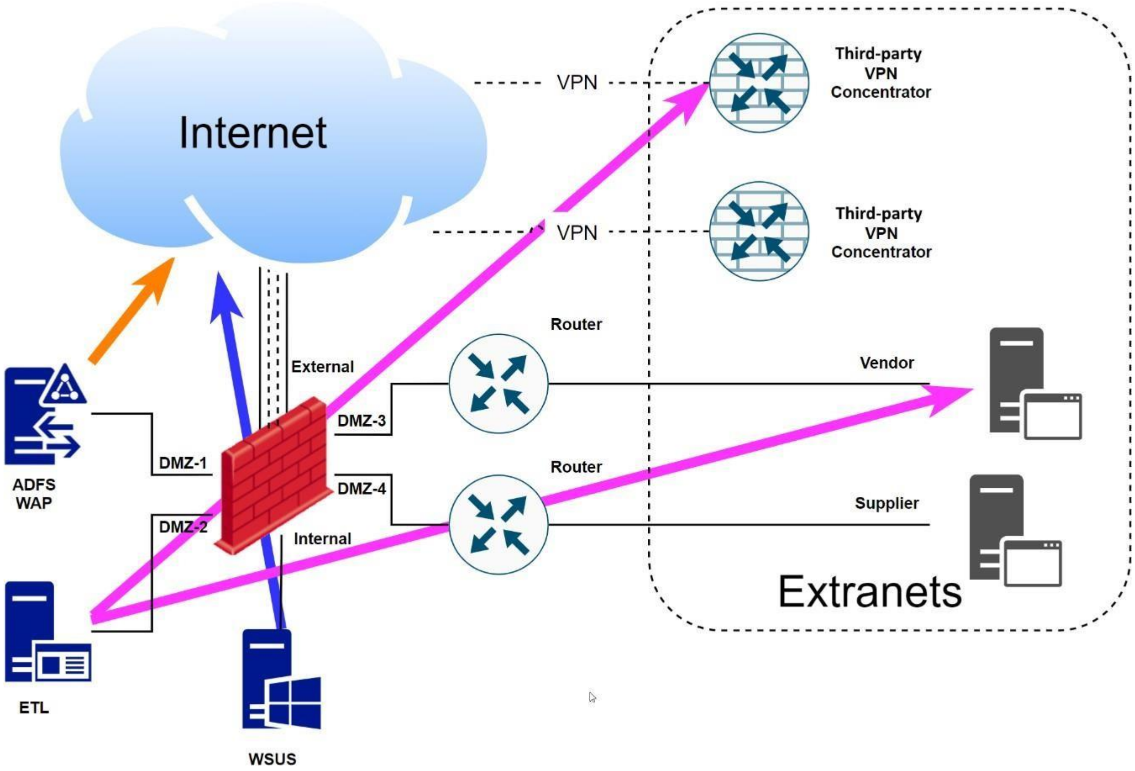

Remote Clients
VPN
Third-party VPN Concentrator
Internet
VPN
ISP Router
BGP
HSRP
ISP Router
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
Check Point Firewall Cluster Member 1
External
DMZ
Sync
Internal
Check Point Firewall Cluster Member 2
External
Sync
DMZ
Internal
L2 Switch (or a common VLAN)
CITRIX
Web Server
ADFS WAP
CITRIX
Web Server
ADFS WAP
L2 Switch
L2 Switch
Leased Line
Trunk
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L3 Switch
L3 Switch
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
L2 Switch (or a common VLAN)
Clients
AD
ADFS
Servers
Servers
AD
ADFS
Clients

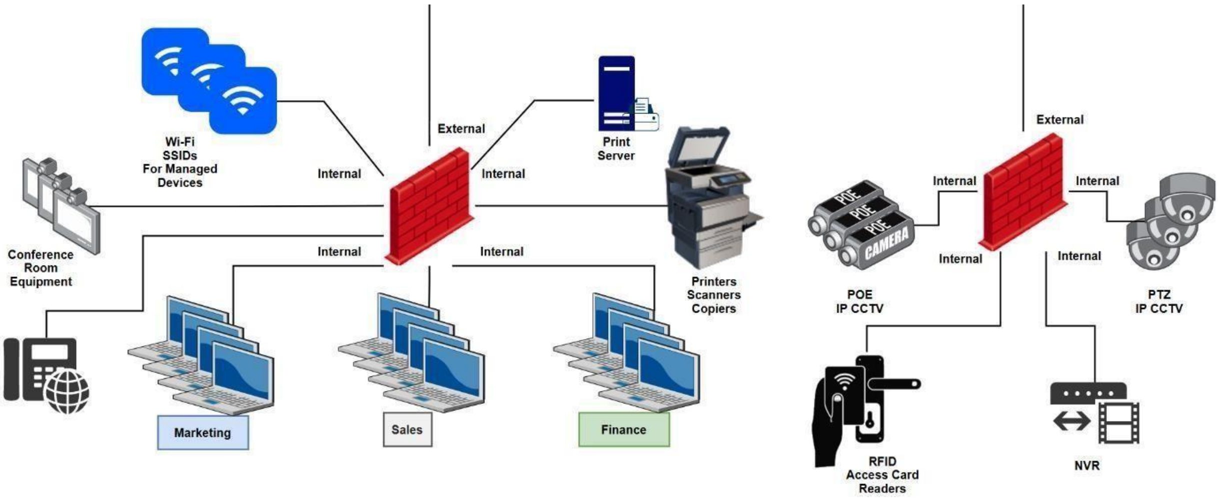

To Core and Perimeter Firewalls
External
Sales
Int-6
Int-7
Marketing
Int-8
Service Desk
Int-9
HR
Int-1
Int-2
Int-3
Int-4
Int-5
IT-1
IT-2
Information Security
PAM (Privileged Access Management)
AD

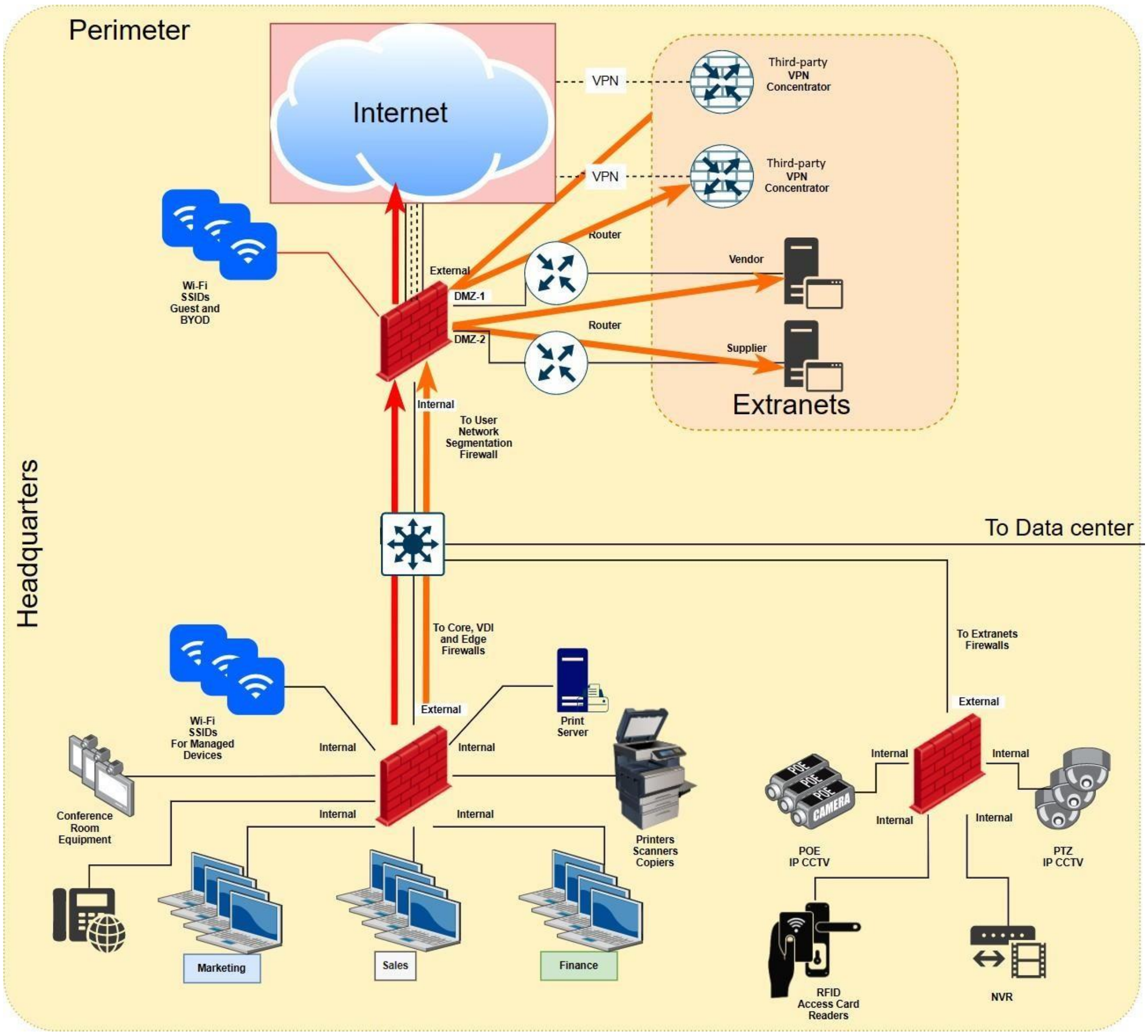

Business Intelligence
Application
Database
To Perimeter Firewalls
Finance
Application
Database
Core
Application
Database
AD
ADFS
Application
Database
Marketing
Sales

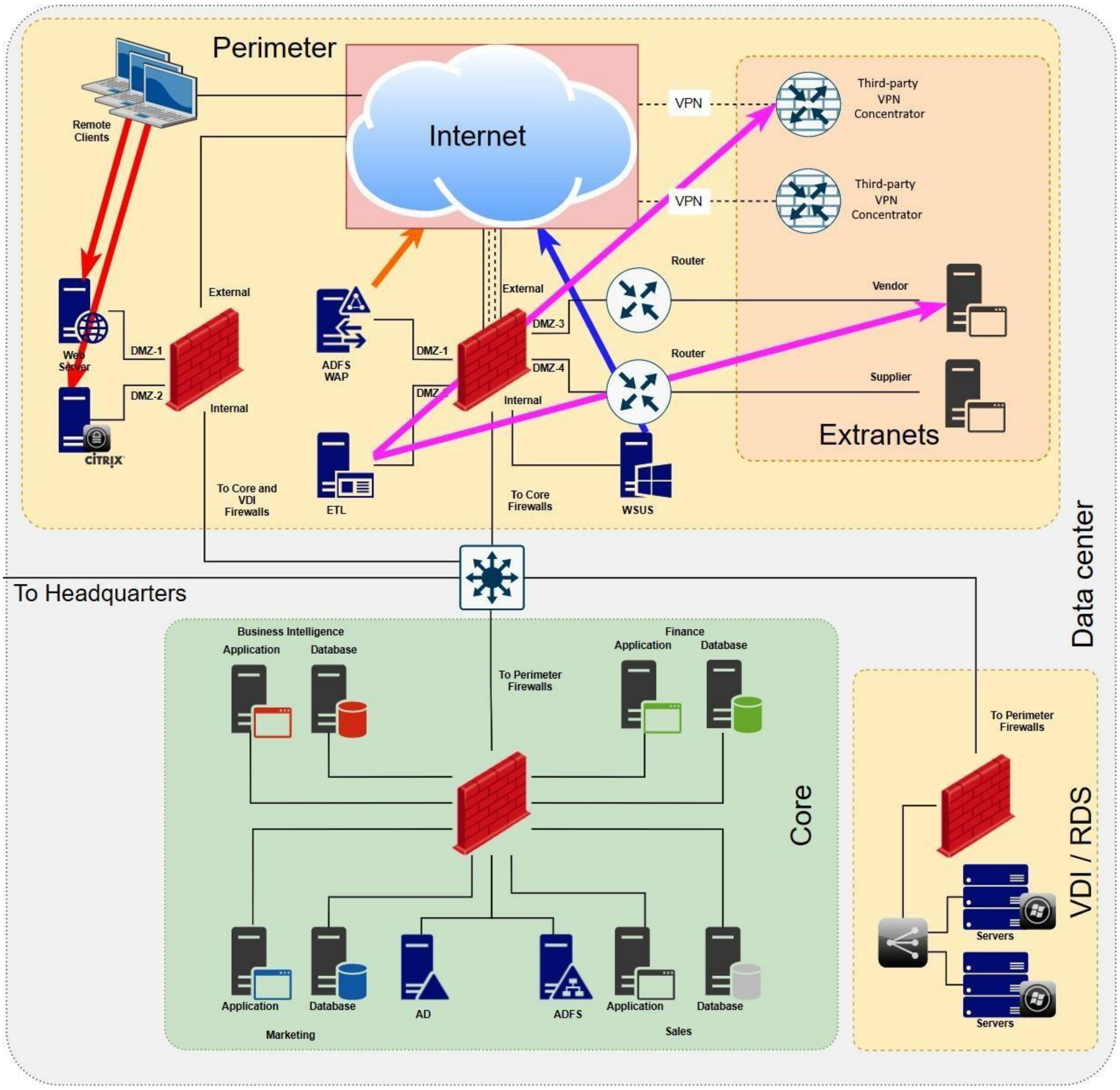

Remote
Clients
Internet
External
DMZ-1
DMZ-2
Web
Server
CiTRiX

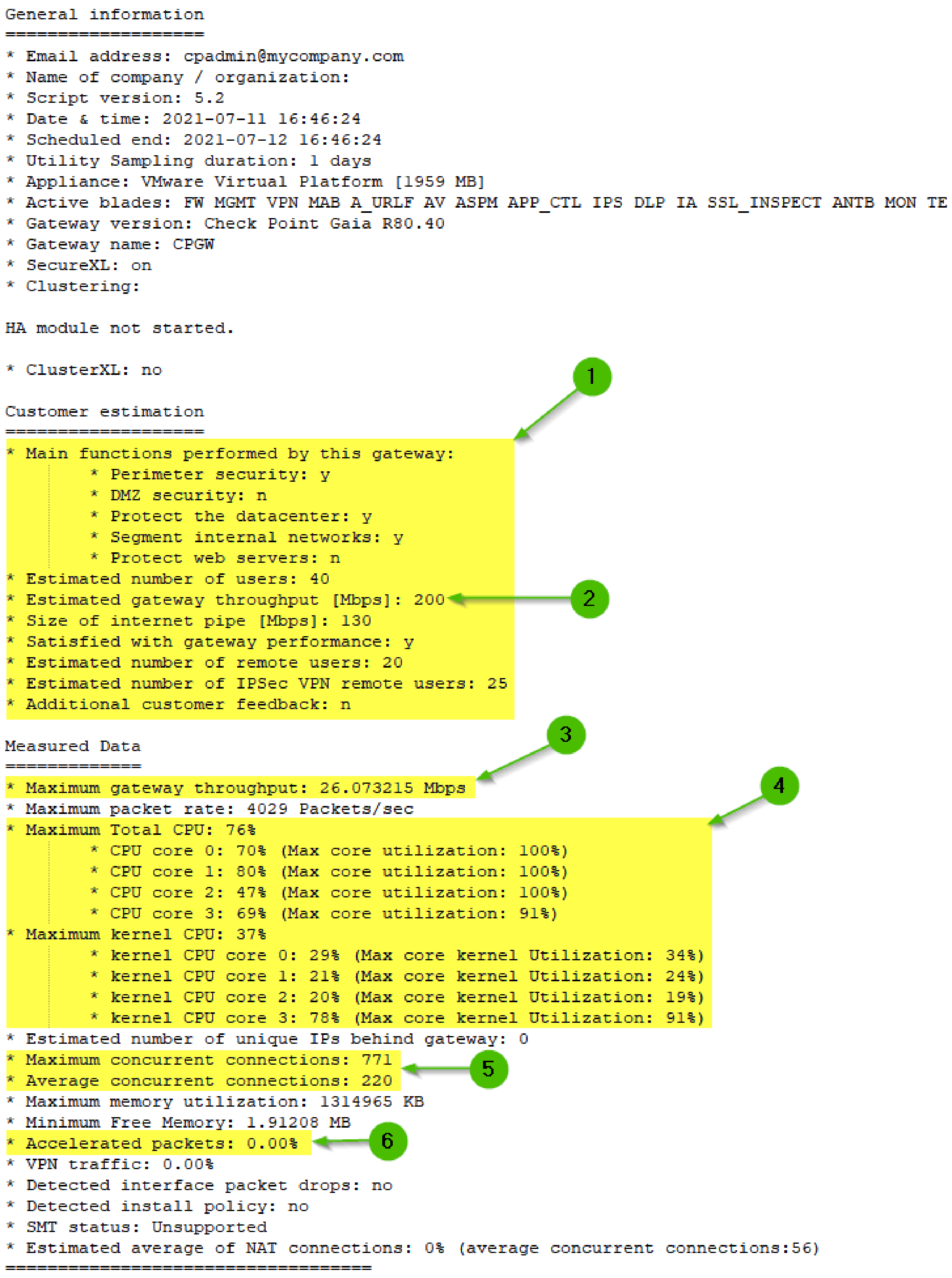

Internet
VPN
Third-party VPN Concentrator
VPN
Third-party VPN Concentrator
Router
External
DMZ-1
Vendor
Router
DMZ-2
Supplier
Internal
Extranets
Internal Clients


Internet
VPN
Third-party VPN Concentrator
VPN
Third-party VPN Concentrator
Router
External
Vendor
DMZ-3
ADFS WAP
DMZ-1
Router
DMZ-4
Supplier
DMZ-2
Internal
Extranets
ETL
WSUS

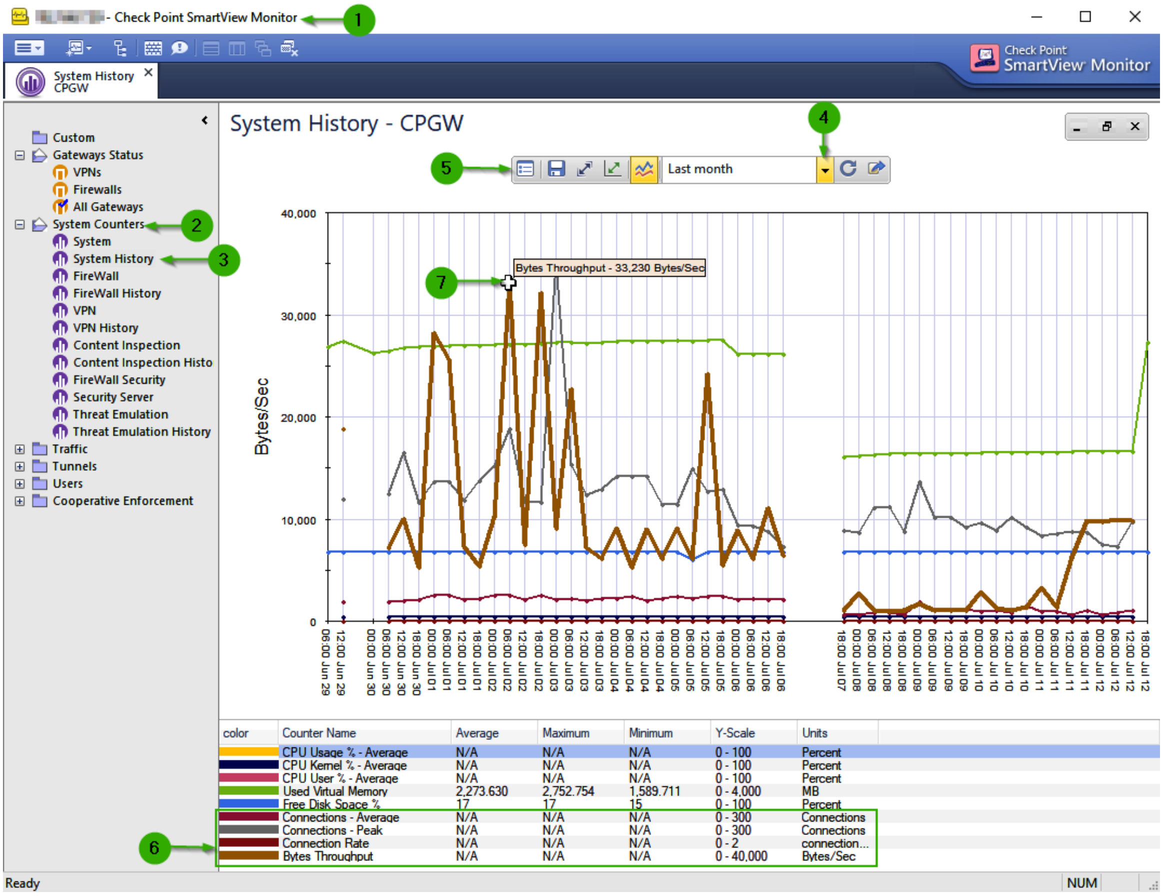

Wi-Fi SSIDs For Managed Devices
External
Internal
Internal
Print Server
Conference Room Equipment
Internal
Internal
Printers Scanners Copiers
Marketing
Sales
Finance
External
Internal
Internal
POE
POE
POE
CAMERA
POE IP CCTV
Internal
Internal
PTZ IP CCTV
RFID Access Card Readers
NVR


Perimeter
Internet
VPN
VPN
Third-party VPN Concentrator
Third-party VPN Concentrator
Router
Vendor
Router
Supplier
Extranets
Wi-Fi SSIDs Guest and BYOD
External
DMZ-1
DMZ-2
Internal
To User Network Segmentation Firewall
Headquarters
To Data center
To Core, VDI and Edge Firewalls
To Extranets Firewalls
Wi-Fi SSIDs For Managed Devices
External
Internal
Internal
Print Server
Conference Room Equipment
Internal
Internal
Printers Scanners Copiers
Marketing
Sales
Finance
External
Internal
Internal
POE
POE
POE
CAMERA
POE IP CCTV
Internal
Internal
PTZ IP CCTV
RFID Access Card Readers
NVR

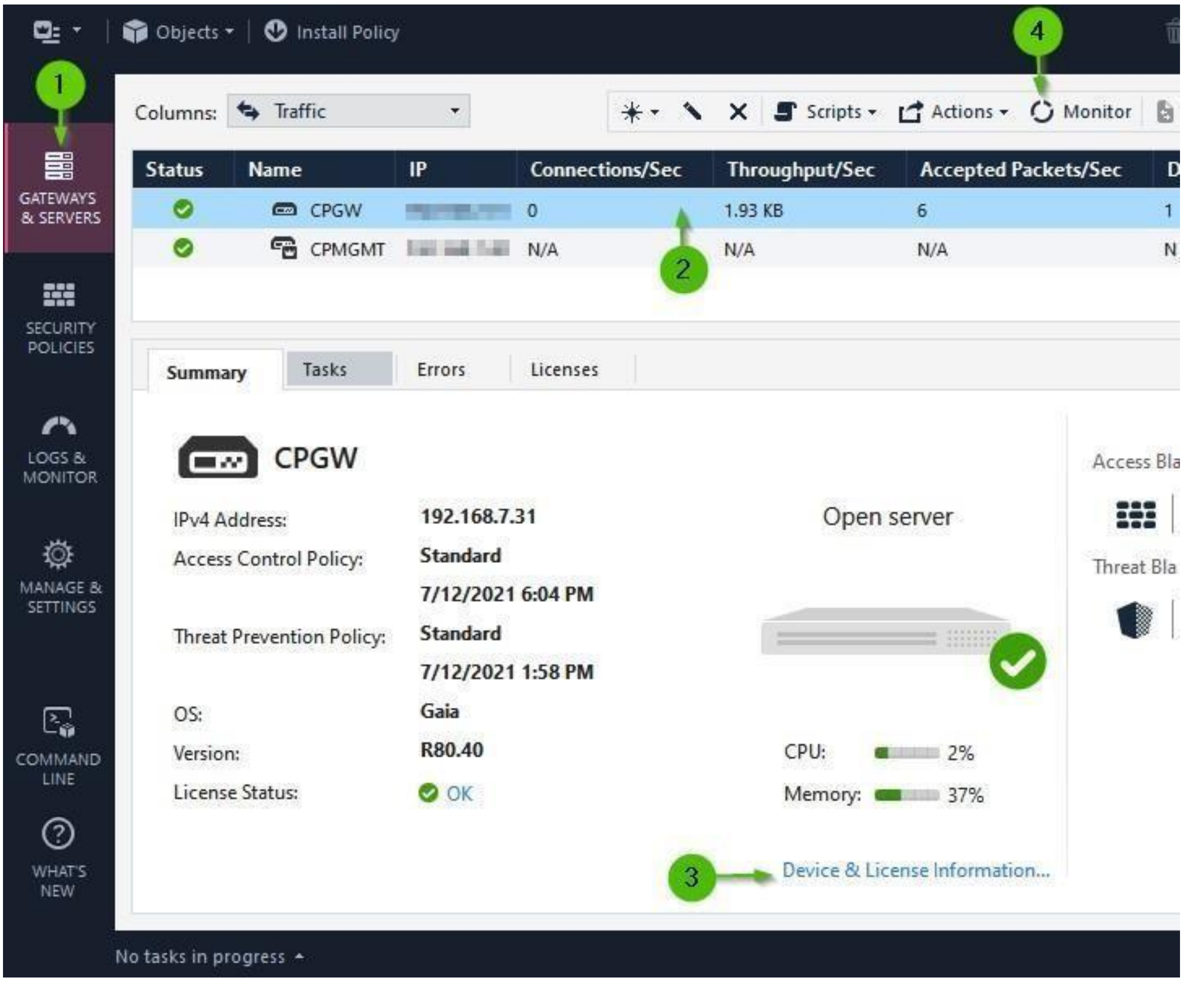

Perimeter
Internet
Remote Clients
VPN
Third-party VPN Concentrator
VPN
Third-party VPN Concentrator
External
Web Server
DMZ-1
DMZ-2
Internal
CITRIX
ADFS WAP
DMZ-1
DMZ-2
External
DMZ-3
DMZ-4
Internal
Router
Vendor
Router
Supplier
Extranets
ETL
WSUS
To Core and VDI Firewalls
To Core Firewalls
To Headquarters
Data center
Business Intelligence
Application
Database
Finance
Application
Database
To Perimeter Firewalls
Core
To Perimeter Firewalls
VDI / RDS
Servers
Servers
Application
Database
Marketing
AD
ADFS
Application
Database
Sales



```
General information
===================
* Email address: cpadmin@mycompany.com
* Name of company / organization:
* Script version: 5.2
* Date & time: 2021-07-11 16:46:24
* Scheduled end: 2021-07-12 16:46:24
* Utility Sampling duration: 1 days
* Appliance: VMware Virtual Platform [1959 MB]
* Active blades: FW MGMT VPN MAB A_URLF AV ASPM APP_CTL IPS DLP IA SSL_INSPECT ANTB MON TE
* Gateway version: Check Point Gaia R80.40
* Gateway name: CPGW
* SecureXL: on
* Clustering:

HA module not started.

* ClusterXL: no

Customer estimation
===================
* Main functions performed by this gateway:
        * Perimeter security: y
        * DMZ security: n
        * Protect the datacenter: y
        * Segment internal networks: y
        * Protect web servers: n
* Estimated number of users: 40
* Estimated gateway throughput [Mbps]: 200
* Size of internet pipe [Mbps]: 130
* Satisfied with gateway performance: y
* Estimated number of remote users: 20
* Estimated number of IPSec VPN remote users: 25
* Additional customer feedback: n

Measured Data
=============
* Maximum gateway throughput: 26.073215 Mbps
* Maximum packet rate: 4029 Packets/sec
* Maximum Total CPU: 76%
        * CPU core 0: 70% (Max core utilization: 100%)
        * CPU core 1: 80% (Max core utilization: 100%)
        * CPU core 2: 47% (Max core utilization: 100%)
        * CPU core 3: 69% (Max core utilization: 91%)
* Maximum kernel CPU: 37%
        * kernel CPU core 0: 29% (Max core kernel Utilization: 34%)
        * kernel CPU core 1: 21% (Max core kernel Utilization: 24%)
        * kernel CPU core 2: 20% (Max core kernel Utilization: 19%)
        * kernel CPU core 3: 78% (Max core kernel Utilization: 91%)
* Estimated number of unique IPs behind gateway: 0
* Maximum concurrent connections: 771
* Average concurrent connections: 220
* Maximum memory utilization: 1314965 KB
* Minimum Free Memory: 1.91208 MB
* Accelerated packets: 0.00%
* VPN traffic: 0.00%
* Detected interface packet drops: no
* Detected install policy: no
* SMT status: Unsupported
* Estimated average of NAT connections: 0% (average concurrent connections:56)
===================================
```



color	Counter Name	Average	Maximum	Minimum	Y-Scale	Units
🟨	CPU Usage % - Average	N/A	N/A	N/A	0 - 100	Percent
■	CPU Kernel % - Average	N/A	N/A	N/A	0 - 100	Percent
🟥	CPU User % - Average	N/A	N/A	N/A	0 - 100	Percent
🟩	Used Virtual Memory	2,273.630	2,752.754	1,589.711	0 - 4,000	MB
🟦	Free Disk Space %	17	17	15	0 - 100	Percent
🟥	Connections - Average	N/A	N/A	N/A	0 - 300	Connections
■	Connections - Peak	N/A	N/A	N/A	0 - 300	Connections
🟥	Connection Rate	N/A	N/A	N/A	0 - 2	connection...
🟫	Bytes Throughput	N/A	N/A	N/A	0 - 40,000	Bytes/Sec



Status	Name	IP	Connections/Sec	Throughput/Sec	Accepted Packets/Sec	D
✓	CPGW	[redacted]	0	1.93 KB	6	1
✓	CPMGMT	[redacted]	N/A	N/A	N/A	N

CPGW

IPv4 Address: 192.168.7.31

Access Control Policy: Standard
7/12/2021 6:04 PM

Threat Prevention Policy: Standard
7/12/2021 1:58 PM

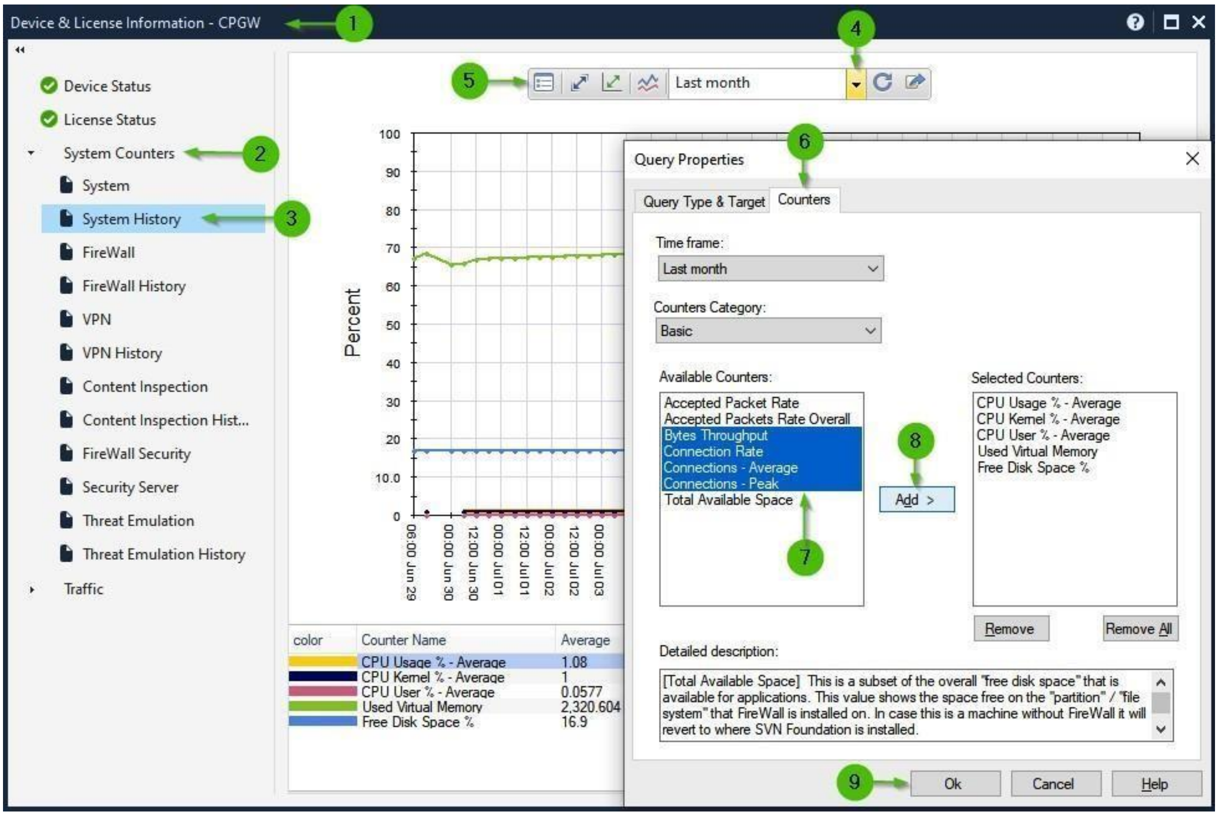
OS: Gaia

Version: R80.40

License Status: ✓ OK

CPU: 2%

Memory: 37%



color	Counter Name	Average
🟨	CPU Usage % - Average	1.08
⬛	CPU Kernel % - Average	1
🟥	CPU User % - Average	0.0577
🟩	Used Virtual Memory	2,320.604
🟦	Free Disk Space %	16.9

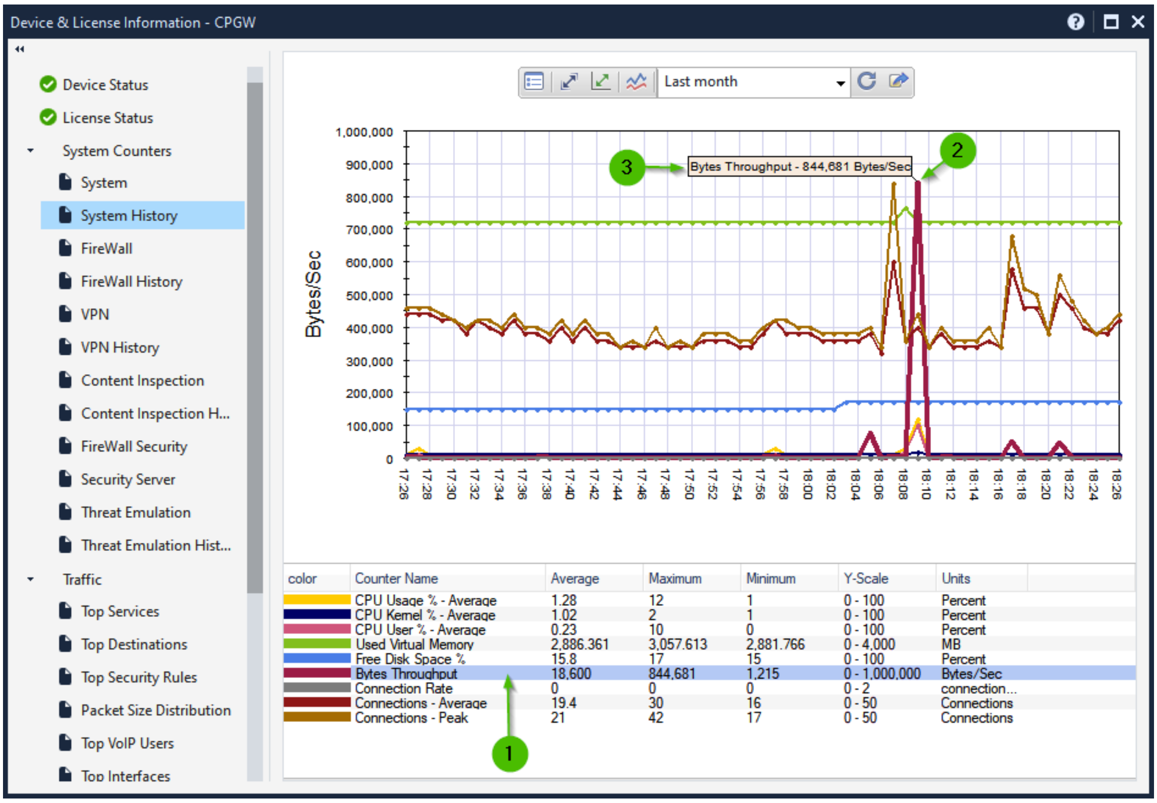
Time frame: Last month

Counters Category: Basic

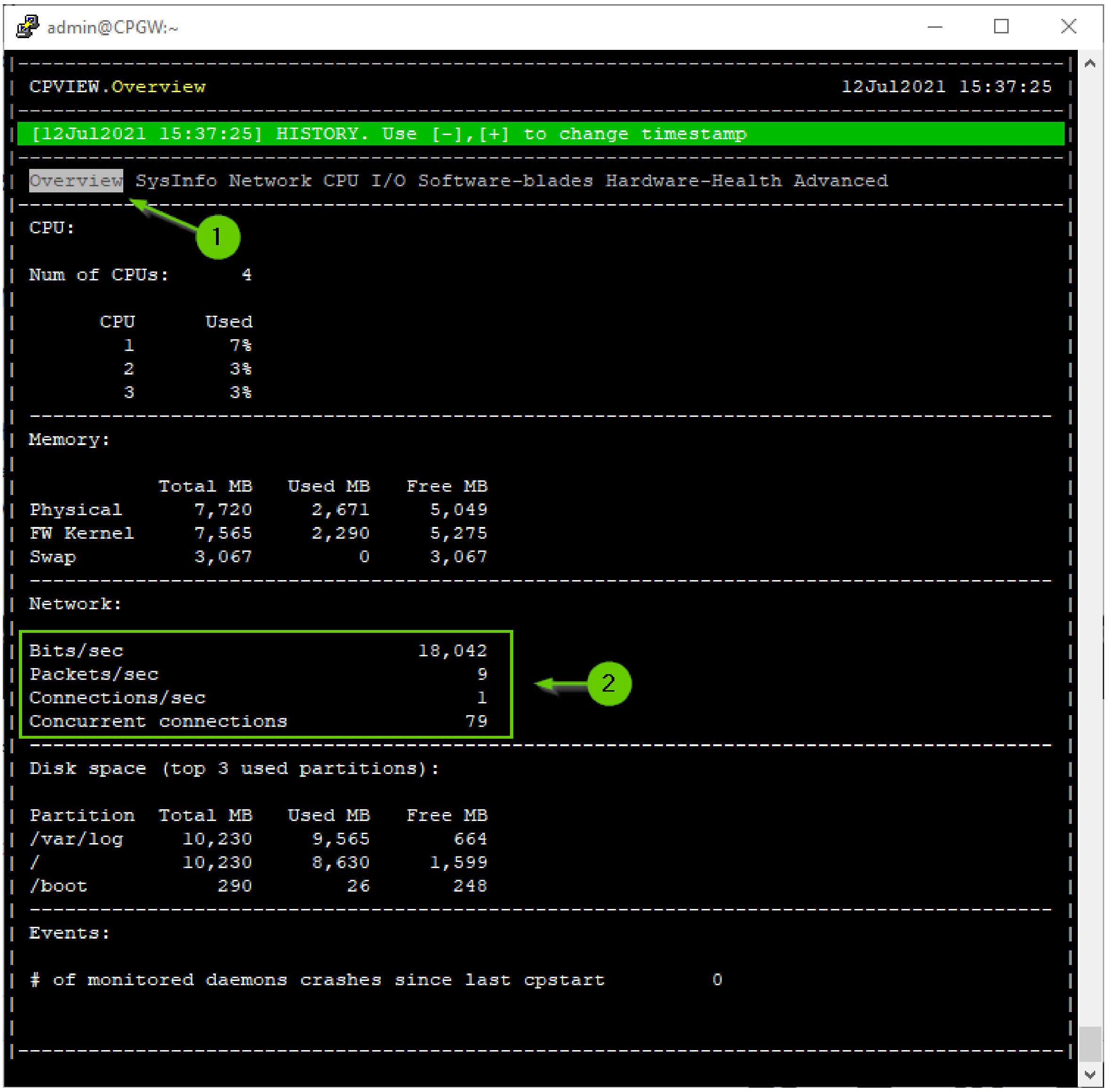
Available Counters:
Accepted Packet Rate
Accepted Packets Rate Overall
Bytes Throughput
Connection Rate
Connections - Average
Connections - Peak
Total Available Space

Selected Counters:
CPU Usage % - Average
CPU Kernel % - Average
CPU User % - Average
Used Virtual Memory
Free Disk Space %

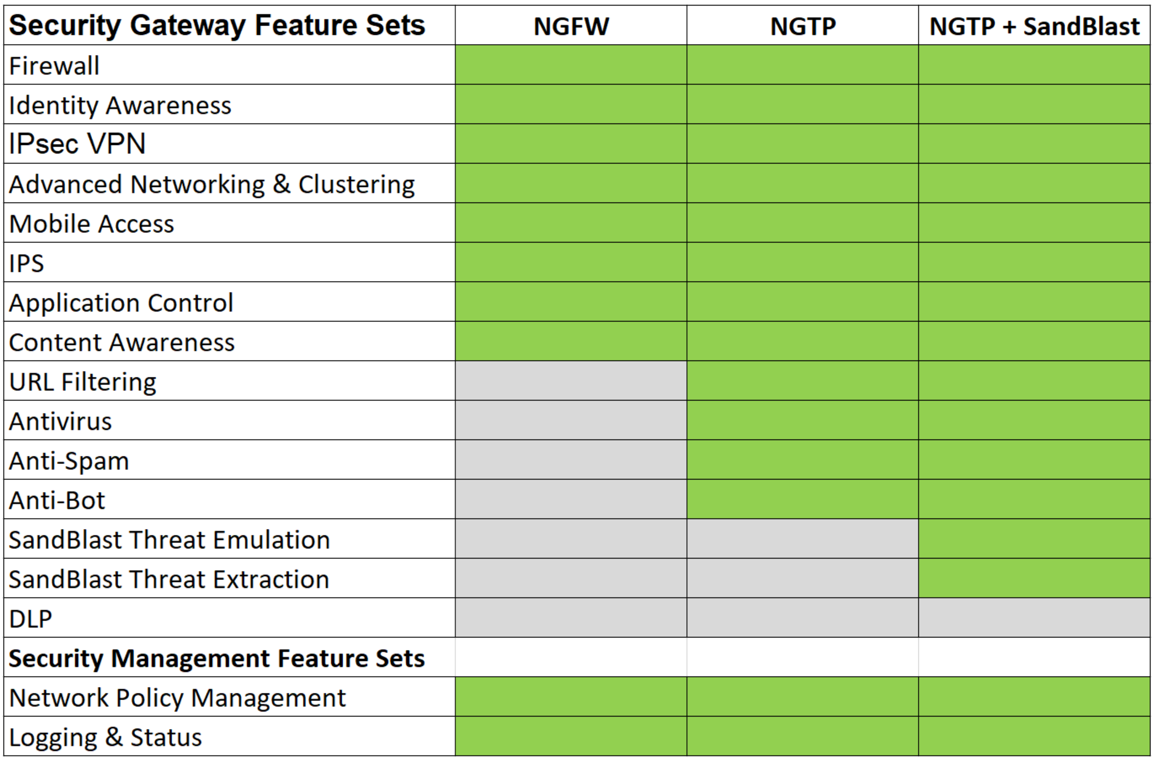
Detailed description:
[Total Available Space] This is a subset of the overall "free disk space" that is available for applications. This value shows the space free on the "partition" / "file system" that FireWall is installed on. In case this is a machine without FireWall it will revert to where SVN Foundation is installed.



color	Counter Name	Average	Maximum	Minimum	Y-Scale	Units
🟨	CPU Usage % - Average	1.28	12	1	0 - 100	Percent
⬛	CPU Kernel % - Average	1.02	2	1	0 - 100	Percent
🟥	CPU User % - Average	0.23	10	0	0 - 100	Percent
🟩	Used Virtual Memory	2,886.361	3,057.613	2,881.766	0 - 4,000	MB
🟦	Free Disk Space %	15.8	17	15	0 - 100	Percent
🟥	Bytes Throughput	18,600	844,681	1,215	0 - 1,000,000	Bytes/Sec
⬜	Connection Rate	0	0	0	0 - 2	connection...
🟥	Connections - Average	19.4	30	16	0 - 50	Connections
🟫	Connections - Peak	21	42	17	0 - 50	Connections



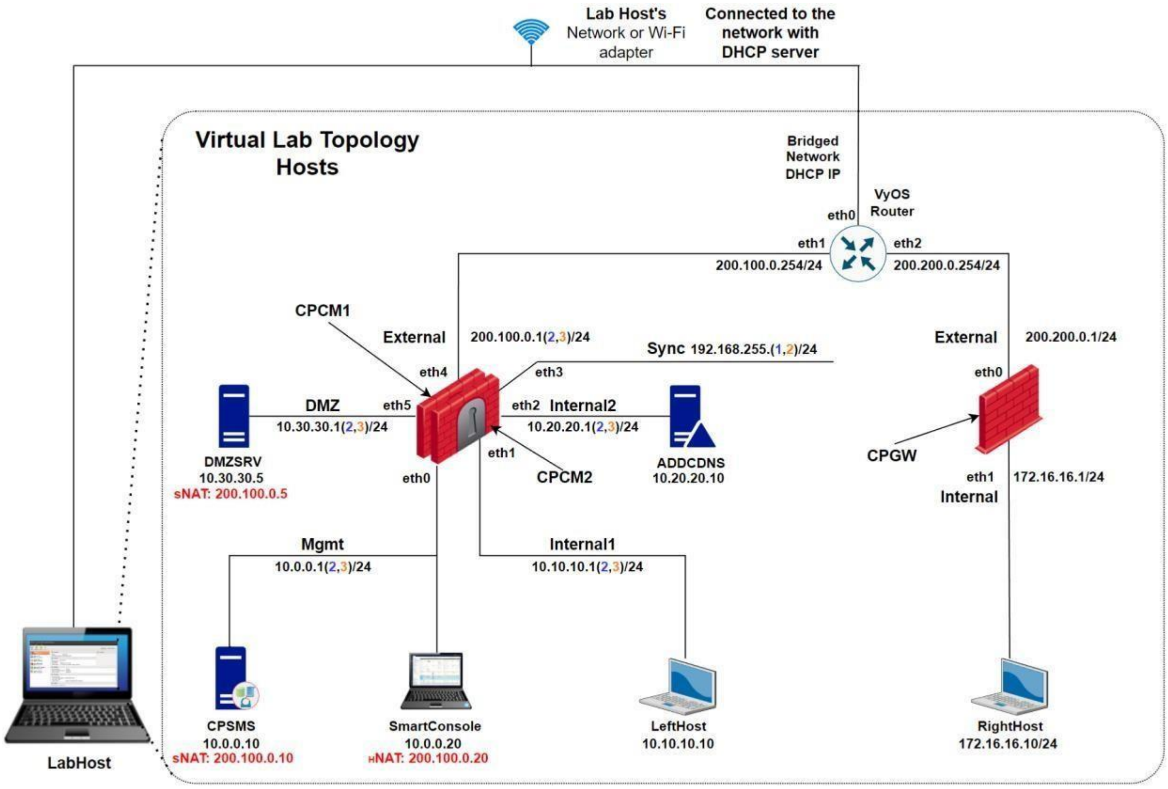
```
|-------------------------------------------------------------------------------------------|
| CPVIEW.Overview                                                      12Jul2021 15:37:25 |
|-------------------------------------------------------------------------------------------|
| [12Jul2021 15:37:25] HISTORY. Use [-],[+] to change timestamp                             |
|-------------------------------------------------------------------------------------------|
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced                 |
|-------------------------------------------------------------------------------------------|
| CPU:                                                                                      |
|                                                                                           |
| Num of CPUs:        4                                                                     |
|                                                                                           |
|       CPU       Used                                                                     |
|         1         7%                                                                     |
|         2         3%                                                                     |
|         3         3%                                                                     |
| ----------------------------------------------------------------------------------------- |
| Memory:                                                                                   |
|                                                                                           |
|            Total MB   Used MB    Free MB                                                  |
| Physical      7,720     2,671      5,049                                                  |
| FW Kernel     7,565     2,290      5,275                                                  |
| Swap          3,067         0      3,067                                                  |
| ----------------------------------------------------------------------------------------- |
| Network:                                                                                  |
|                                                                                           |
| Bits/sec                               18,042                                             |
| Packets/sec                                 9                                             |
| Connections/sec                             1                                             |
| Concurrent connections                     79                                             |
| ----------------------------------------------------------------------------------------- |
| Disk space (top 3 used partitions):                                                       |
|                                                                                           |
| Partition  Total MB   Used MB    Free MB                                                  |
| /var/log     10,230     9,565        664                                                  |
| /            10,230     8,630      1,599                                                  |
| /boot           290        26        248                                                  |
| ----------------------------------------------------------------------------------------- |
| Events:                                                                                   |
|                                                                                           |
| # of monitored daemons crashes since last cpstart         0                               |
|                                                                                           |
|                                                                                           |
|-------------------------------------------------------------------------------------------|
```

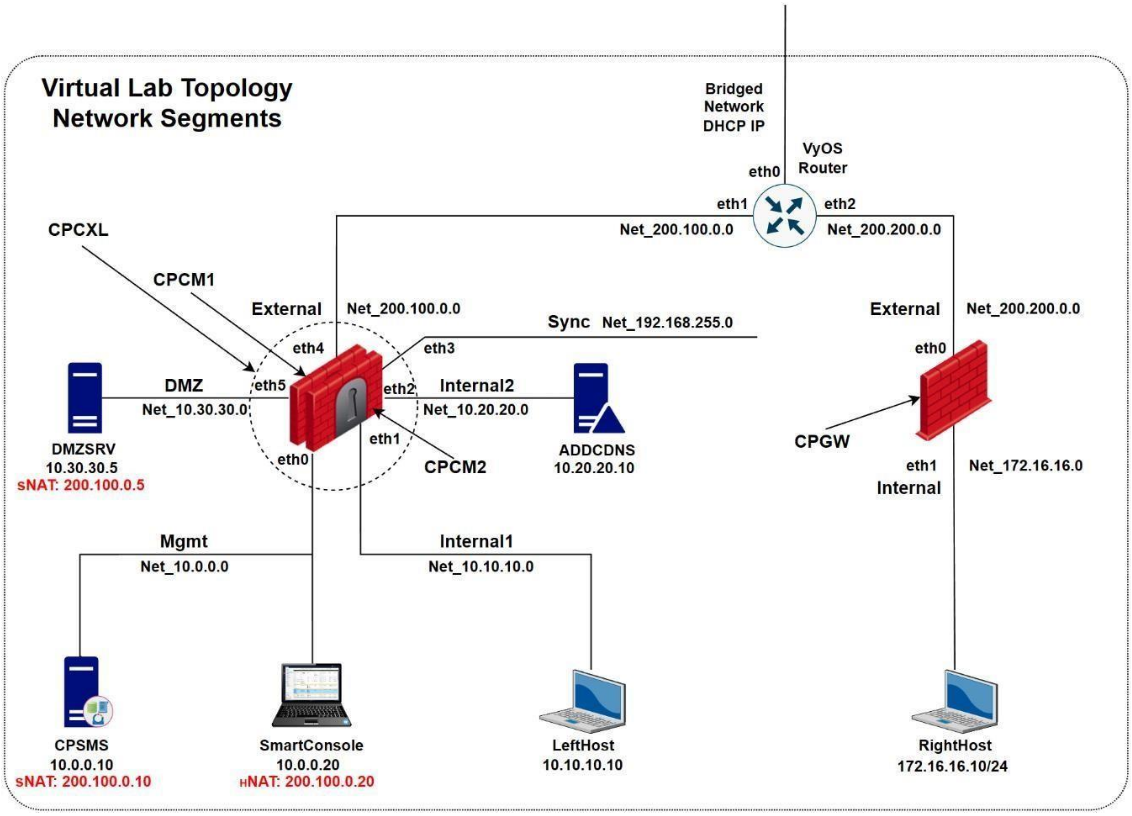


Security Gateway Feature Sets	NGFW	NGTP	NGTP + SandBlast
Firewall	🟩	🟩	🟩
Identity Awareness	🟩	🟩	🟩
IPsec VPN	🟩	🟩	🟩
Advanced Networking & Clustering	🟩	🟩	🟩
Mobile Access	🟩	🟩	🟩
IPS	🟩	🟩	🟩
Application Control	🟩	🟩	🟩
Content Awareness	🟩	🟩	🟩
URL Filtering	▨	🟩	🟩
Antivirus	▨	🟩	🟩
Anti-Spam	▨	🟩	🟩
Anti-Bot	▨	🟩	🟩
SandBlast Threat Emulation	▨	▨	🟩
SandBlast Threat Extraction	▨	▨	🟩
DLP	▨	▨	▨
Security Management Feature Sets			
Network Policy Management	🟩	🟩	🟩
Logging & Status	🟩	🟩	🟩

Chapter 3: Building a Check Point Lab Environment – Part 1

10.0.0.1(2,3)/24 = 10.0.0.1/24 Virtual IP of the Cluster's interface
10.0.0.2/24 IP of the Cluster Member 1 interface
10.0.0.3/24 IP of the Cluster Member 2 interface




Virtual Lab Topology
Network Segments
Bridged
Network
DHCP IP
VyOS
Router
eth0
eth1
eth2
Net_200.100.0.0
Net_200.200.0.0
CPCXL
CPCM1
External
Net_200.100.0.0
Sync
Net_192.168.255.0
External
Net_200.200.0.0
eth4
eth3
eth0
eth5
DMZ
Net_10.30.30.0
eth2
Internal2
Net_10.20.20.0
eth1
CPCM2
CPGW
eth0
DMZSRV
10.30.30.5
sNAT: 200.100.0.5
ADDCDNS
10.20.20.10
eth1
Net_172.16.16.0
Internal
Mgmt
Net_10.0.0.0
Internal1
Net_10.10.10.0
CPSMS
10.0.0.10
sNAT: 200.100.0.10
SmartConsole
10.0.0.20
HNAT: 200.100.0.20
LeftHost
10.10.10.10
RightHost
172.16.16.10/24

VyOS (Router)

Interface	IP	Description	Network
eth0	DHCP	Outside	Bridged Adapter
eth1	200.100.0.254	Left	Net_200.100.0.0
eth2	200.200.0.254	Right	Net_200.200.0.0

Cluster (Virtual IPs, CPCM1 and CPCM2)

Interface	Virtual IP	CPCM1	CPCM2	Description	Network
eth0	10.0.0.1	10.0.0.2	10.0.0.3	Mgmt	Net_10.0.0.0
eth1	10.10.10.1	10.10.10.2	10.10.10.3	Internal1	Net_10.10.10.0
eth2	10.20.20.1	10.20.20.2	10.20.20.3	Internal2	Net_10.20.20.0
eth3		192.168.255.1	192.168.255.2	Sync	Net_192.168.255.0
eth4	200.100.0.1	200.100.0.2	200.100.0.3	External	Net_200.100.0.0
eth5	10.30.30.1	10.30.30.2	10.30.30.3	DMZ	Net_10.30.30.0

Single Gateway (CPGW)

Interface	IP	Description	Network
eth0	200.200.0.1	External	Net_200.200.0.0
eth1	172.16.16.1	Internal	Net_172.16.16.0

Security Management Server (CPSMS)

Interface	IP	Network
Ethernet	10.0.0.10	Net_10.0.0.0

LeftHost

Interface	IP	Network
Ethernet	10.10.10.10	Net_10.10.10.0

ADDCDNS

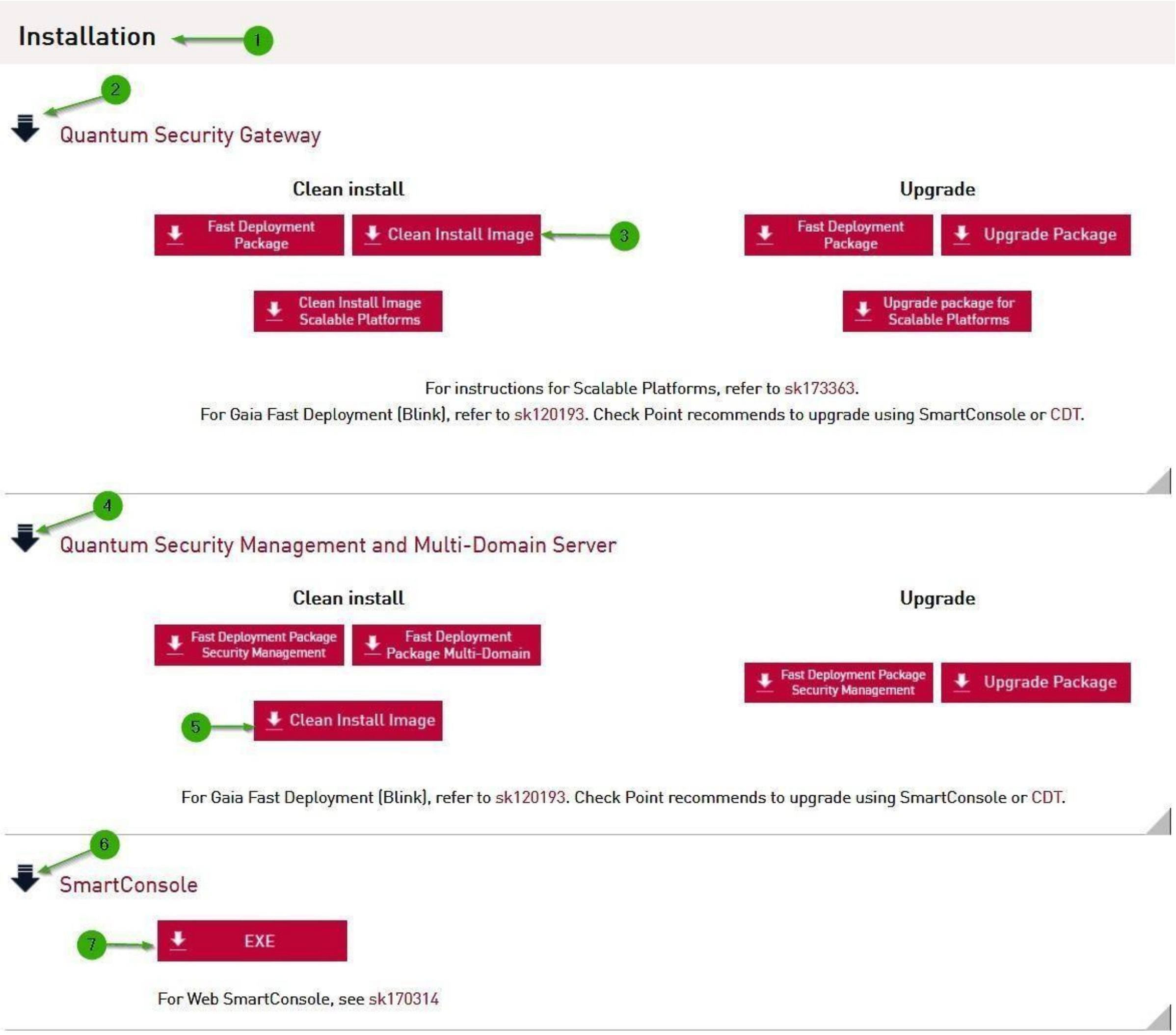
Interface	IP	Network
Ethernet	10.20.20.10	Net_10.20.20.0

DMZSRV

Interface	IP	Network
Ethernet	10.30.30.10	Net_10.30.30.0

RightHost

Interface	IP	Network
Ethernet	172.16.16.100	Net_172.16.16.0


1
2
3
4
5
6
7
Fast Deployment Package
Clean Install Image
Clean Install Image Scalable Platforms
Fast Deployment Package
Upgrade Package
Upgrade package for Scalable Platforms
Fast Deployment Package Security Management
Fast Deployment Package Multi-Domain
Clean Install Image
Fast Deployment Package Security Management
Upgrade Package
EXE

Installation

Quantum Security Gateway

Clean install

Upgrade

For instructions for Scalable Platforms, refer to sk173363.

For Gaia Fast Deployment (Blink), refer to sk120193. Check Point recommends to upgrade using SmartConsole or CDT.

Quantum Security Management and Multi-Domain Server

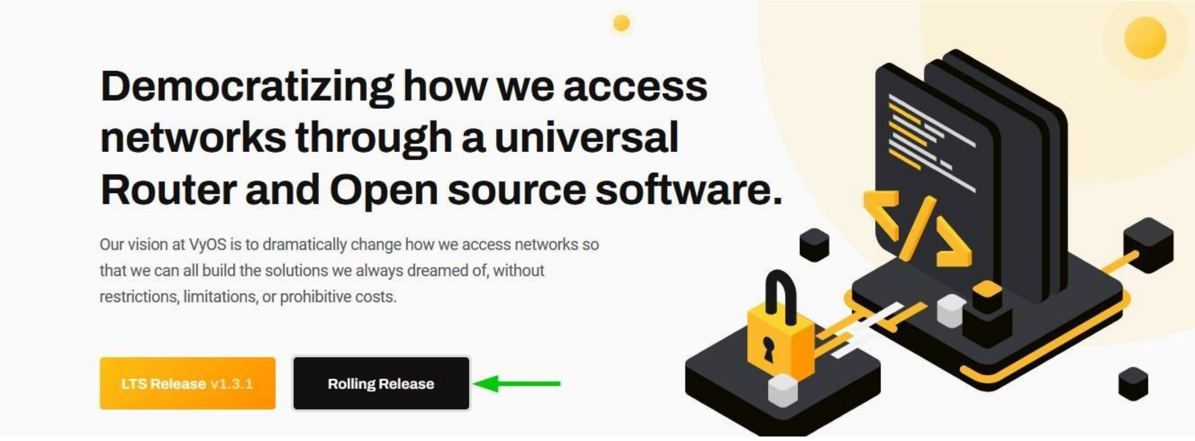
Clean install

Upgrade

For Gaia Fast Deployment (Blink), refer to sk120193. Check Point recommends to upgrade using SmartConsole or CDT.

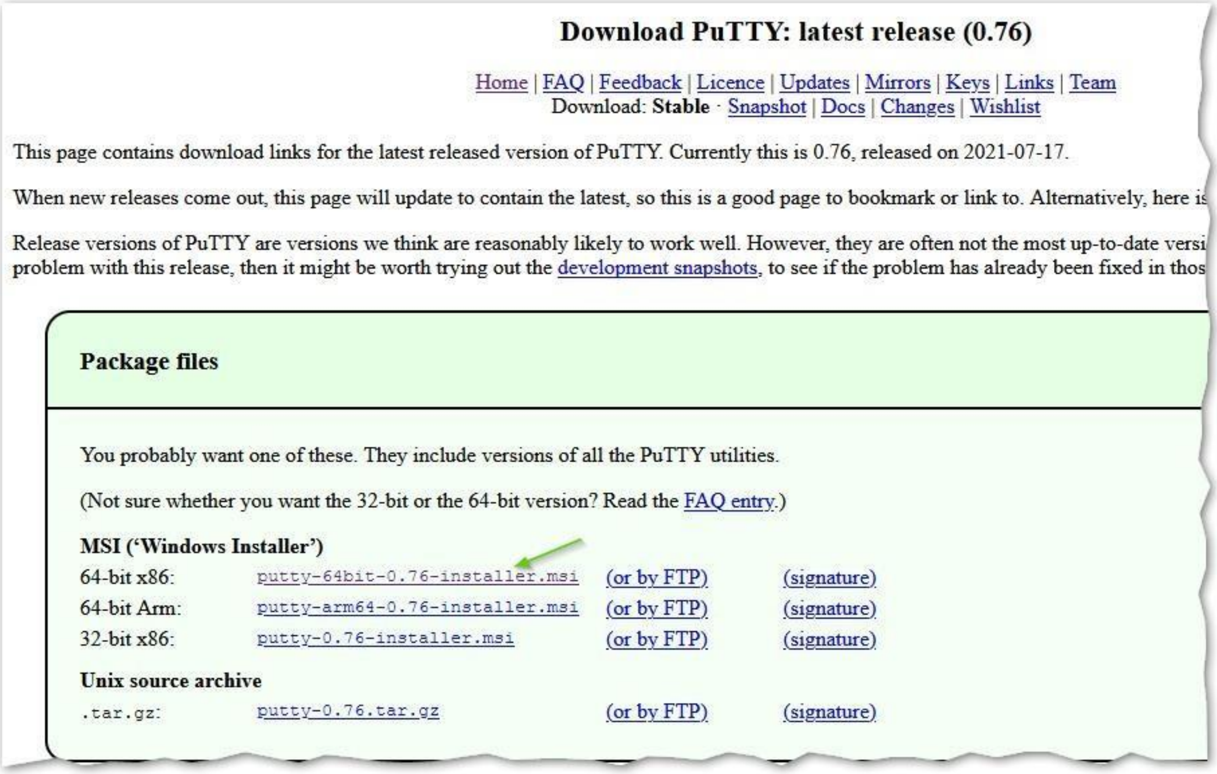
SmartConsole

For Web SmartConsole, see sk170314



Democratizing how we access networks through a universal Router and Open source software.

Our vision at VyOS is to dramatically change how we access networks so that we can all build the solutions we always dreamed of, without restrictions, limitations, or prohibitive costs.



Download PuTTY: latest release (0.76)

Home | FAQ | Feedback | Licence | Updates | Mirrors | Keys | Links | Team
Download: **Stable** · Snapshot | Docs | Changes | Wishlist

This page contains download links for the latest released version of PuTTY. Currently this is 0.76, released on 2021-07-17.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date versi problem with this release, then it might be worth trying out the development snapshots, to see if the problem has already been fixed in thos

Package files

You probably want one of these. They include versions of all the PuTTY utilities.

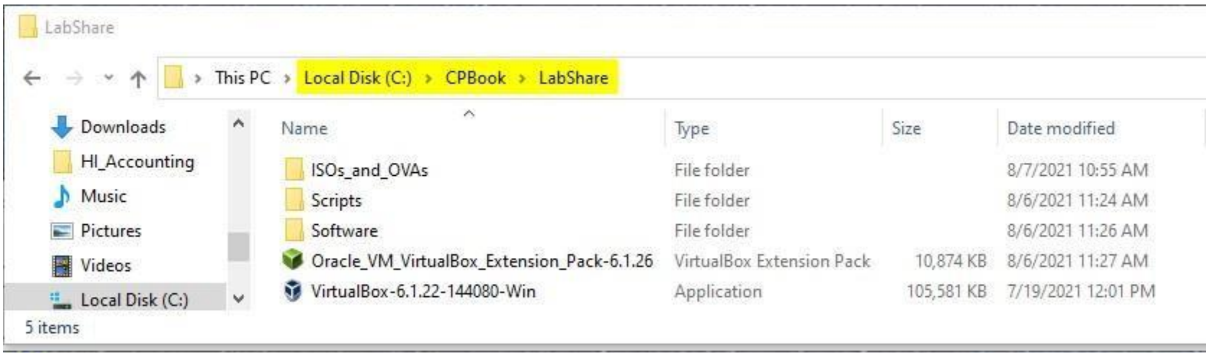
(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

MSI ('Windows Installer')

64-bit x86:	`putty-64bit-0.76-installer.msi`	(or by FTP)	(signature)
64-bit Arm:	`putty-arm64-0.76-installer.msi`	(or by FTP)	(signature)
32-bit x86:	`putty-0.76-installer.msi`	(or by FTP)	(signature)

Unix source archive

`.tar.gz:`	`putty-0.76.tar.gz`	(or by FTP)	(signature)

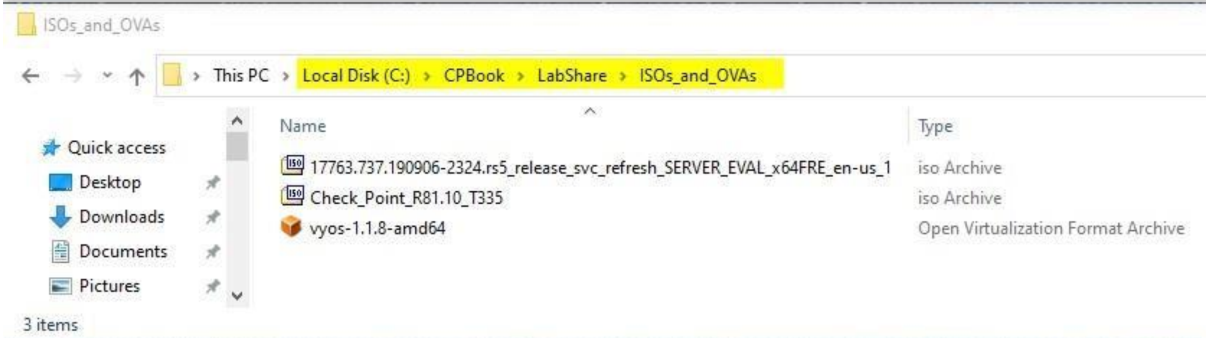


LabShare

This PC › Local Disk (C:) › CPBook › LabShare

Name	Type	Size	Date modified
ISOs_and_OVAs	File folder		8/7/2021 10:55 AM
Scripts	File folder		8/6/2021 11:24 AM
Software	File folder		8/6/2021 11:26 AM
Oracle_VM_VirtualBox_Extension_Pack-6.1.26	VirtualBox Extension Pack	10,874 KB	8/6/2021 11:27 AM
VirtualBox-6.1.22-144080-Win	Application	105,581 KB	7/19/2021 12:01 PM

5 items

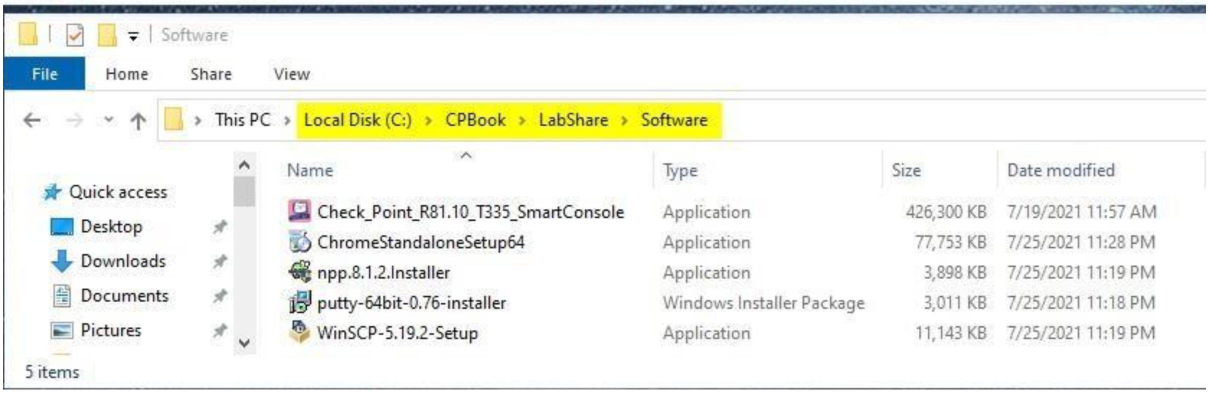


ISOs_and_OVAs

This PC › Local Disk (C:) › CPBook › LabShare › ISOs_and_OVAs

Name	Type
17763.737.190906-2324.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_en-us_1	iso Archive
Check_Point_R81.10_T335	iso Archive
vyos-1.1.8-amd64	Open Virtualization Format Archive

3 items

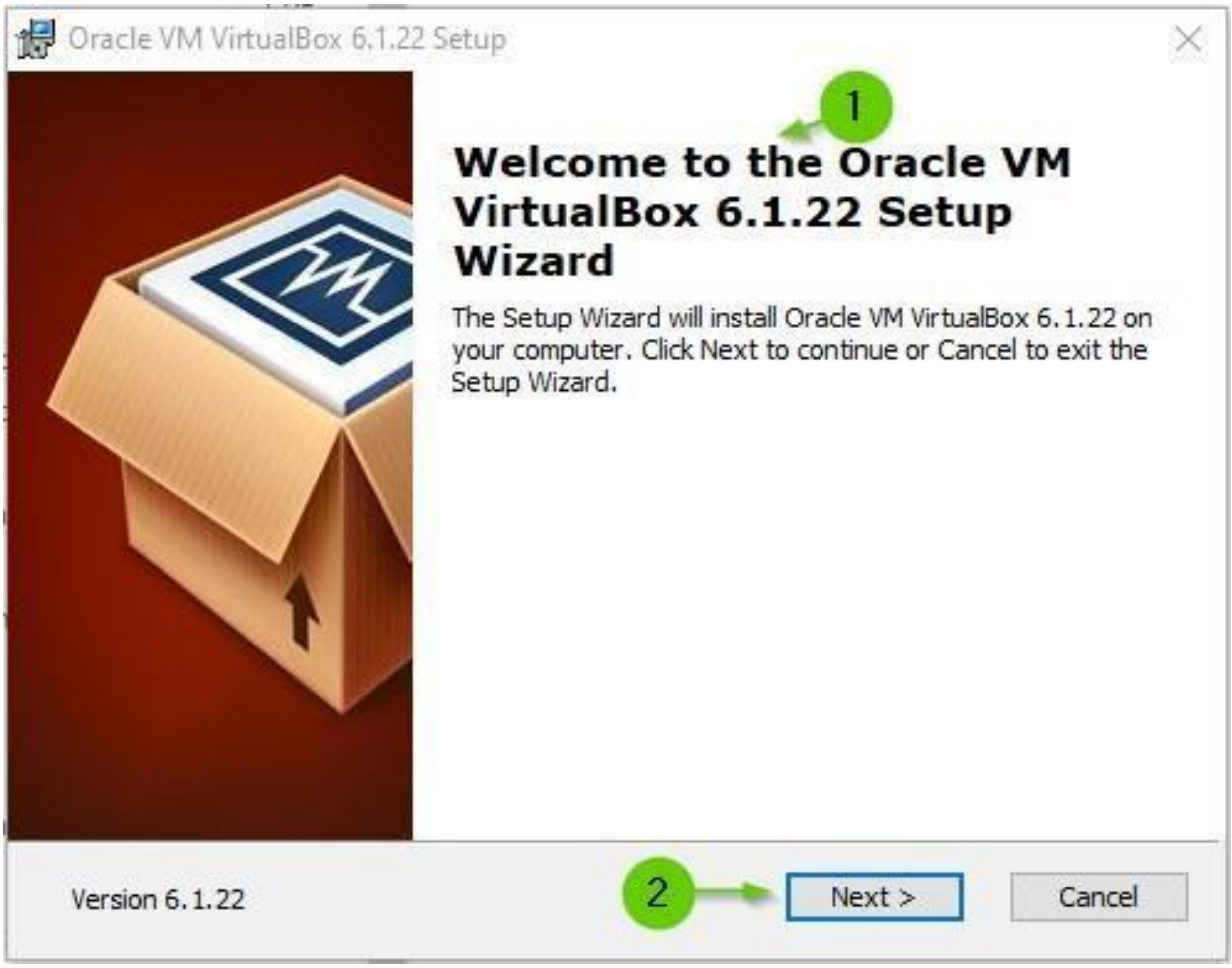


Software

This PC › Local Disk (C:) › CPBook › LabShare › Software

Name	Type	Size	Date modified
Check_Point_R81.10_T335_SmartConsole	Application	426,300 KB	7/19/2021 11:57 AM
ChromeStandaloneSetup64	Application	77,753 KB	7/25/2021 11:28 PM
npp.8.1.2.Installer	Application	3,898 KB	7/25/2021 11:19 PM
putty-64bit-0.76-installer	Windows Installer Package	3,011 KB	7/25/2021 11:18 PM
WinSCP-5.19.2-Setup	Application	11,143 KB	7/25/2021 11:19 PM

5 items

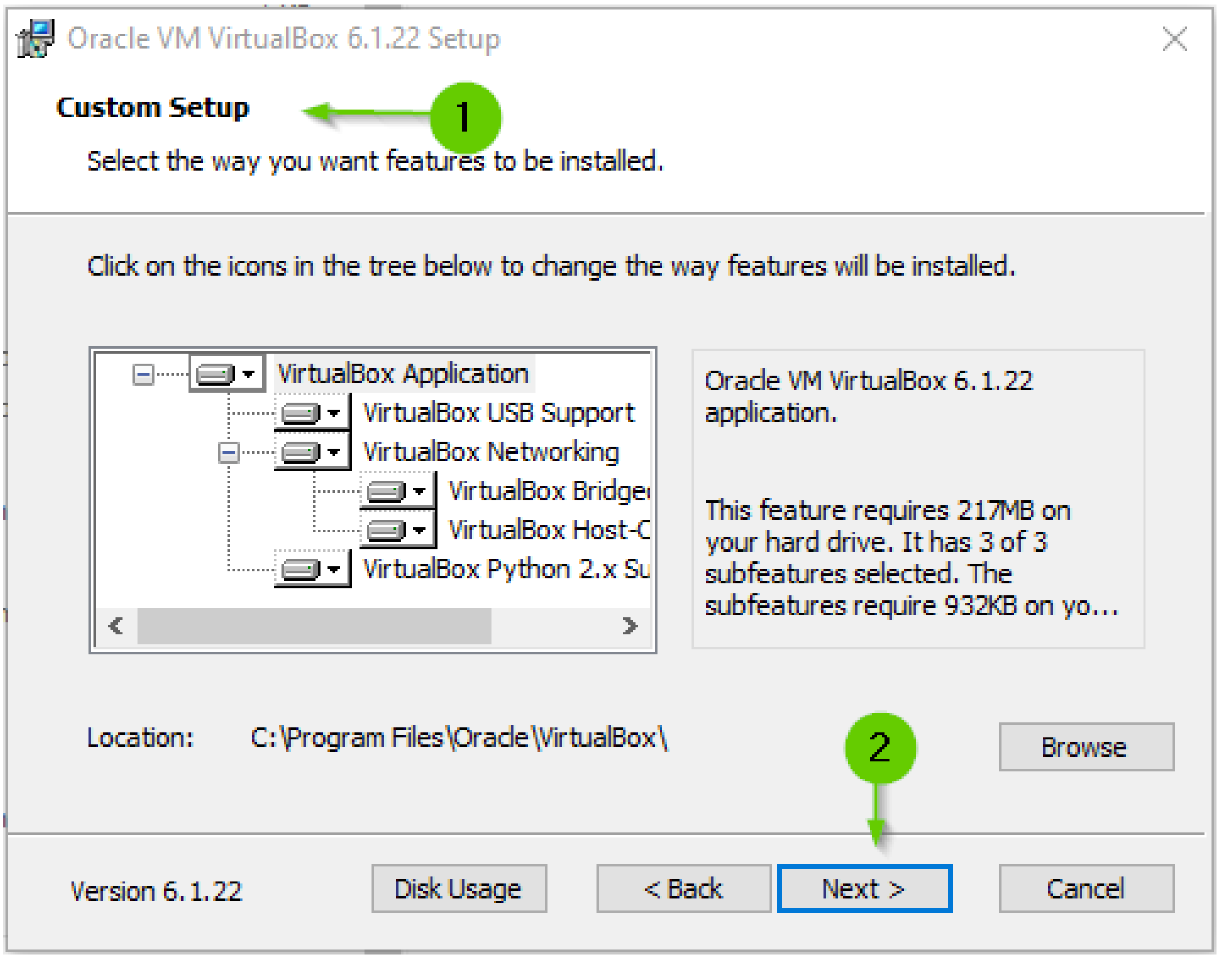


Oracle VM VirtualBox 6.1.22 Setup

Welcome to the Oracle VM VirtualBox 6.1.22 Setup Wizard

The Setup Wizard will install Oracle VM VirtualBox 6.1.22 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Version 6.1.22



Oracle VM VirtualBox 6.1.22 Setup

Custom Setup

Select the way you want features to be installed.

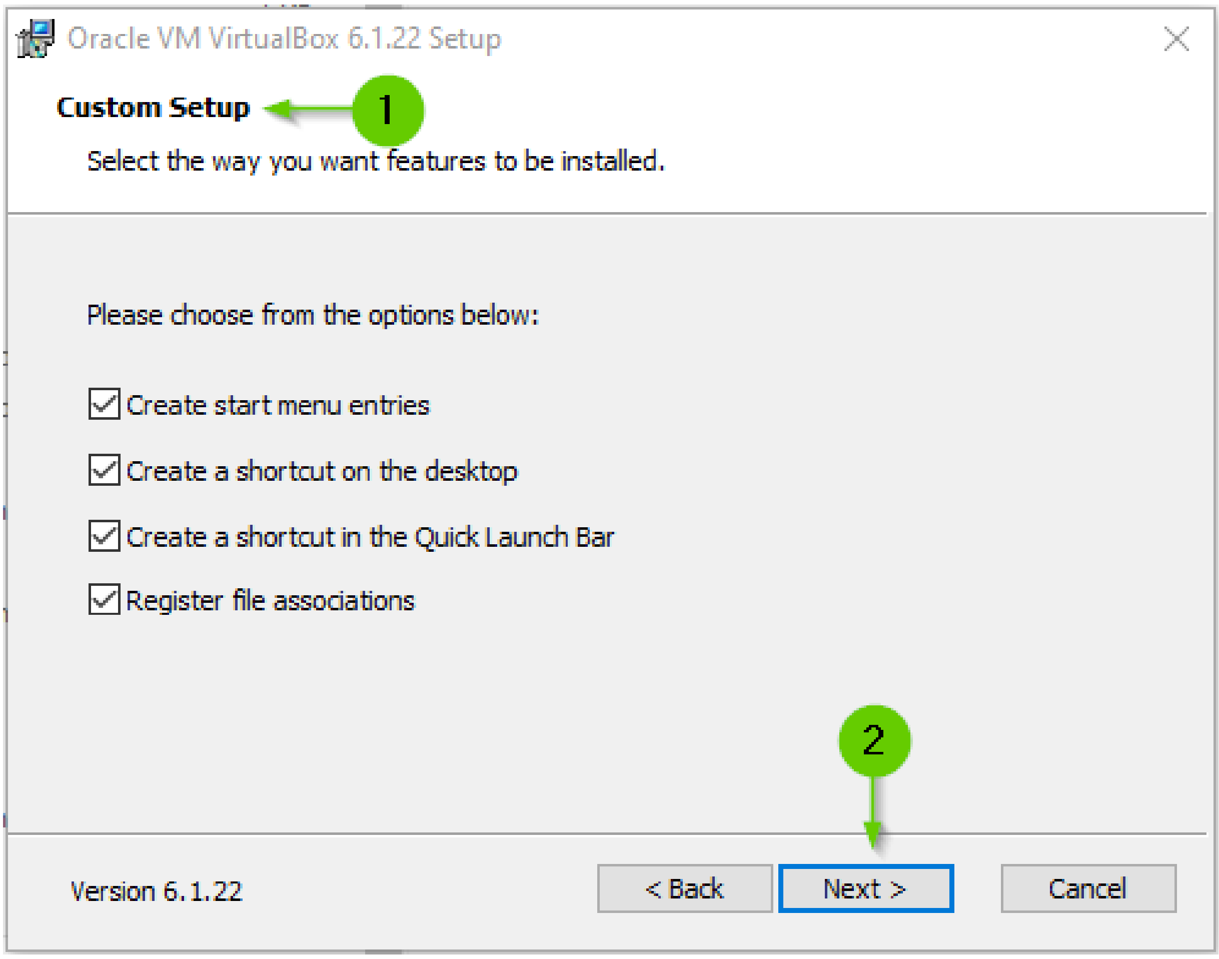
Click on the icons in the tree below to change the way features will be installed.

Oracle VM VirtualBox 6.1.22 application.

This feature requires 217MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 932KB on yo...

Location: C:\Program Files\Oracle\VirtualBox\

Version 6.1.22



Custom Setup

1

Select the way you want features to be installed.

Please choose from the options below:

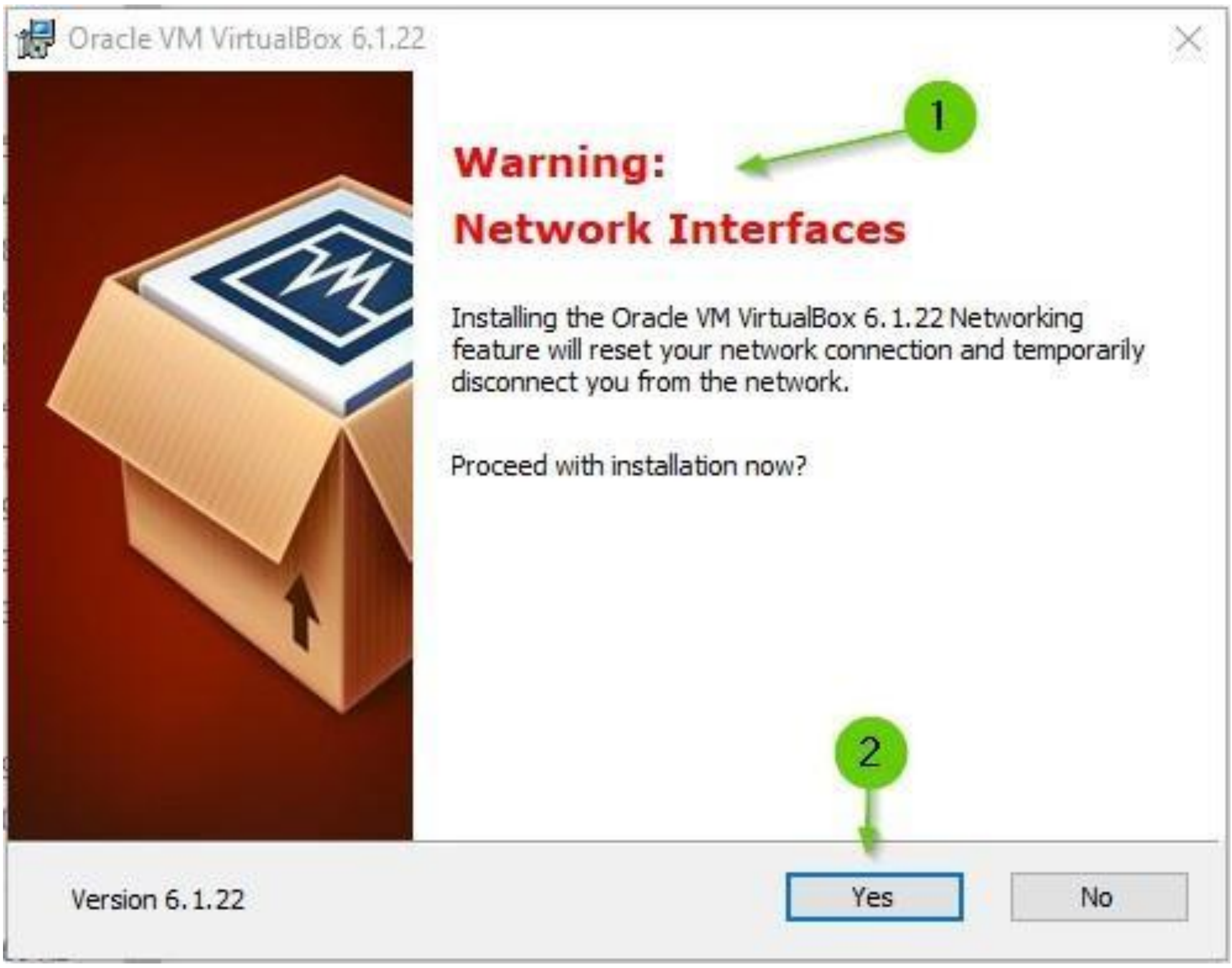
☑ Create start menu entries

☑ Create a shortcut on the desktop

☑ Create a shortcut in the Quick Launch Bar

☑ Register file associations

2

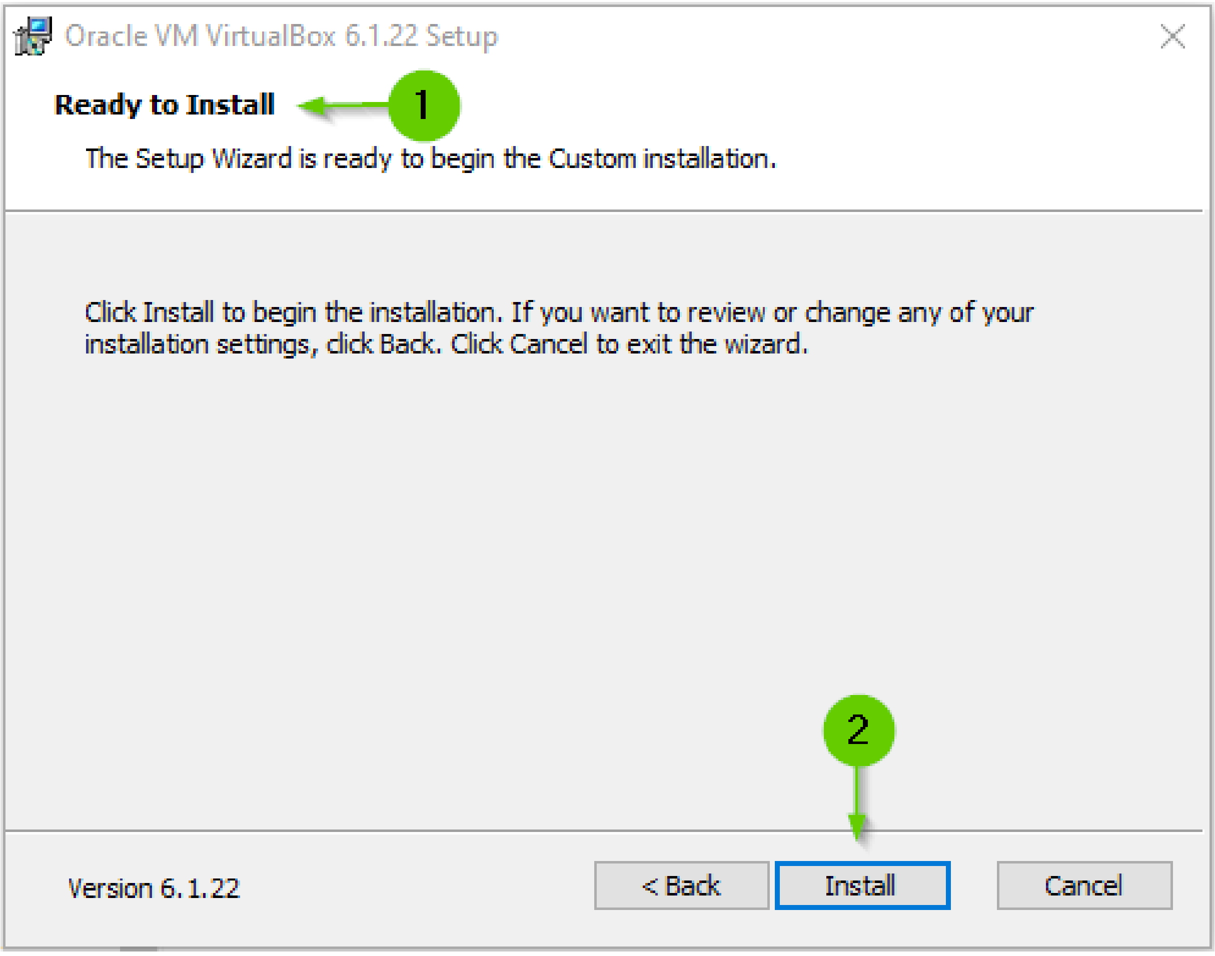


Warning: Network Interfaces

Installing the Oracle VM VirtualBox 6.1.22 Networking feature will reset your network connection and temporarily disconnect you from the network.

Proceed with installation now?

Version 6.1.22

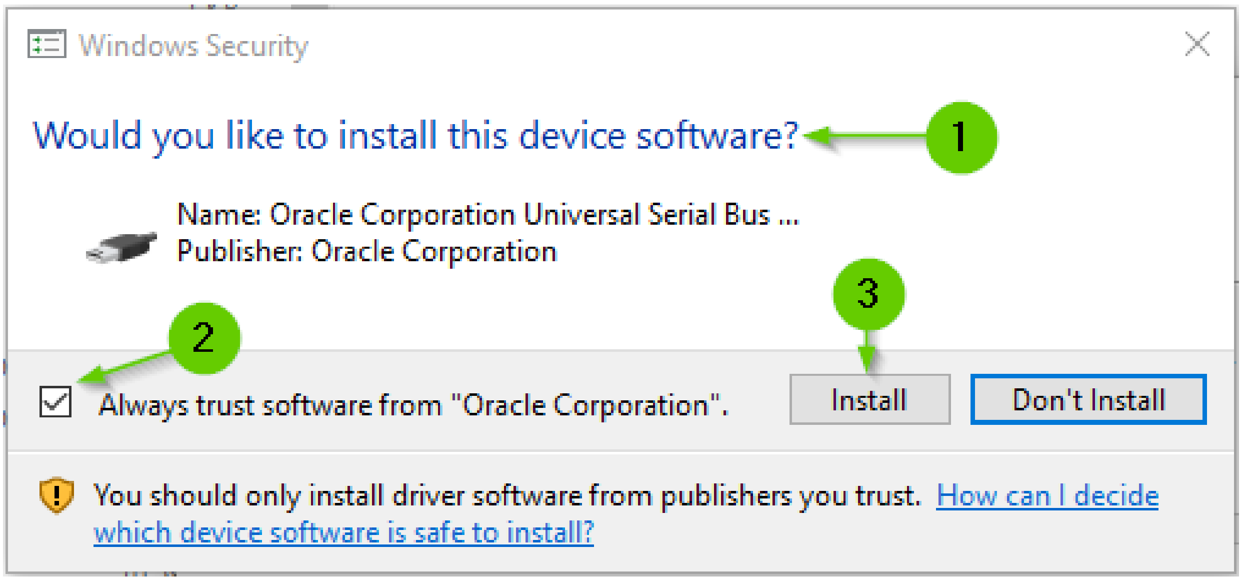


Ready to Install

The Setup Wizard is ready to begin the Custom installation.

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Version 6.1.22



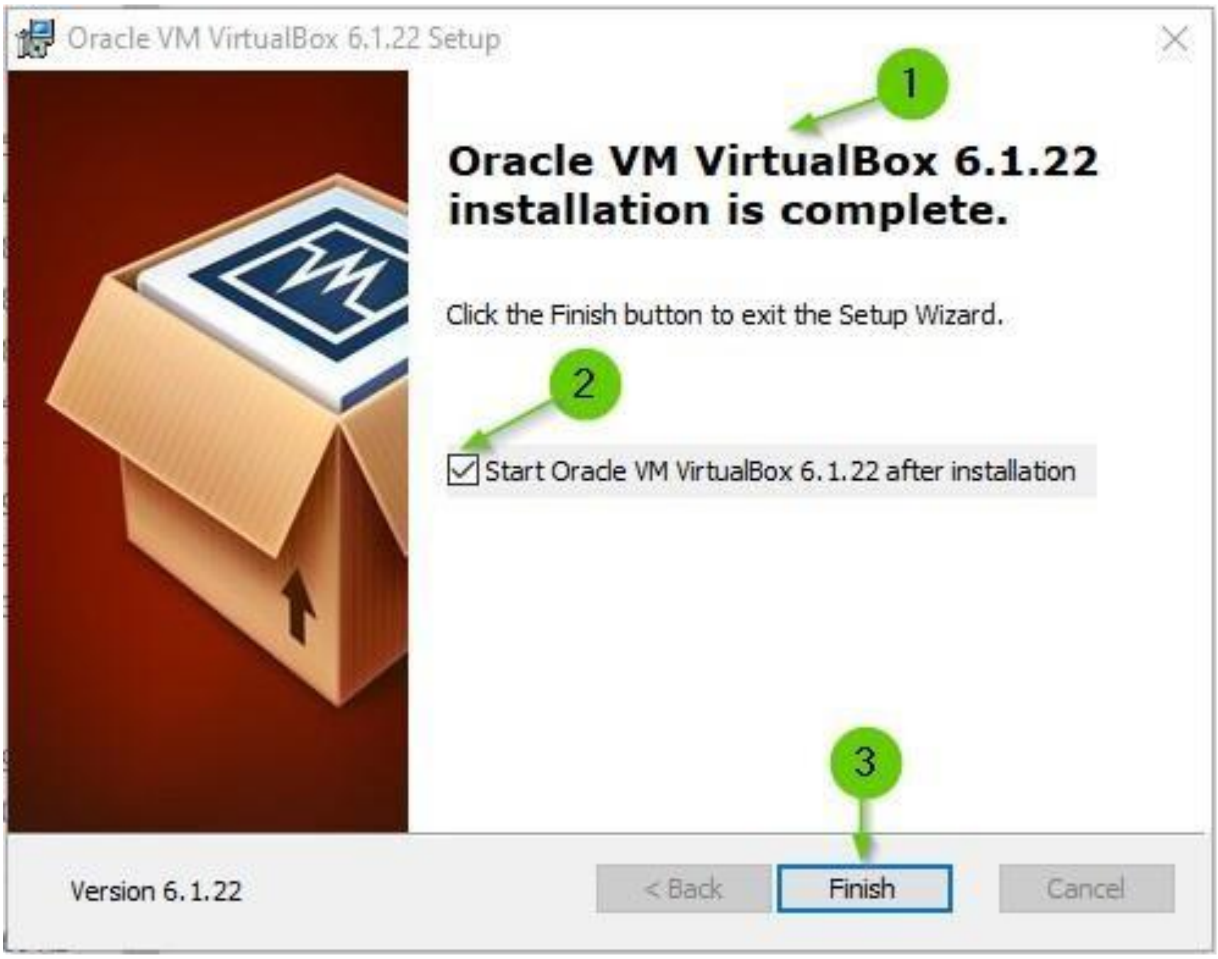
Windows Security

Would you like to install this device software?

Name: Oracle Corporation Universal Serial Bus ...
Publisher: Oracle Corporation

☑ Always trust software from "Oracle Corporation".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?



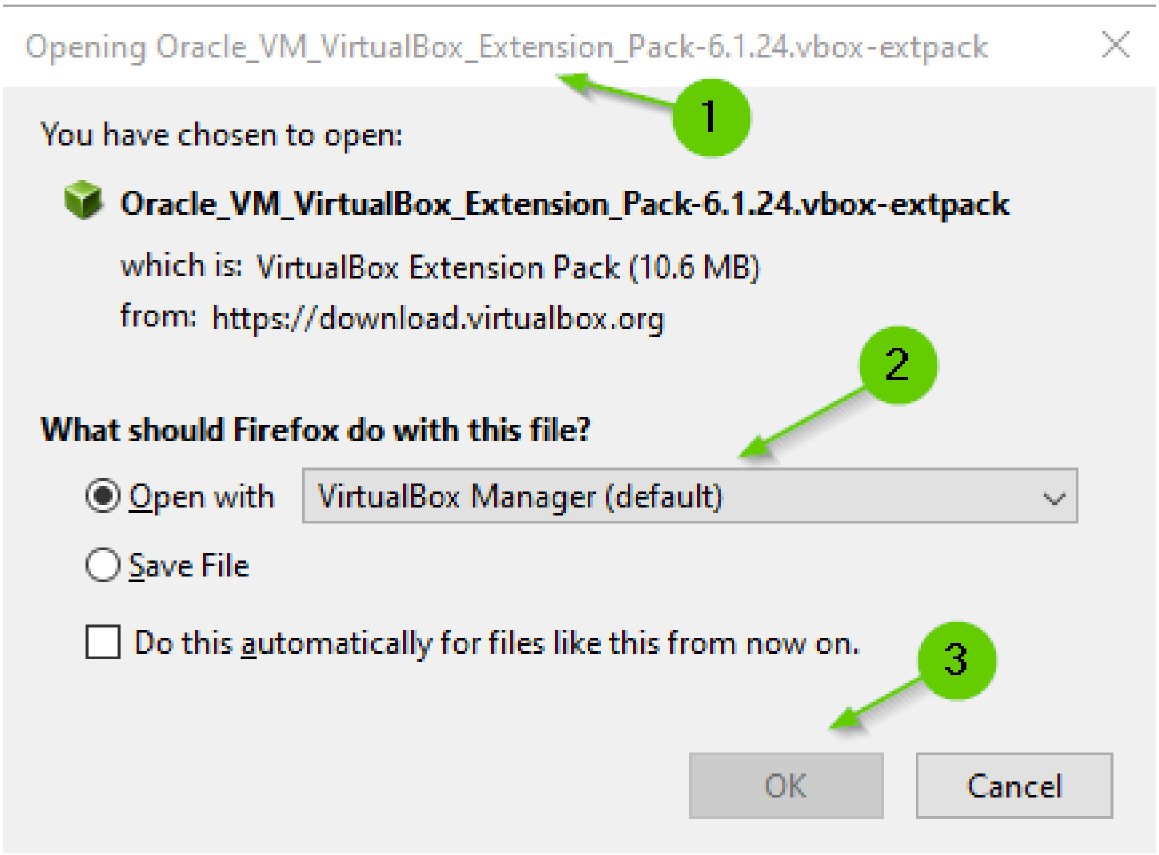
Oracle VM VirtualBox 6.1.22 Setup

Oracle VM VirtualBox 6.1.22 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VM VirtualBox 6.1.22 after installation

Version 6.1.22



Opening Oracle_VM_VirtualBox_Extension_Pack-6.1.24.vbox-extpack

You have chosen to open:

Oracle_VM_VirtualBox_Extension_Pack-6.1.24.vbox-extpack

which is: VirtualBox Extension Pack (10.6 MB)

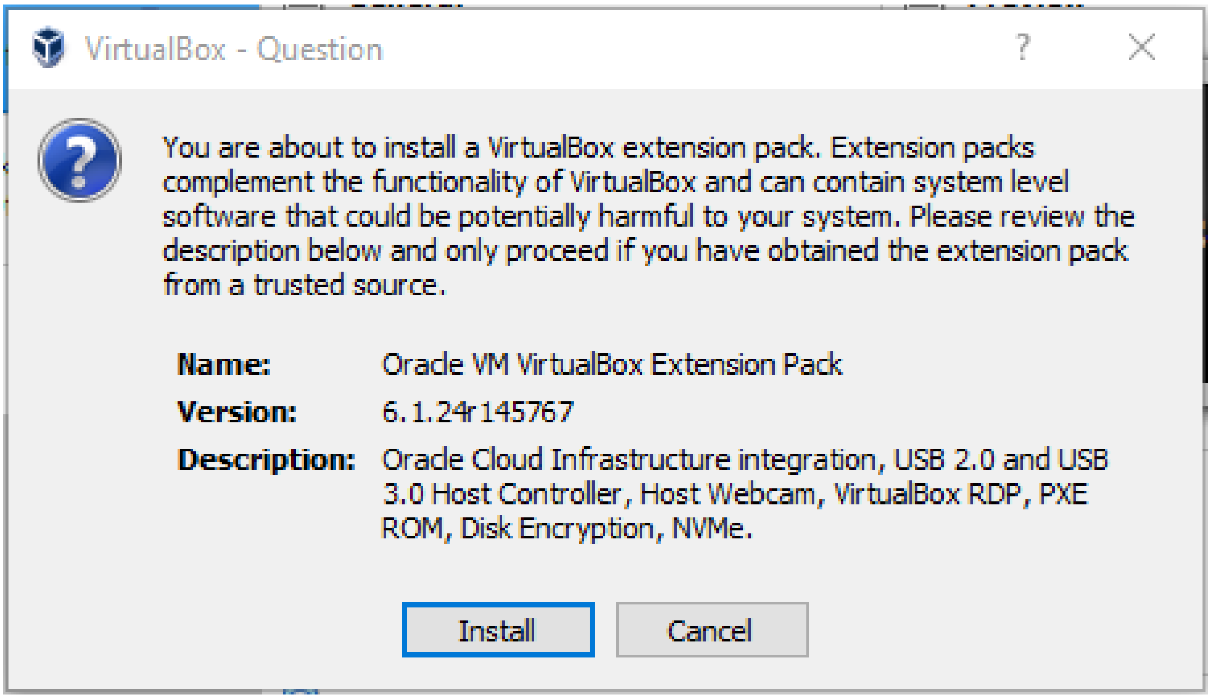
from: https://download.virtualbox.org

What should Firefox do with this file?

● Open with VirtualBox Manager (default)

○ Save File

□ Do this automatically for files like this from now on.



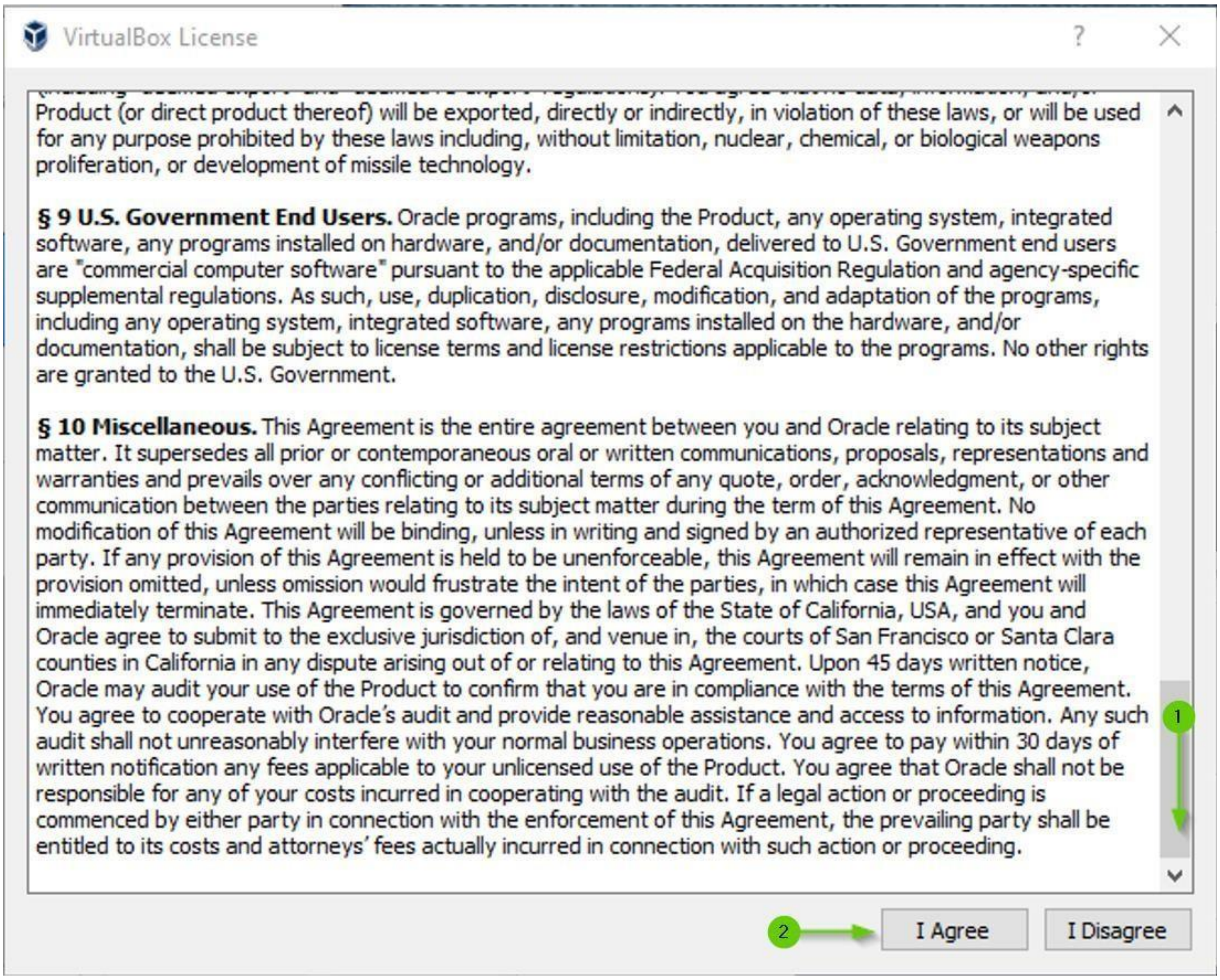
VirtualBox - Question

You are about to install a VirtualBox extension pack. Extension packs complement the functionality of VirtualBox and can contain system level software that could be potentially harmful to your system. Please review the description below and only proceed if you have obtained the extension pack from a trusted source.

Name: Oracle VM VirtualBox Extension Pack

Version: 6.1.24r145767

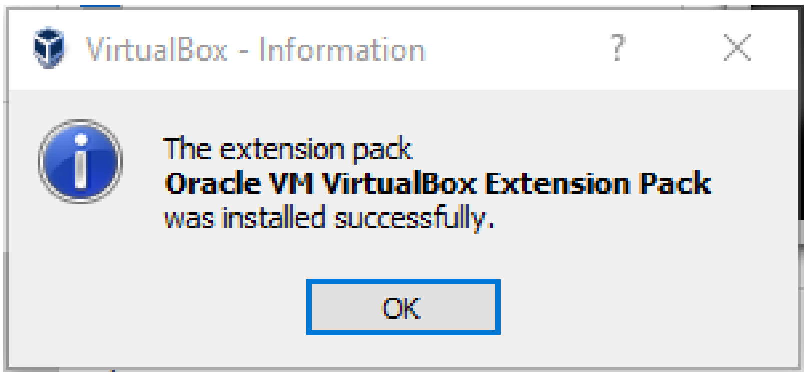
Description: Oracle Cloud Infrastructure integration, USB 2.0 and USB 3.0 Host Controller, Host Webcam, VirtualBox RDP, PXE ROM, Disk Encryption, NVMe.



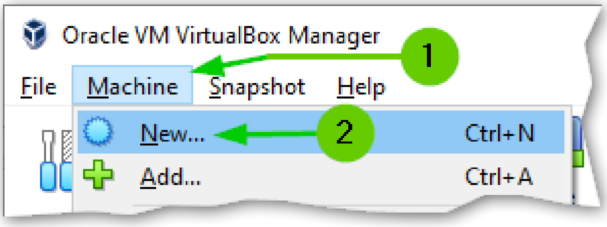
Product (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

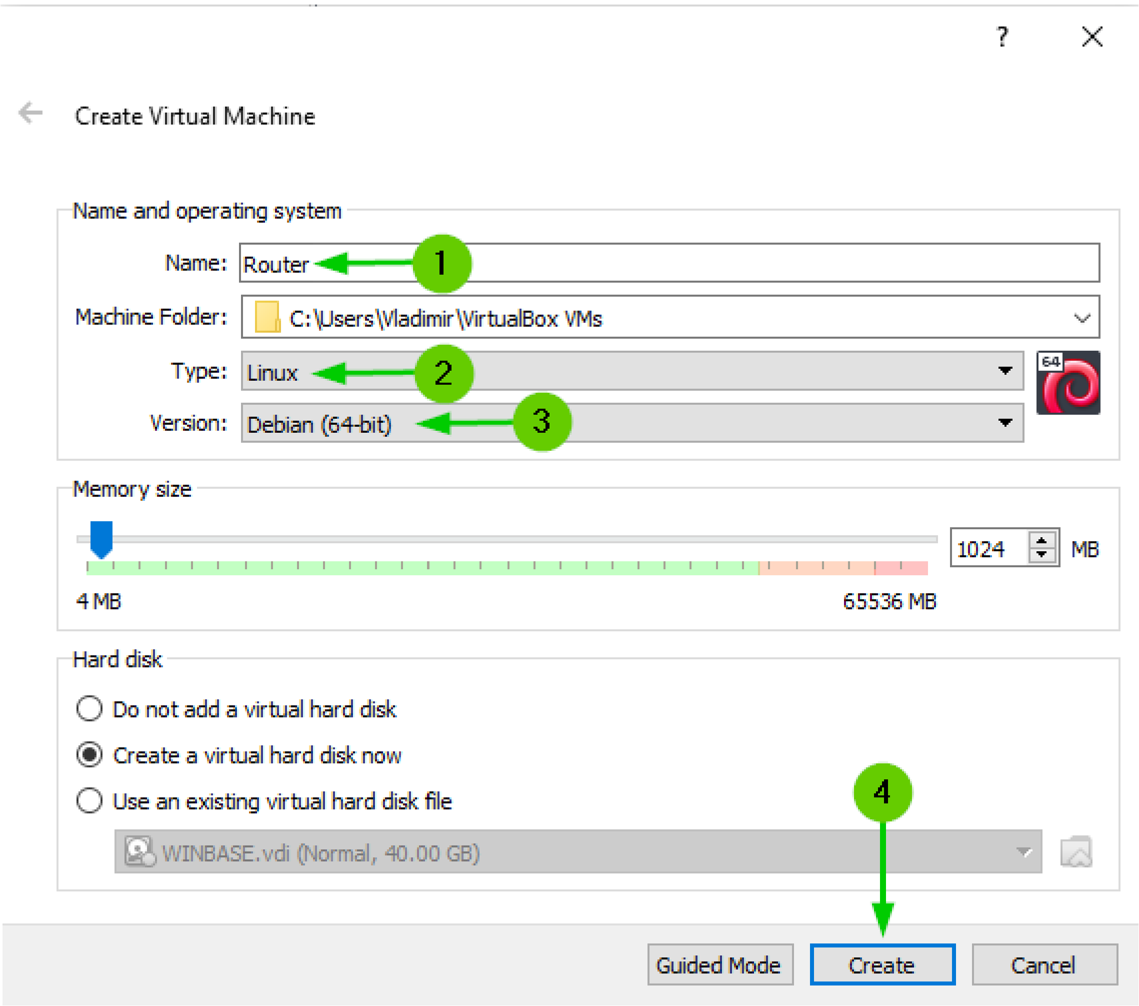
§ 9 U.S. Government End Users. Oracle programs, including the Product, any operating system, integrated software, any programs installed on hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

§ 10 Miscellaneous. This Agreement is the entire agreement between you and Oracle relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate. This Agreement is governed by the laws of the State of California, USA, and you and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco or Santa Clara counties in California in any dispute arising out of or relating to this Agreement. Upon 45 days written notice, Oracle may audit your use of the Product to confirm that you are in compliance with the terms of this Agreement. You agree to cooperate with Oracle's audit and provide reasonable assistance and access to information. Any such audit shall not unreasonably interfere with your normal business operations. You agree to pay within 30 days of written notification any fees applicable to your unlicensed use of the Product. You agree that Oracle shall not be responsible for any of your costs incurred in cooperating with the audit. If a legal action or proceeding is commenced by either party in connection with the enforcement of this Agreement, the prevailing party shall be entitled to its costs and attorneys' fees actually incurred in connection with such action or proceeding.



The extension pack
Oracle VM VirtualBox Extension Pack
was installed successfully.




Create Virtual Machine

Name and operating system

Name: Router

Machine Folder: C:\Users\Vladimir\VirtualBox VMs

Type: Linux

Version: Debian (64-bit)

Memory size

1024 MB

4 MB

65536 MB

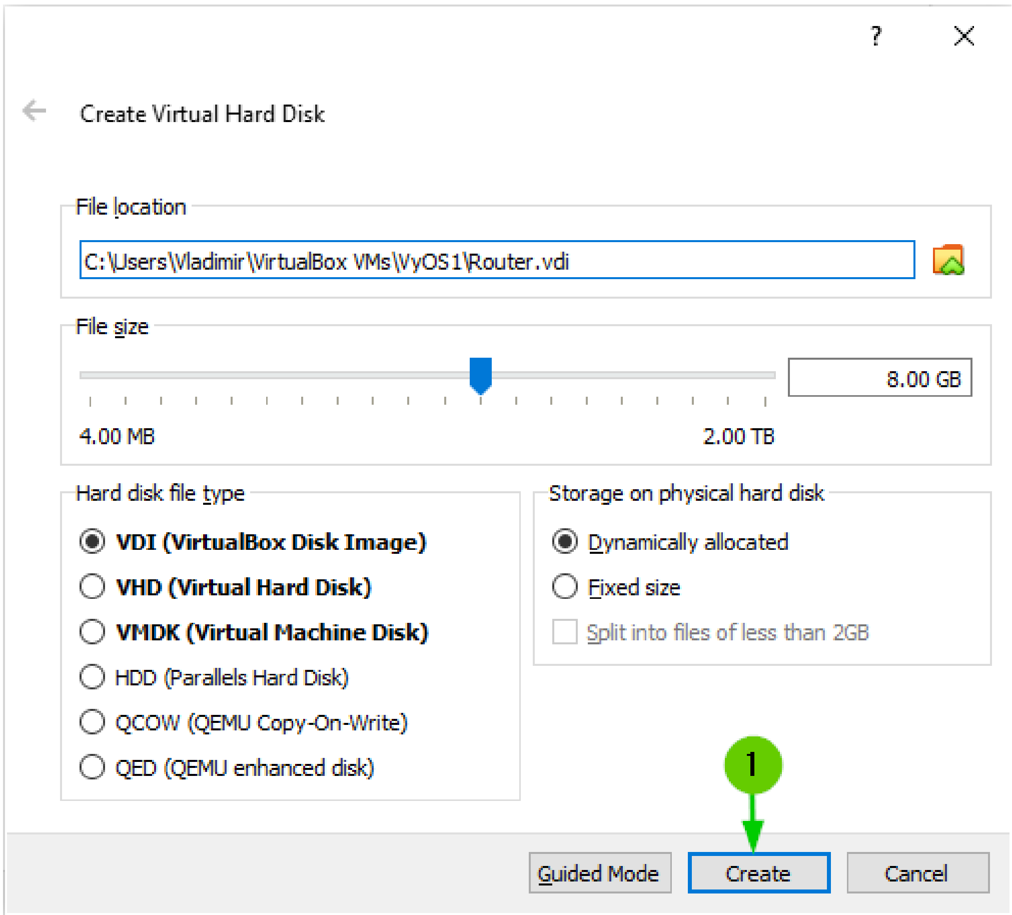
Hard disk

○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

WINBASE.vdi (Normal, 40.00 GB)


Create Virtual Hard Disk

File location

C:\Users\Vladimir\VirtualBox VMs\VyOS1\Router.vdi

File size

8.00 GB

4.00 MB

2.00 TB

Hard disk file type

● **VDI (VirtualBox Disk Image)**

○ **VHD (Virtual Hard Disk)**

○ **VMDK (Virtual Machine Disk)**

○ HDD (Parallels Hard Disk)

○ QCOW (QEMU Copy-On-Write)

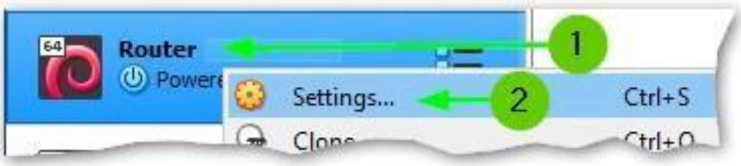
○ QED (QEMU enhanced disk)

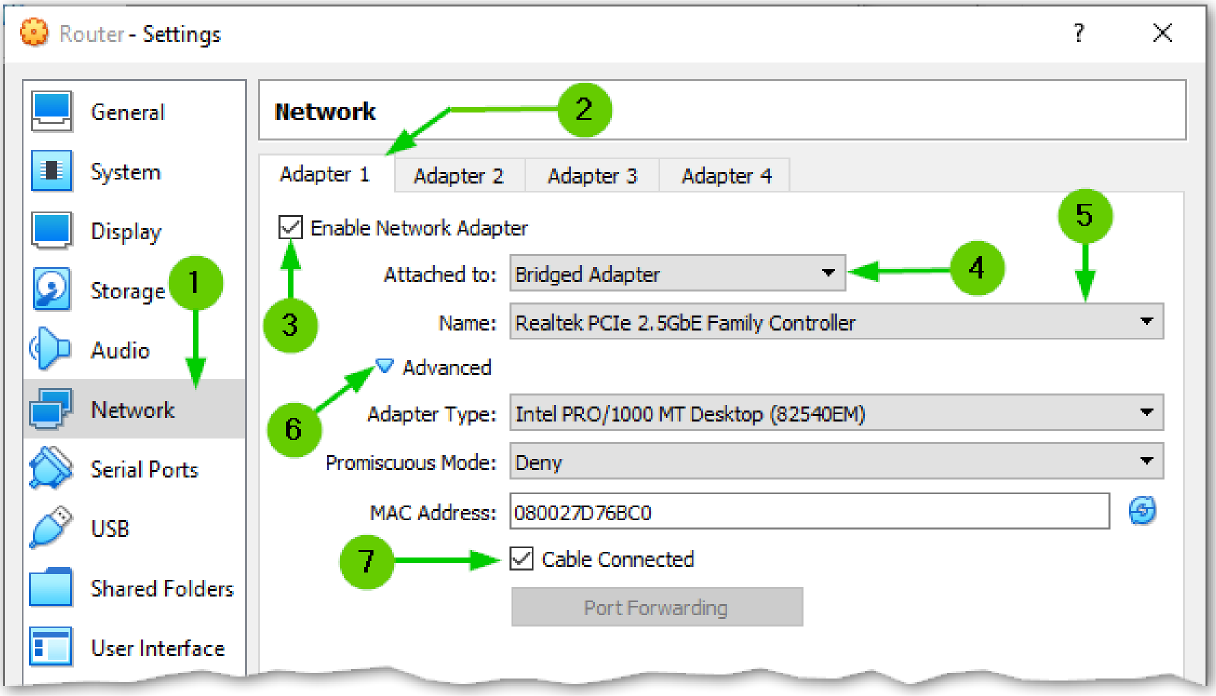
Storage on physical hard disk

● Dynamically allocated

○ Fixed size

□ Split into files of less than 2GB





Router - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek PCIe 2.5GbE Family Controller

Advanced

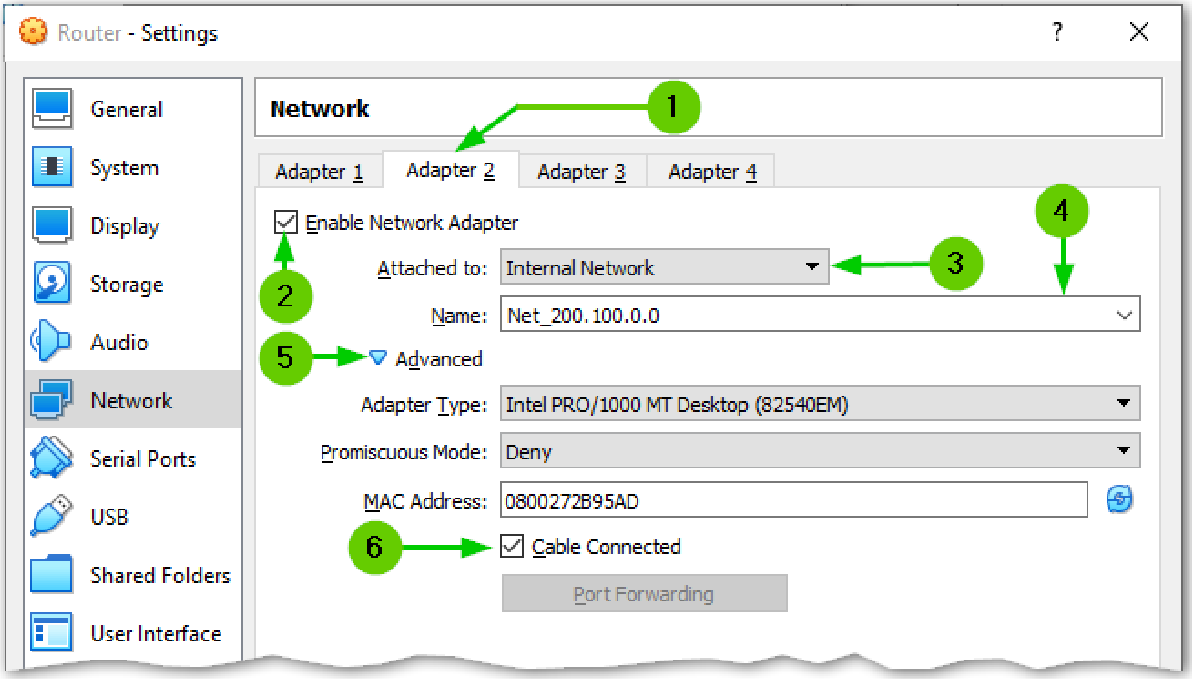
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027D76BC0

☑ Cable Connected

Port Forwarding



Router - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: Net_200.100.0.0

Advanced

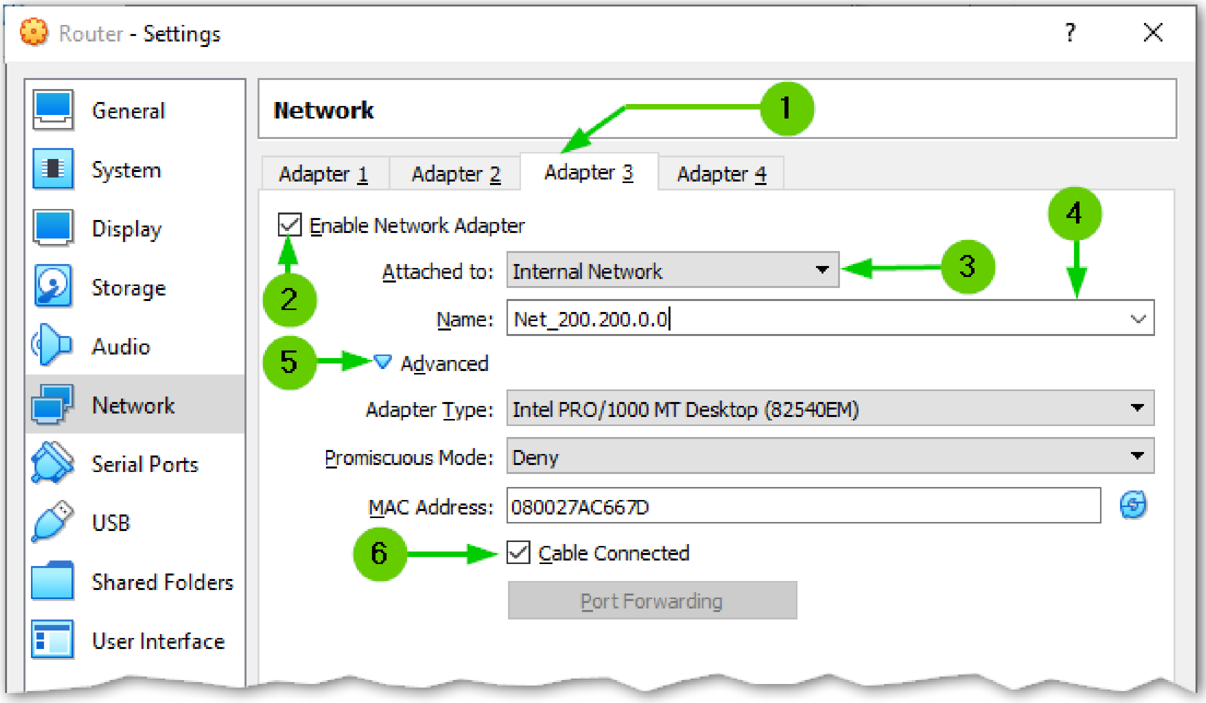
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800272B95AD

☑ Cable Connected

Port Forwarding



Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: Net_200.200.0.0

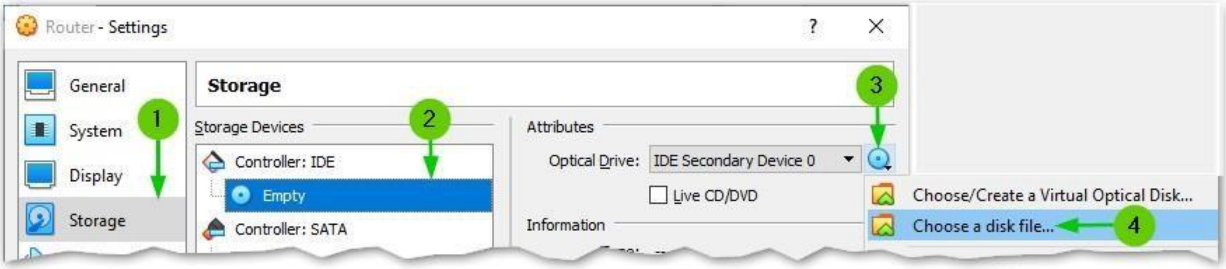
Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027AC667D

☑ Cable Connected



Storage

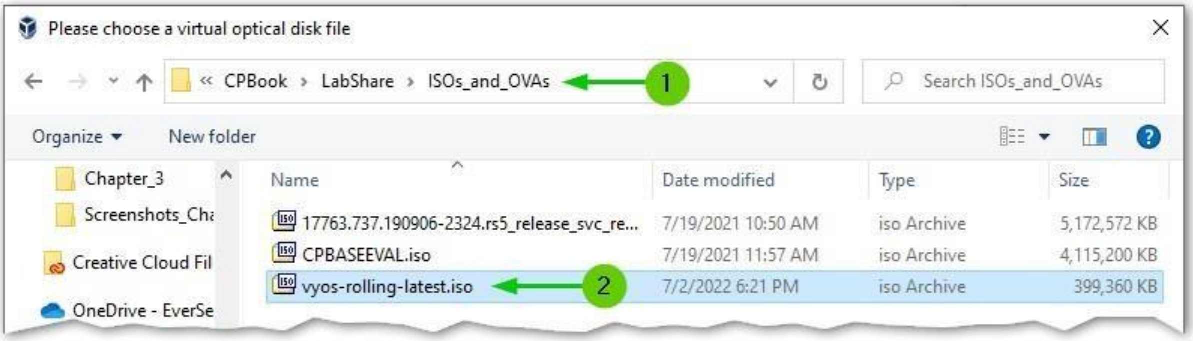
Controller: IDE

Empty

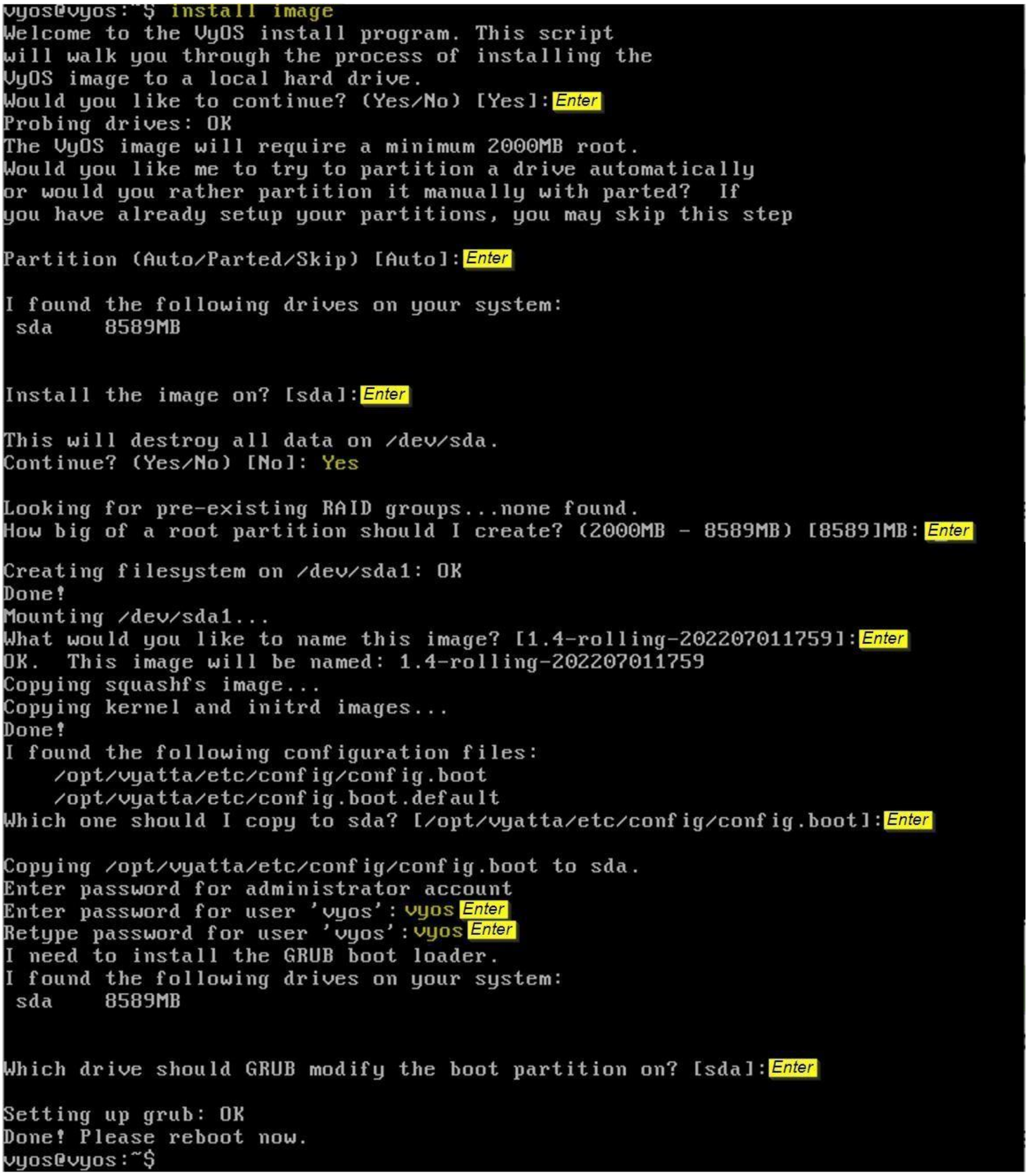
Controller: SATA

Optical Drive: IDE Secondary Device 0

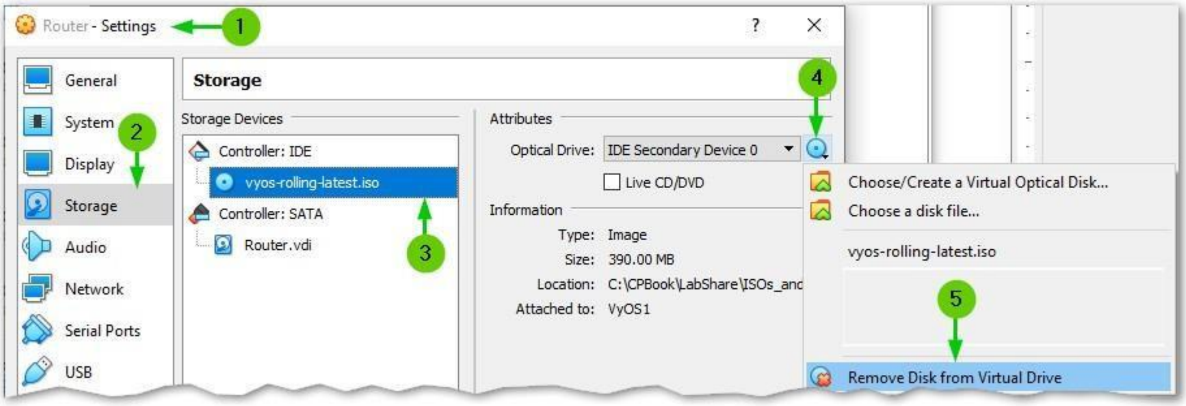
□ Live CD/DVD



Name	Date modified	Type	Size
17763.737.190906-2324.rs5_release_svc_re...	7/19/2021 10:50 AM	iso Archive	5,172,572 KB
CPBASEEVAL.iso	7/19/2021 11:57 AM	iso Archive	4,115,200 KB
vyos-rolling-latest.iso	7/2/2022 6:21 PM	iso Archive	399,360 KB



```
vyos@vyos:~$ install image
Welcome to the VyOS install program. This script
will walk you through the process of installing the
VyOS image to a local hard drive.
Would you like to continue? (Yes/No) [Yes]:Enter
Probing drives: OK
The VyOS image will require a minimum 2000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted?  If
you have already setup your partitions, you may skip this step

Partition (Auto/Parted/Skip) [Auto]:Enter

I found the following drives on your system:
 sda     8589MB


Install the image on? [sda]:Enter

This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: Yes

Looking for pre-existing RAID groups...none found.
How big of a root partition should I create? (2000MB - 8589MB) [8589]MB:Enter

Creating filesystem on /dev/sda1: OK
Done!
Mounting /dev/sda1...
What would you like to name this image? [1.4-rolling-202207011759]:Enter
OK.  This image will be named: 1.4-rolling-202207011759
Copying squashfs image...
Copying kernel and initrd images...
Done!
I found the following configuration files:
    /opt/vyatta/etc/config/config.boot
    /opt/vyatta/etc/config/config.boot.default
Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:Enter

Copying /opt/vyatta/etc/config/config.boot to sda.
Enter password for administrator account
Enter password for user 'vyos':vyos Enter
Retype password for user 'vyos':vyos Enter
I need to install the GRUB boot loader.
I found the following drives on your system:
 sda     8589MB


Which drive should GRUB modify the boot partition on? [sda]:Enter

Setting up grub: OK
Done! Please reboot now.
vyos@vyos:~$
```



Router - Settings

Storage

Storage Devices

Controller: IDE
vyos-rolling-latest.iso
Controller: SATA
Router.vdi

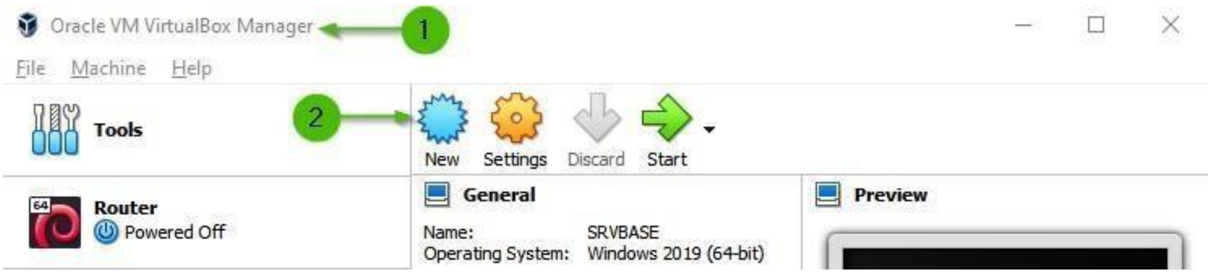
Attributes

Optical Drive: IDE Secondary Device 0

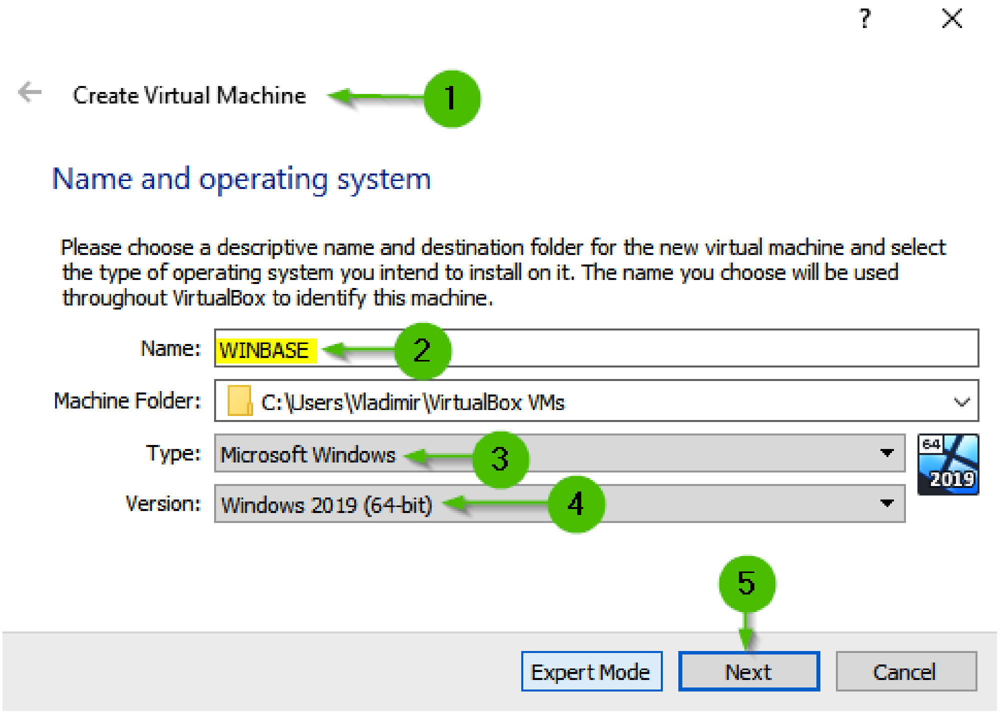
□ Live CD/DVD

Information

Type: Image
Size: 390.00 MB
Location: C:\CPBook\LabShare\ISOs_and
Attached to: VyOS1



Name: SRVBASE
Operating System: Windows 2019 (64-bit)



Name and operating system

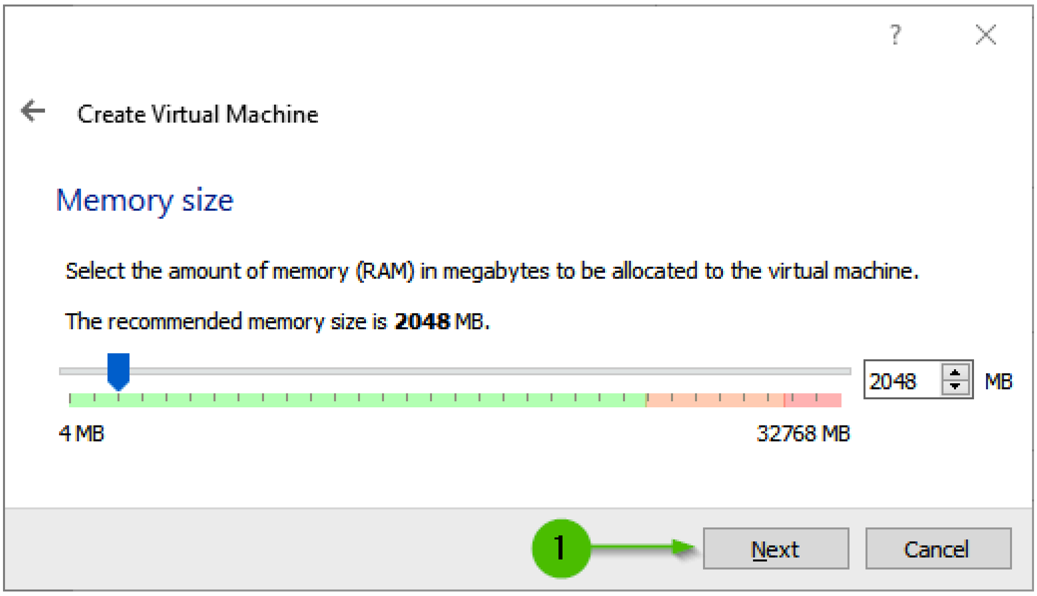
Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: WINBASE

Machine Folder: C:\Users\Vladimir\VirtualBox VMs

Type: Microsoft Windows

Version: Windows 2019 (64-bit)



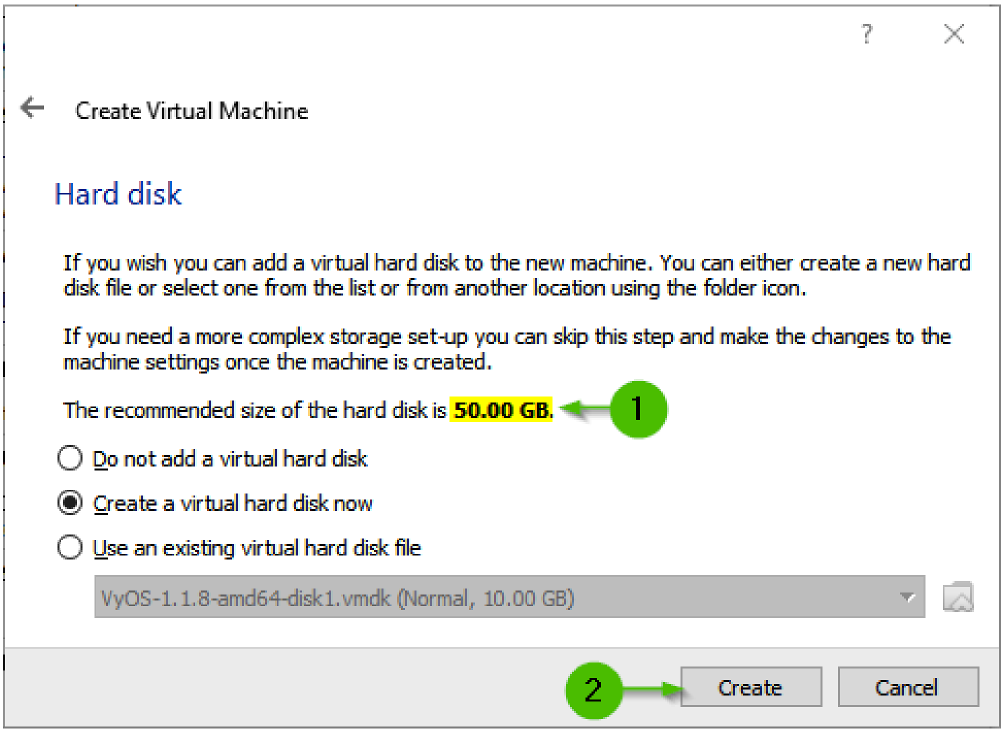
Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048** MB.

2048 MB



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

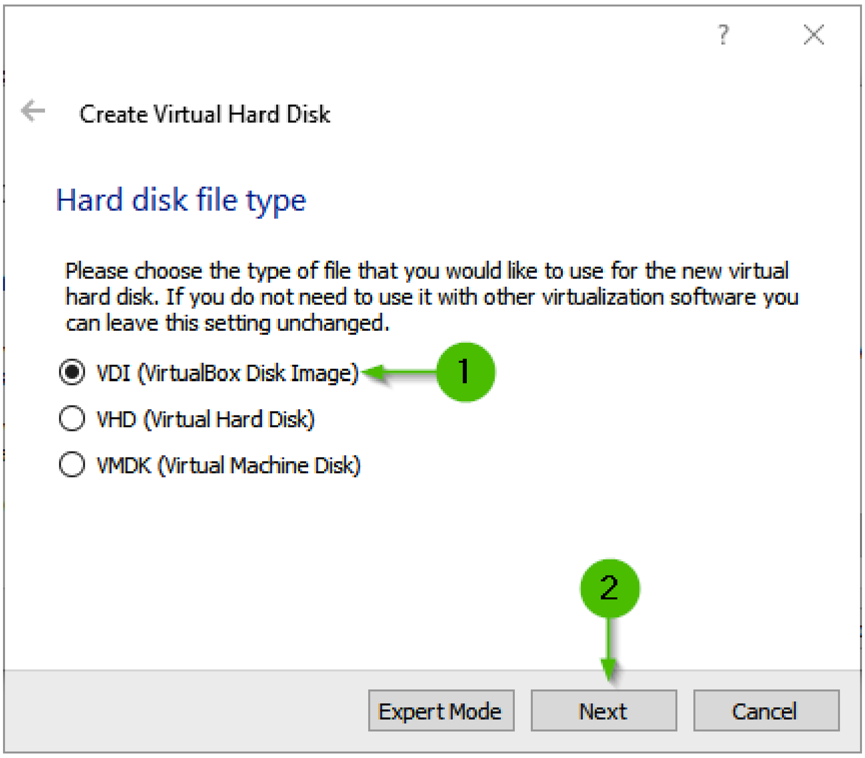
The recommended size of the hard disk is **50.00 GB.**

○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

VyOS-1.1.8-amd64-disk1.vmdk (Normal, 10.00 GB)



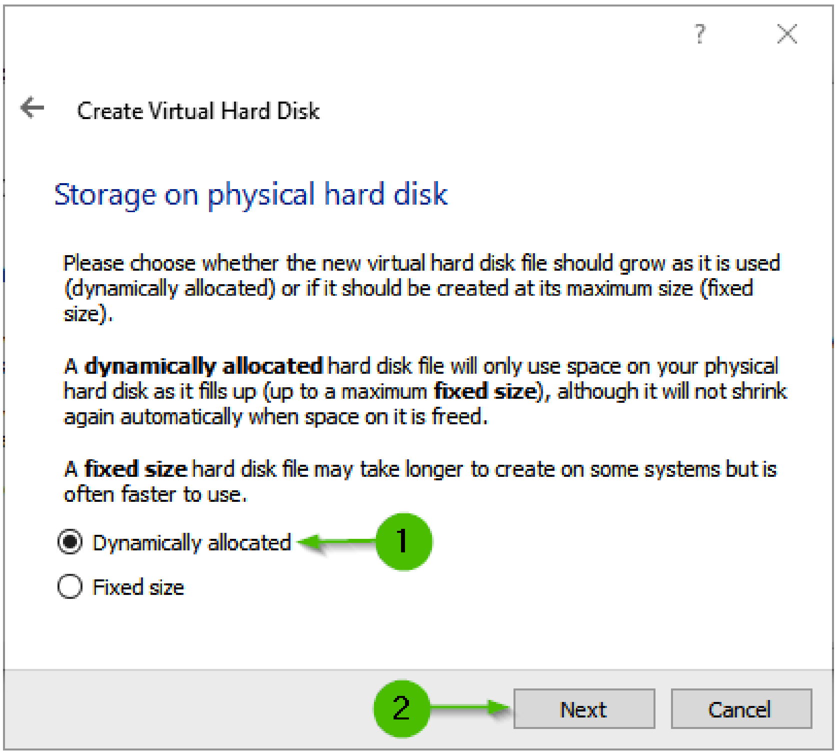
Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)



Storage on physical hard disk

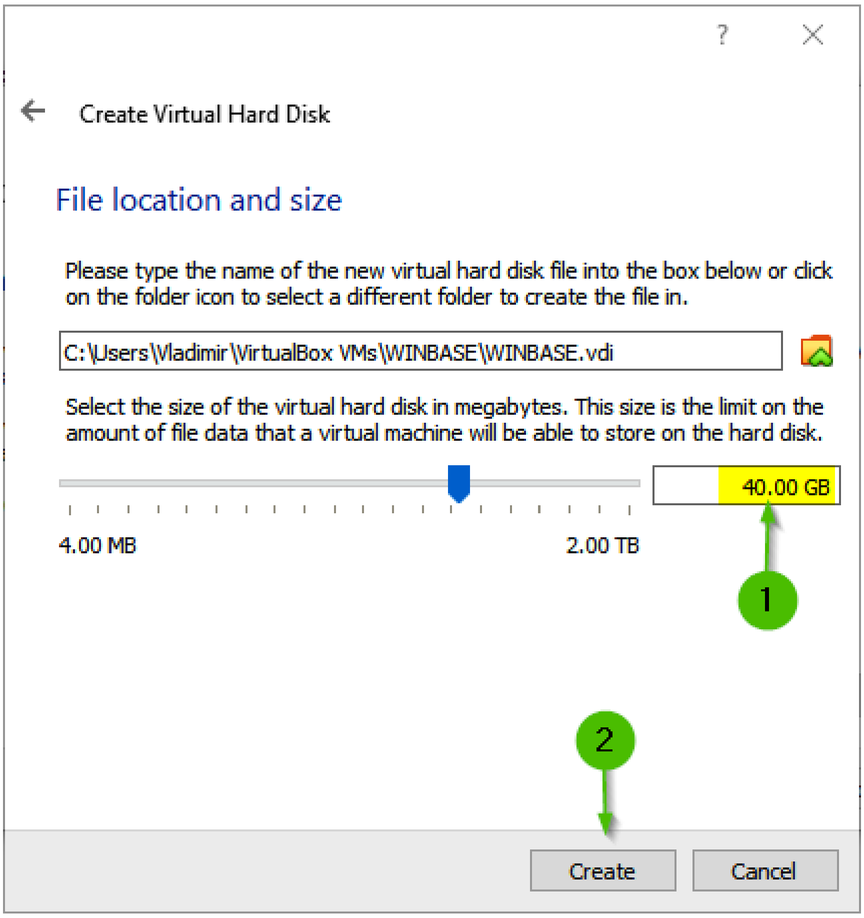
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size



Create Virtual Hard Disk

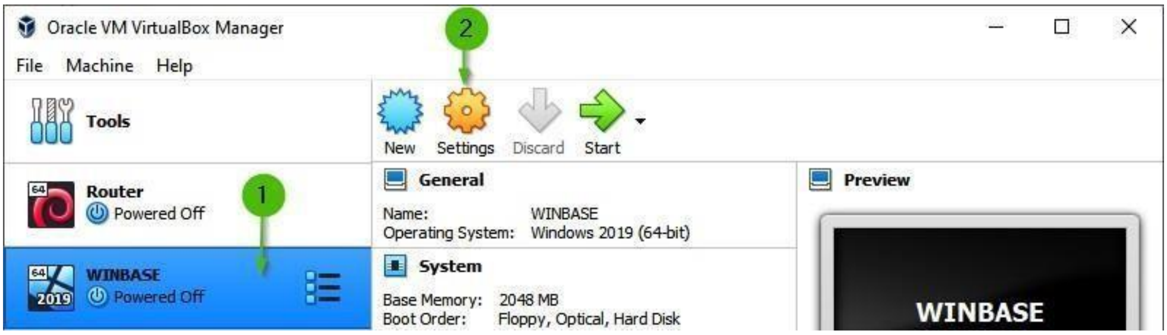
File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\Users\Vladimir\VirtualBox VMs\WINBASE\WINBASE.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

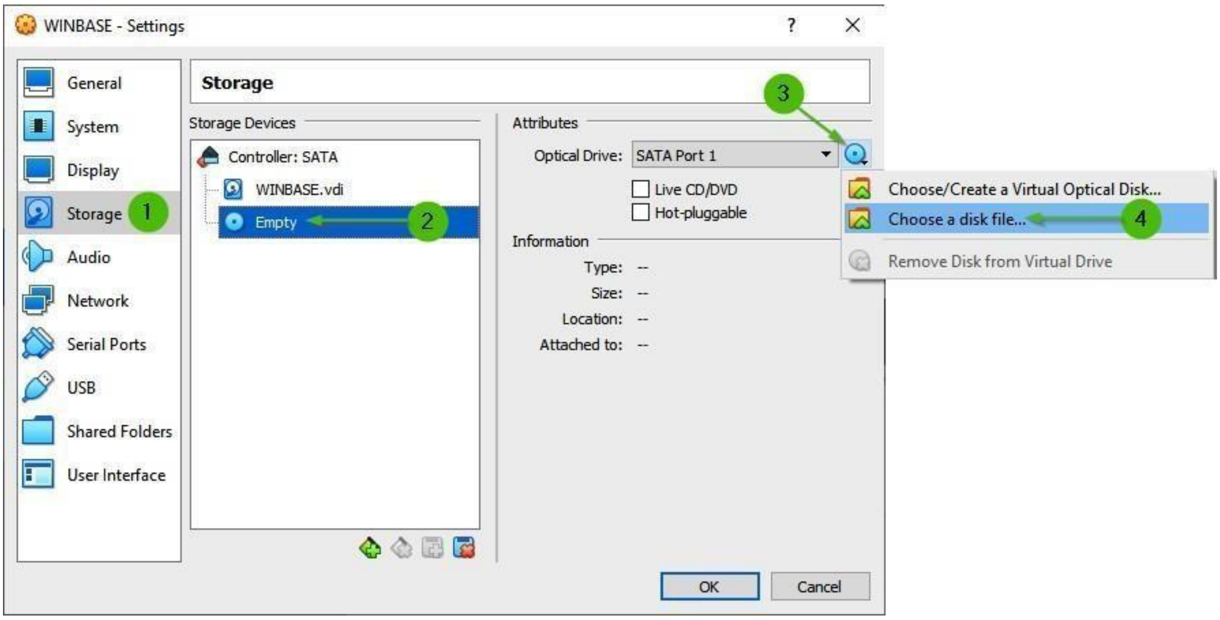
40.00 GB



Oracle VM VirtualBox Manager

Name: WINBASE
Operating System: Windows 2019 (64-bit)

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk



Storage

Storage Devices

Controller: SATA
WINBASE.vdi
Empty

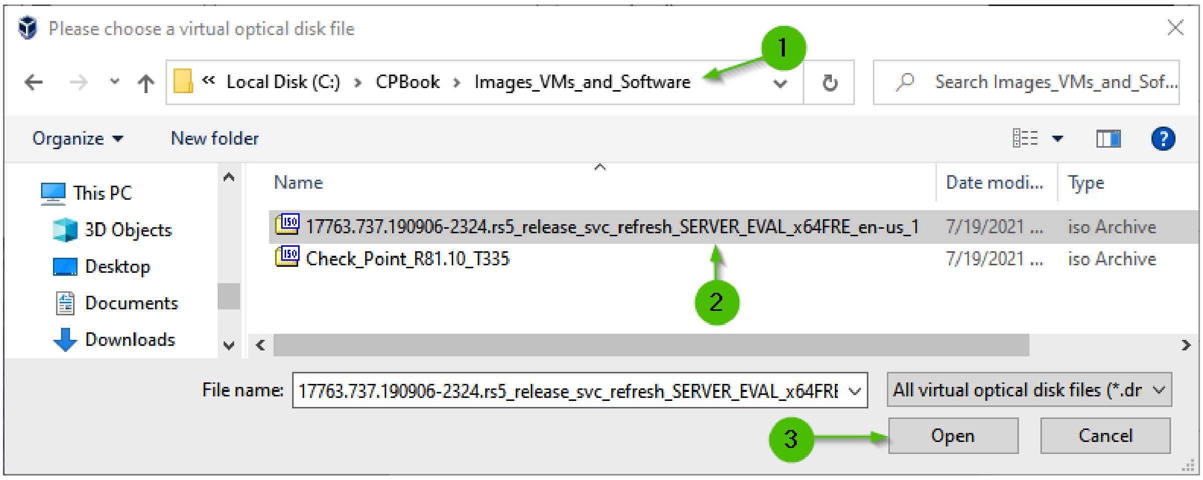
Attributes

Optical Drive: SATA Port 1

☐ Live CD/DVD
☐ Hot-pluggable

Information

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



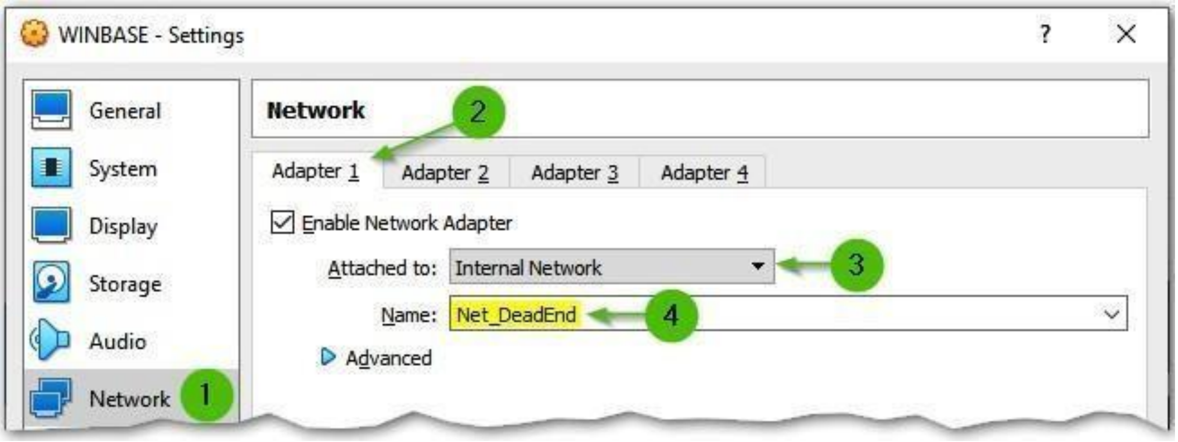
« Local Disk (C:) › CPBook › Images_VMs_and_Software

Search Images_VMs_and_Sof...

Name	Date modi...	Type
17763.737.190906-2324.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_en-us_1	7/19/2021 ...	iso Archive
Check_Point_R81.10_T335	7/19/2021 ...	iso Archive

File name: 17763.737.190906-2324.rs5_release_svc_refresh_SERVER_EVAL_x64FRE

All virtual optical disk files (*.dr

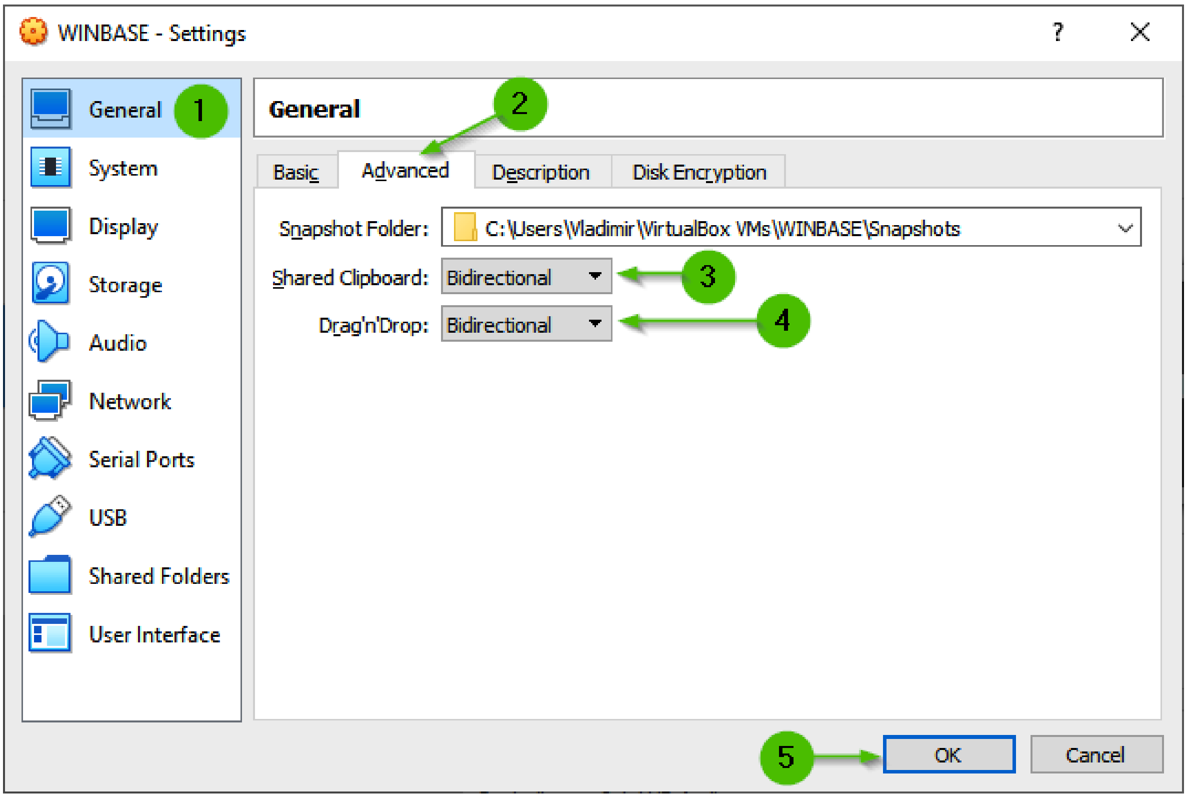


Network

☑ Enable Network Adapter

Attached to: Internal Network

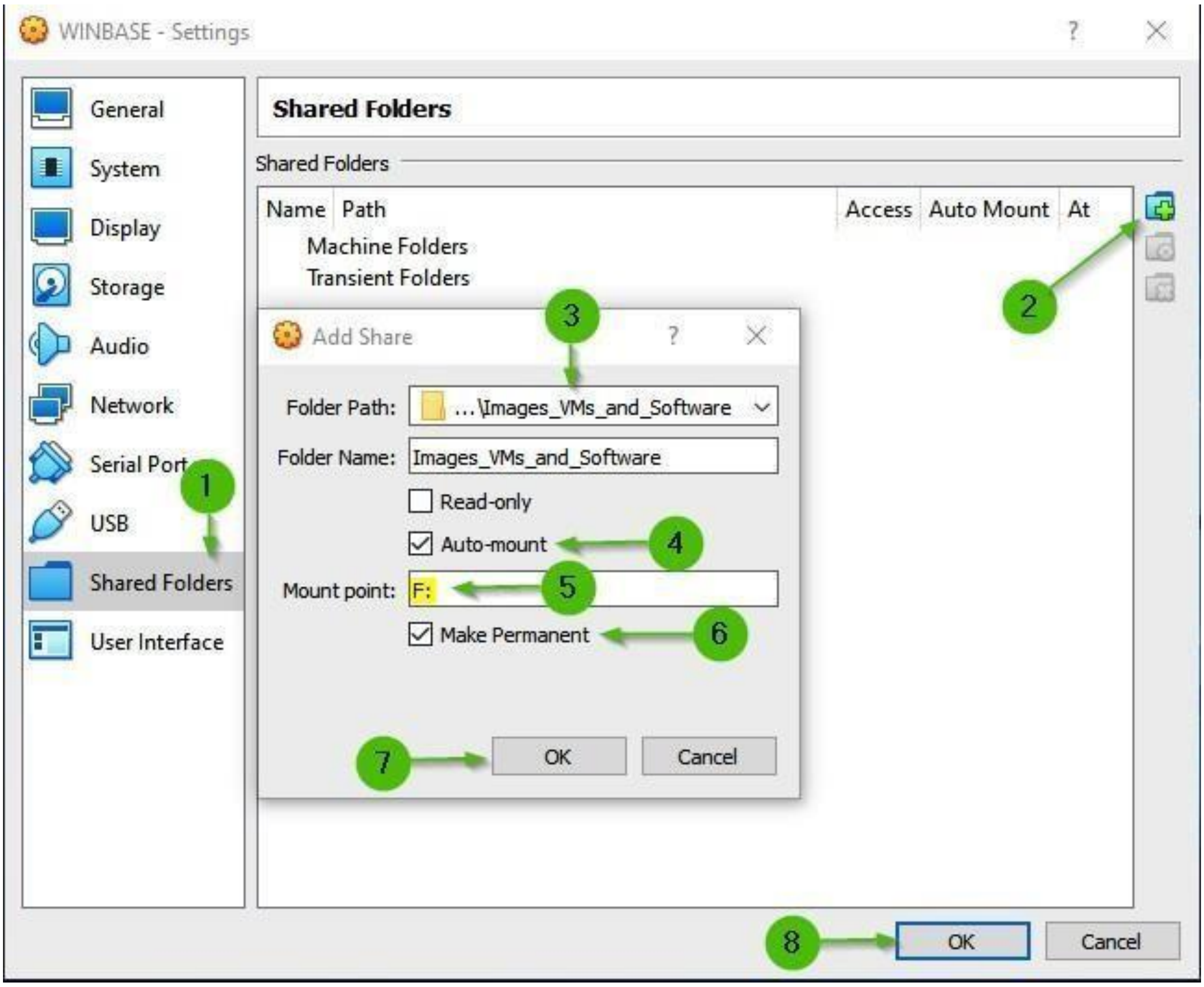
Name: Net_DeadEnd



Snapshot Folder: C:\Users\Vladimir\VirtualBox VMs\WINBASE\Snapshots

Shared Clipboard: Bidirectional

Drag'n'Drop: Bidirectional



Folder Path: ...\Images_VMs_and_Software

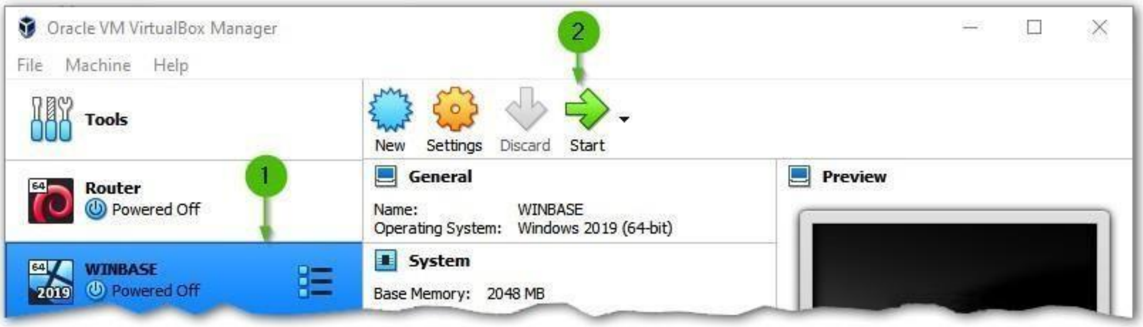
Folder Name: Images_VMs_and_Software

□ Read-only

☑ Auto-mount

Mount point: F:

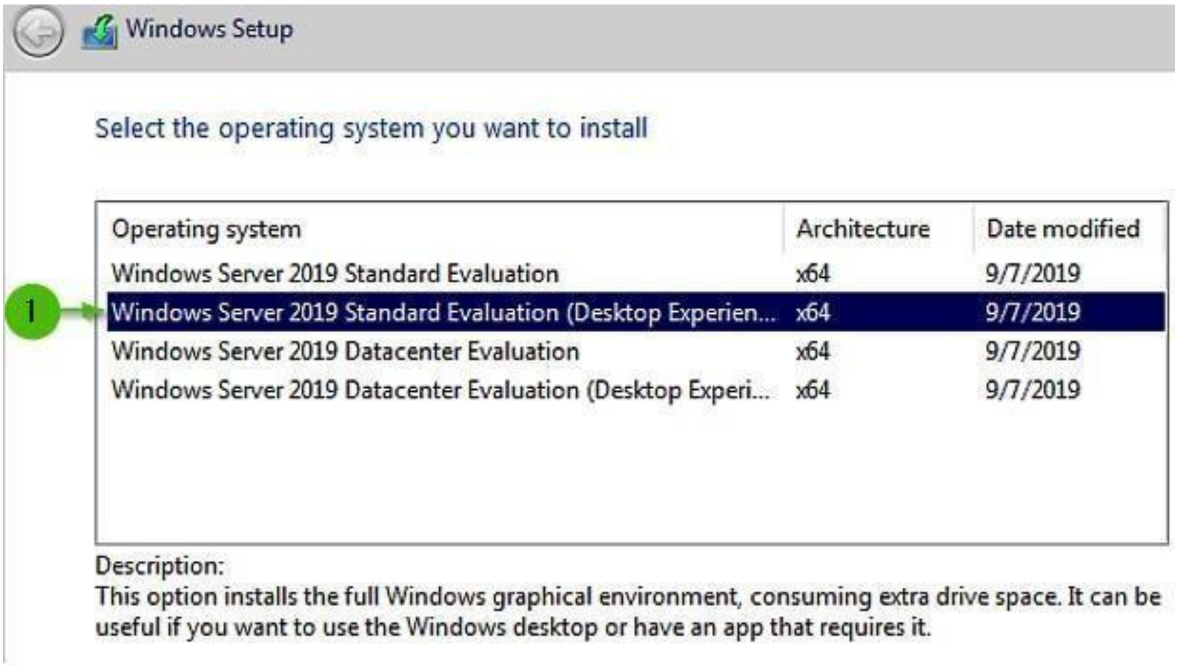
☑ Make Permanent



Name: WINBASE

Operating System: Windows 2019 (64-bit)

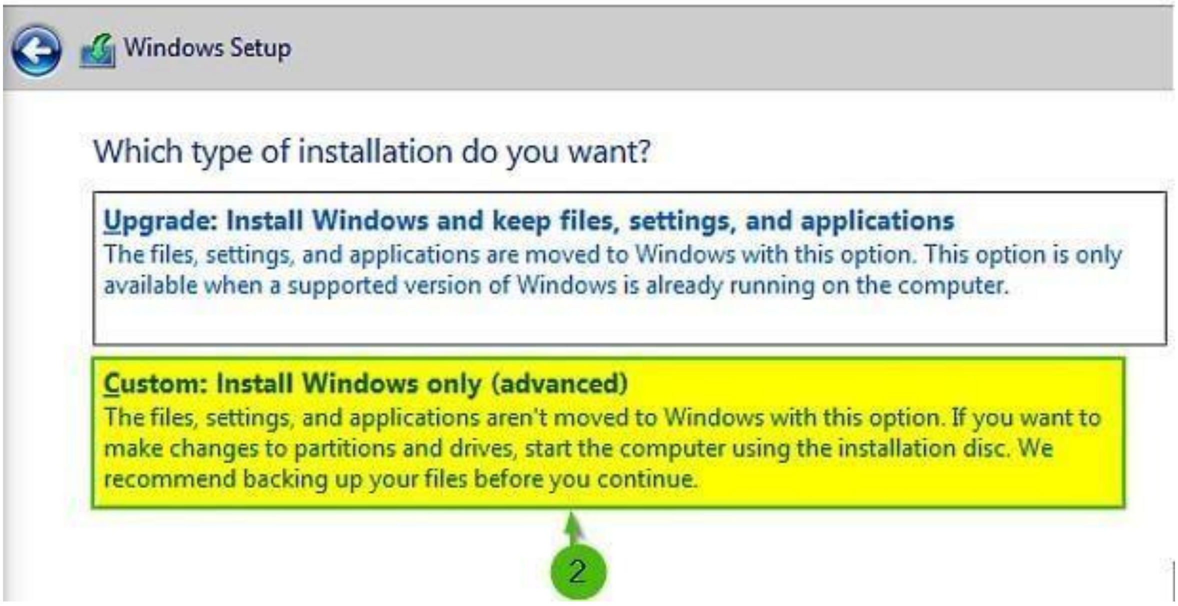
Base Memory: 2048 MB



Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2019 Standard Evaluation	x64	9/7/2019
Windows Server 2019 Standard Evaluation (Desktop Experien...	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation	x64	9/7/2019
Windows Server 2019 Datacenter Evaluation (Desktop Experi...	x64	9/7/2019

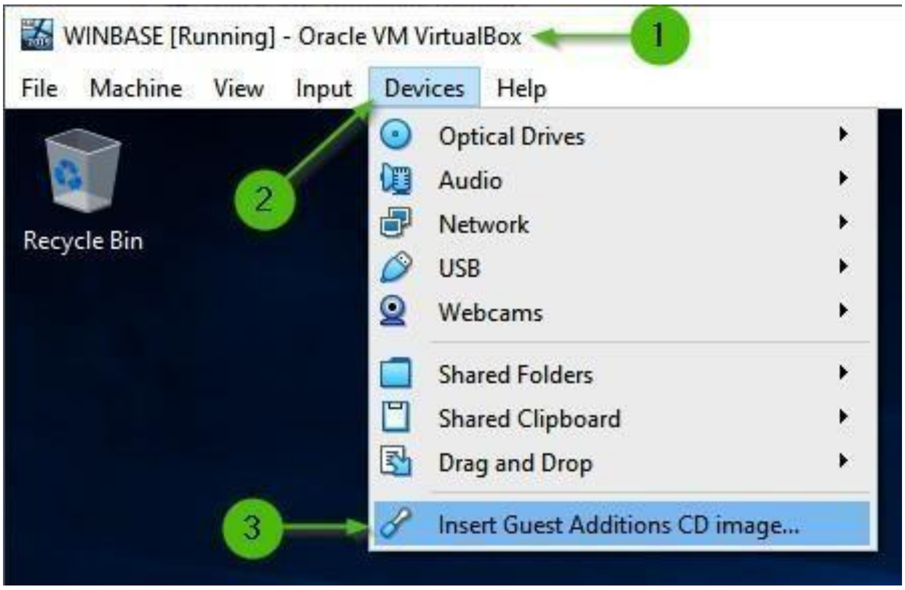
Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.

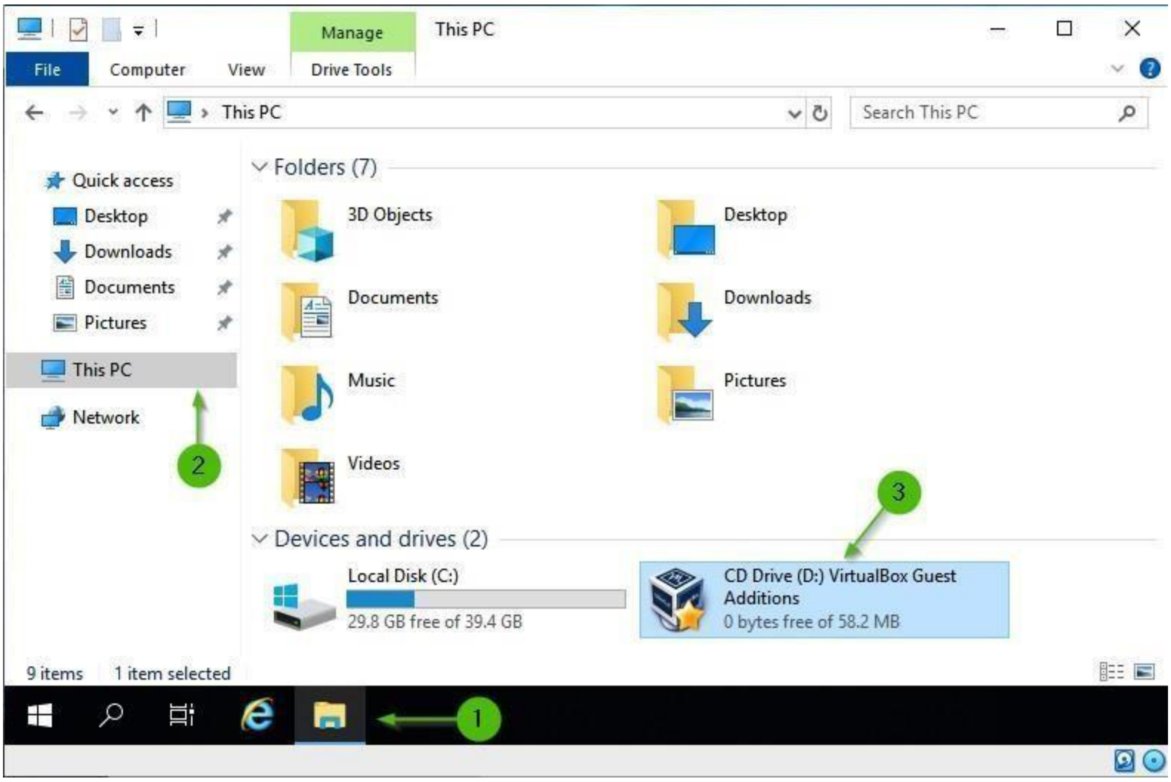


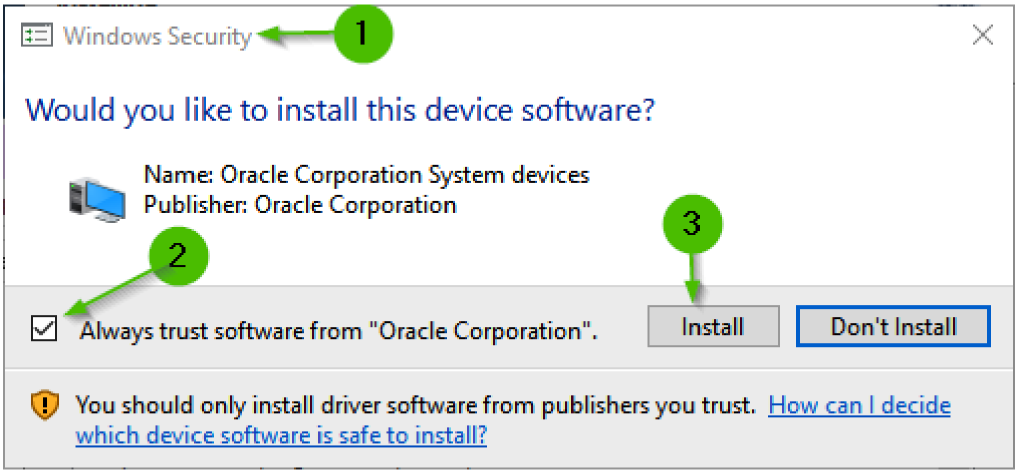
Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.


WINBASE [Running] - Oracle VM VirtualBox
1
File
Machine
View
Input
Devices
Help
2
Recycle Bin
Optical Drives
Audio
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
3
Insert Guest Additions CD image...


Manage
This PC
File
Computer
View
Drive Tools
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
2
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
3
Devices and drives (2)
Local Disk (C:)
29.8 GB free of 39.4 GB
CD Drive (D:) VirtualBox Guest Additions
0 bytes free of 58.2 MB
9 items
1 item selected
1



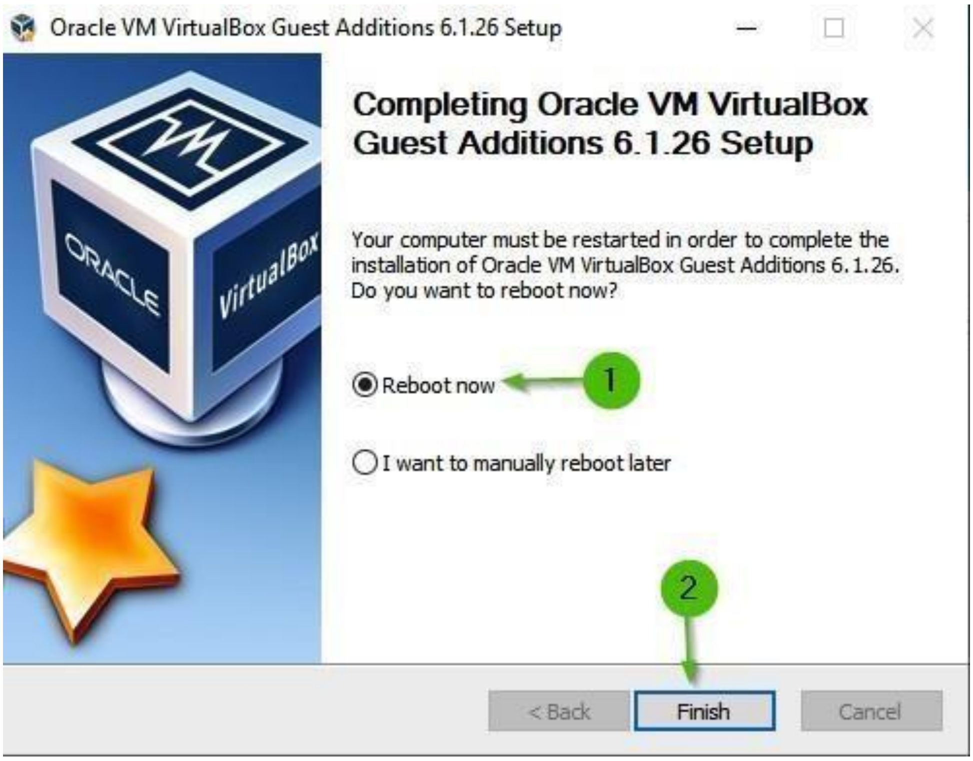
Windows Security

Would you like to install this device software?

Name: Oracle Corporation System devices
Publisher: Oracle Corporation

☑ Always trust software from "Oracle Corporation".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?



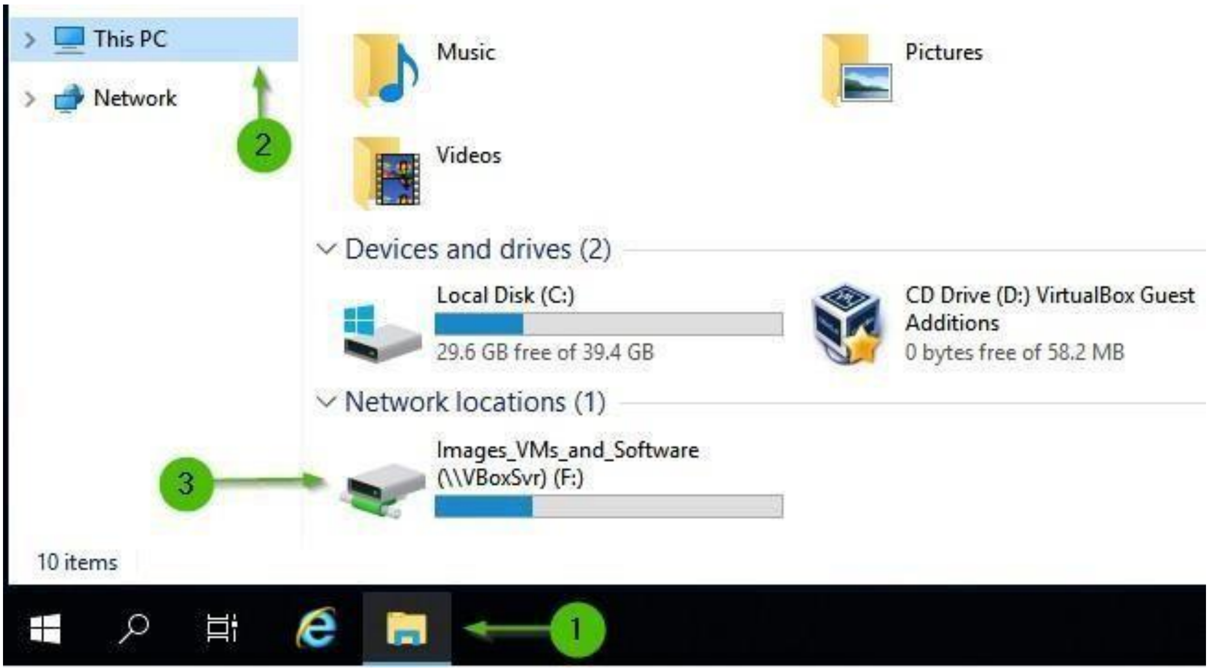
Oracle VM VirtualBox Guest Additions 6.1.26 Setup

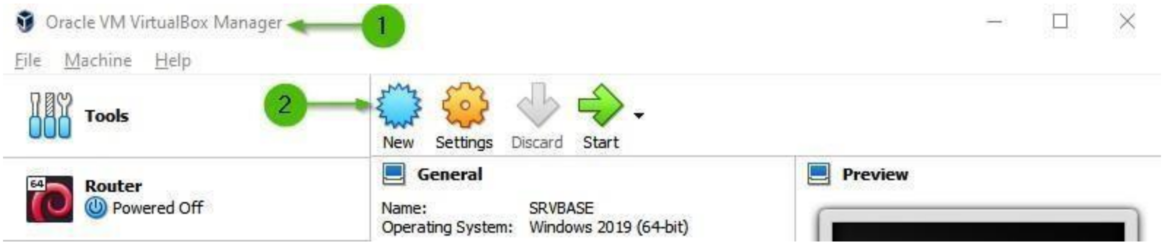
Completing Oracle VM VirtualBox Guest Additions 6.1.26 Setup

Your computer must be restarted in order to complete the installation of Oracle VM VirtualBox Guest Additions 6.1.26. Do you want to reboot now?

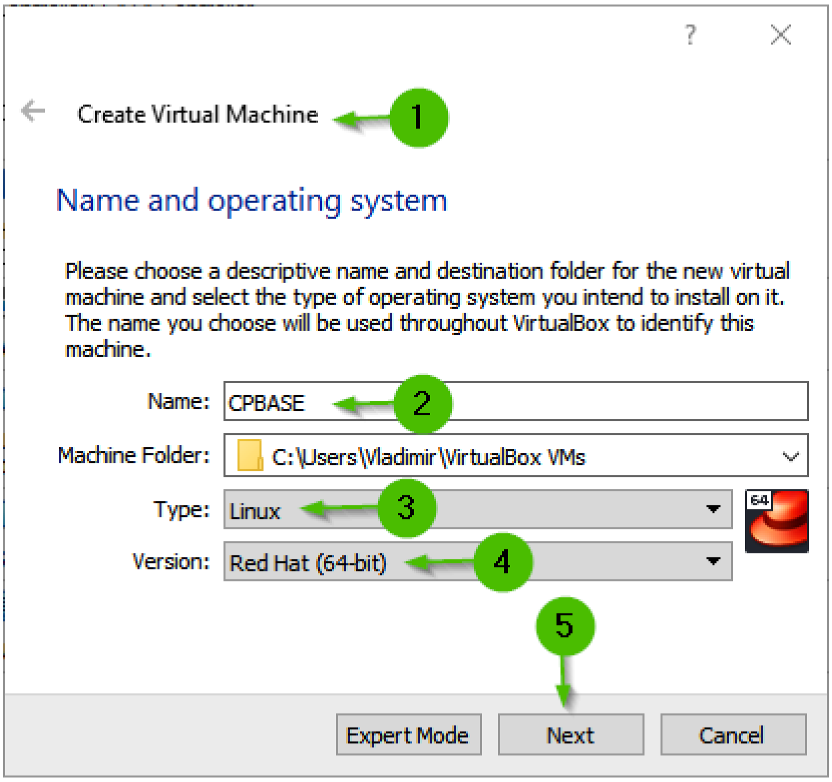
● Reboot now

○ I want to manually reboot later





Name: SRVBASE
Operating System: Windows 2019 (64-bit)



Create Virtual Machine

Name and operating system

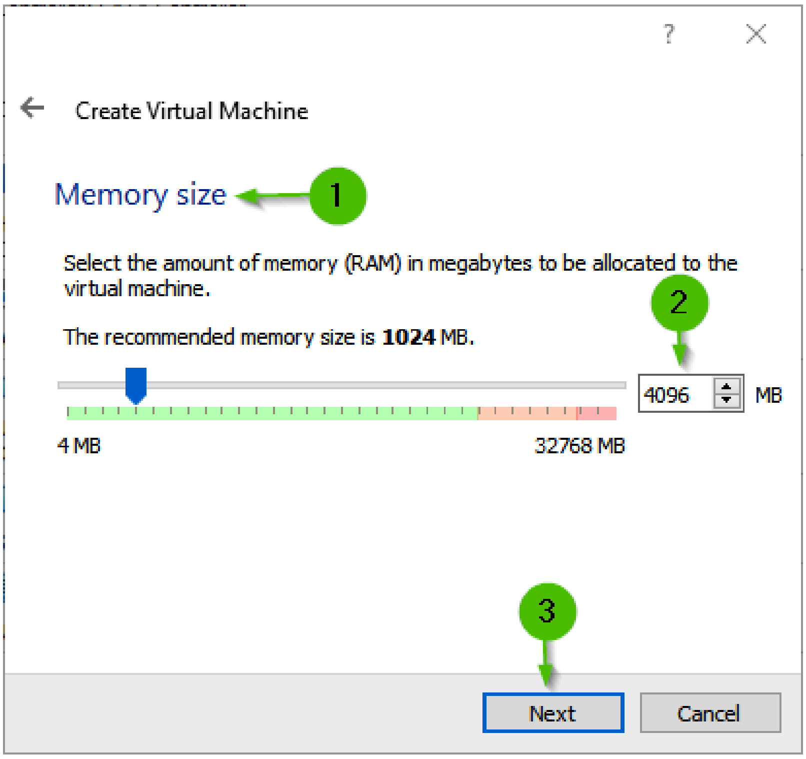
Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: CPBASE

Machine Folder: C:\Users\Vladimir\VirtualBox VMs

Type: Linux

Version: Red Hat (64-bit)



Create Virtual Machine

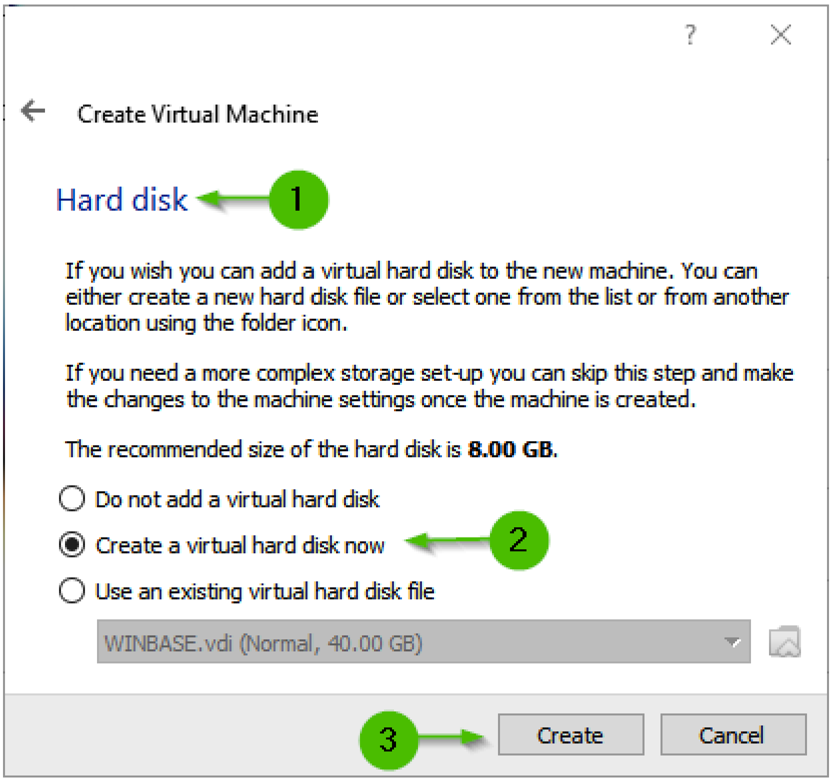
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

4096 MB

4 MB 32768 MB



Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

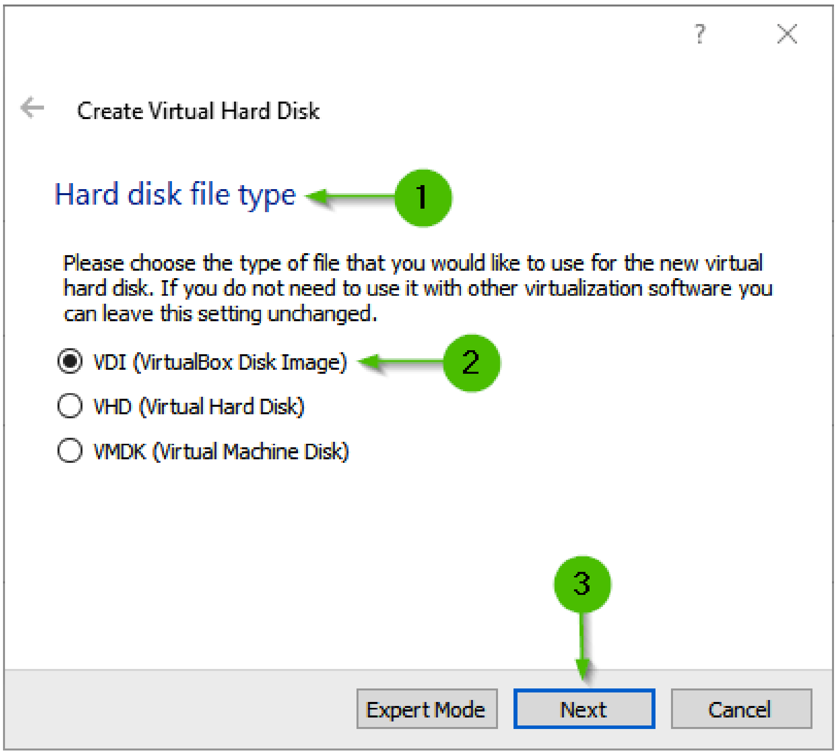
The recommended size of the hard disk is **8.00 GB**.

○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

WINBASE.vdi (Normal, 40.00 GB)



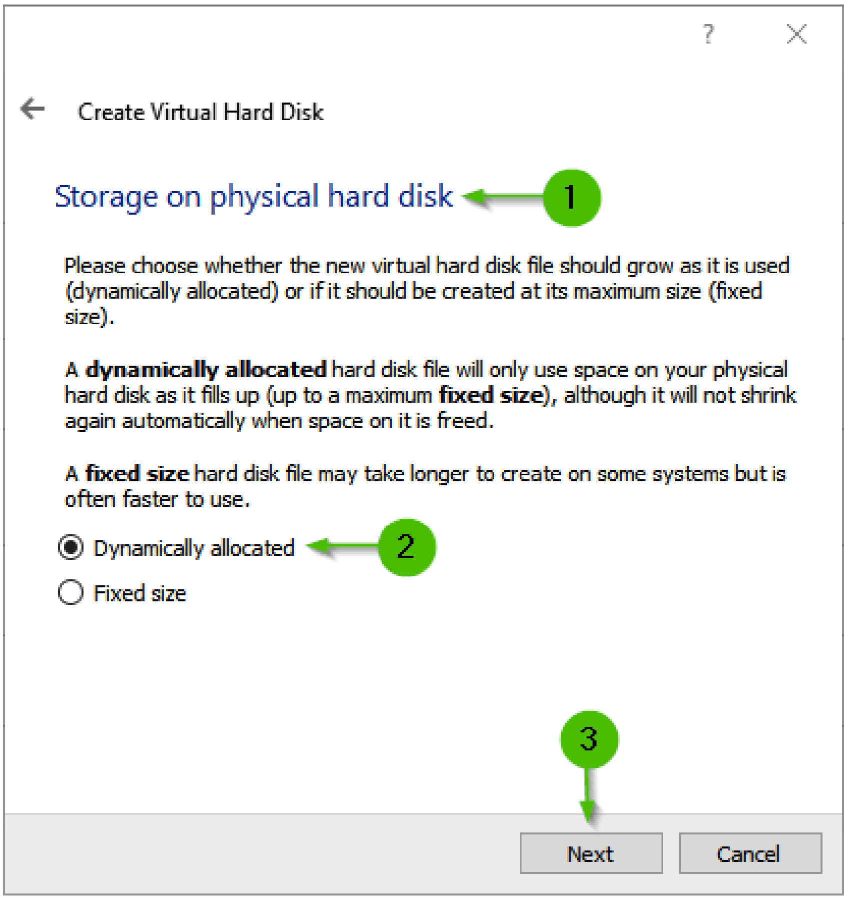
Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)



Create Virtual Hard Disk

Storage on physical hard disk

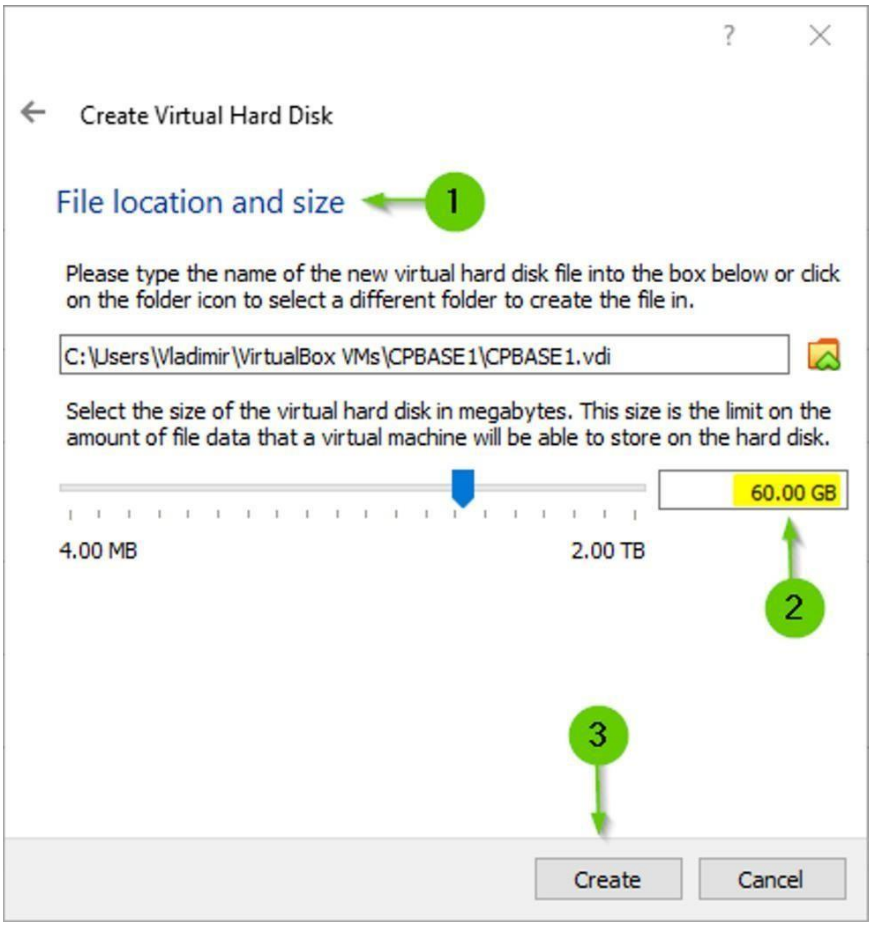
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size



Create Virtual Hard Disk

File location and size

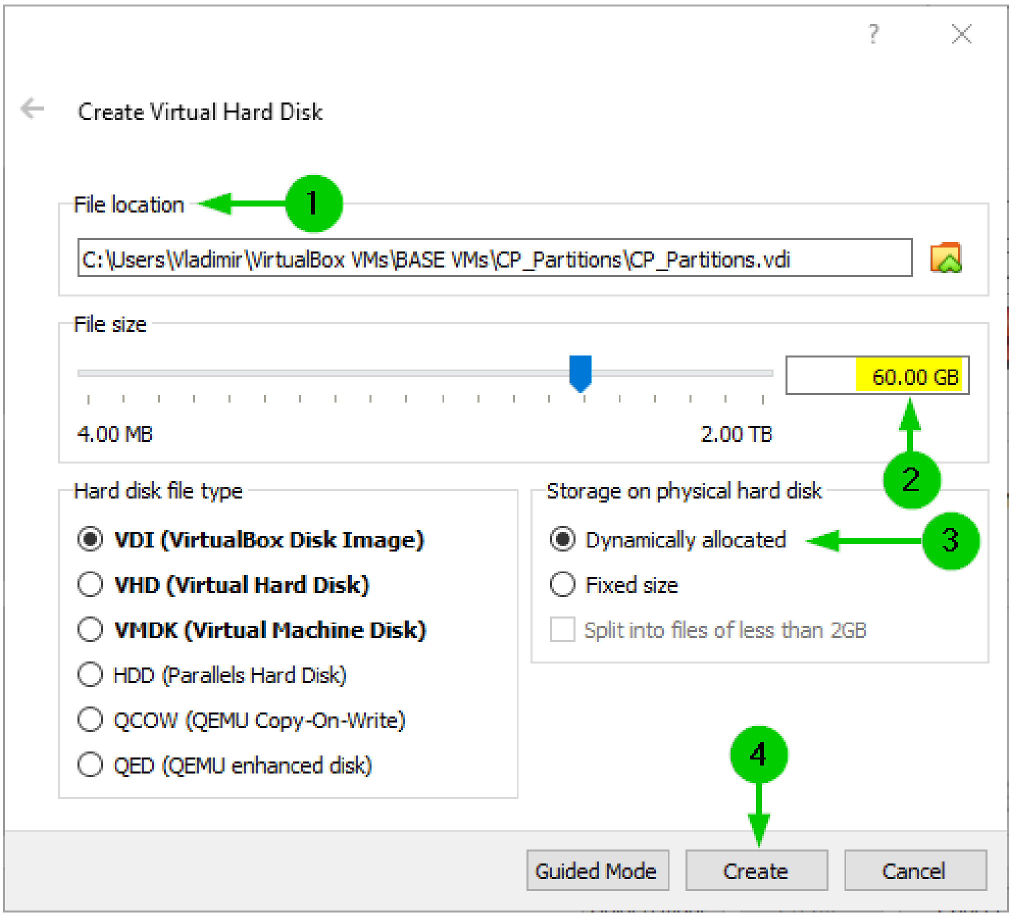
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\Users\Vladimir\VirtualBox VMs\CPBASE1\CPBASE1.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

60.00 GB

4.00 MB 2.00 TB



Create Virtual Hard Disk

File location

C:\Users\Vladimir\VirtualBox VMs\BASE VMs\CP_Partitions\CP_Partitions.vdi

File size

60.00 GB

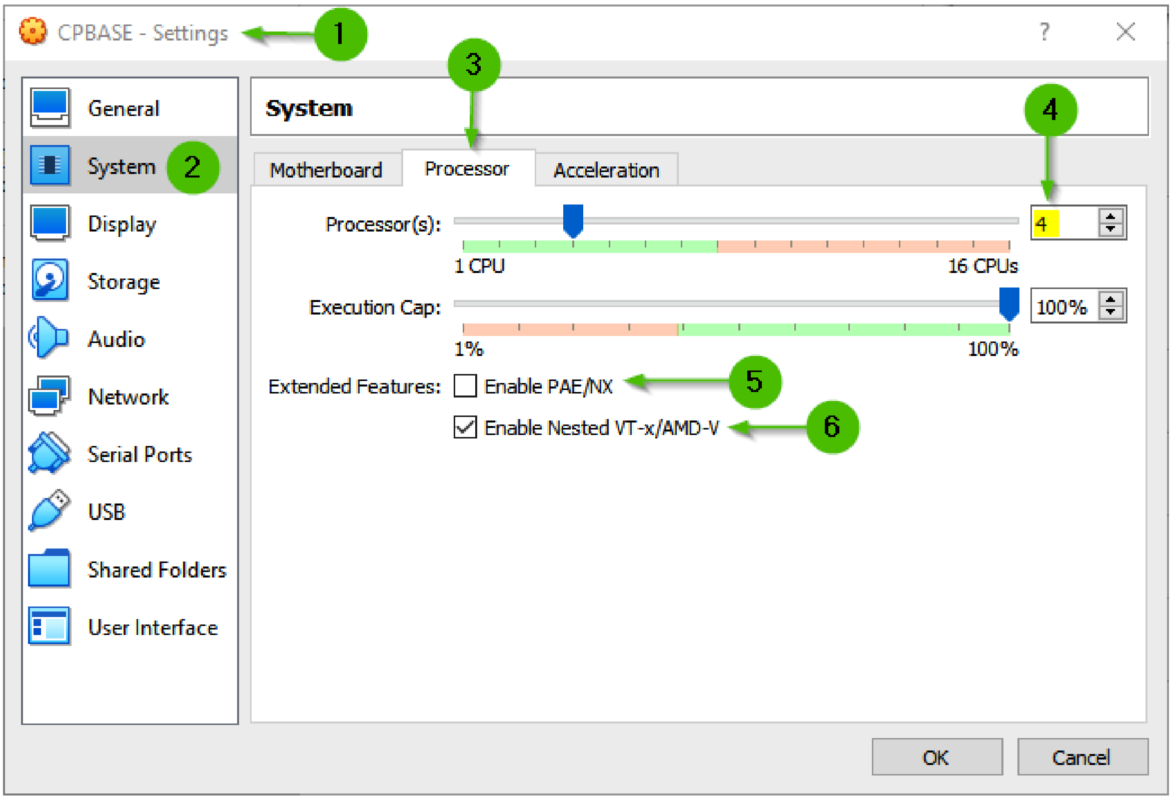
4.00 MB 2.00 TB

Hard disk file type

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

Storage on physical hard disk

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



CPBASE - Settings

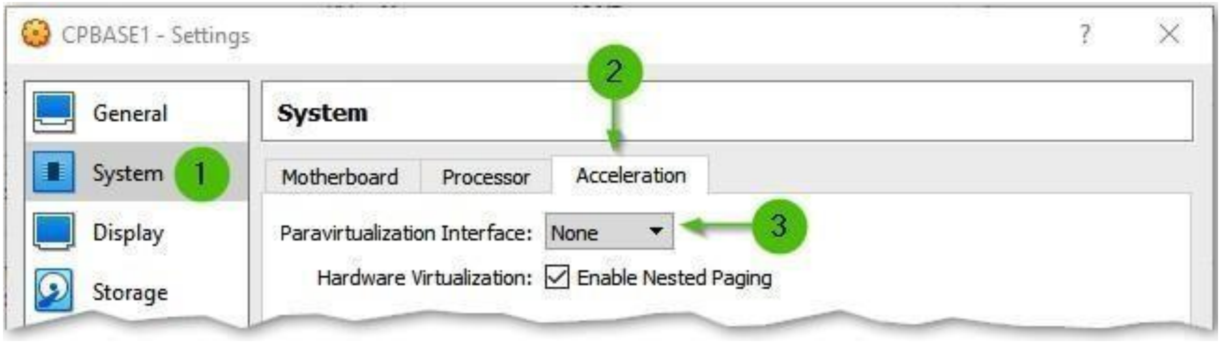
System

Processor(s): 4

Execution Cap: 100%

Extended Features: □ Enable PAE/NX

☑ Enable Nested VT-x/AMD-V

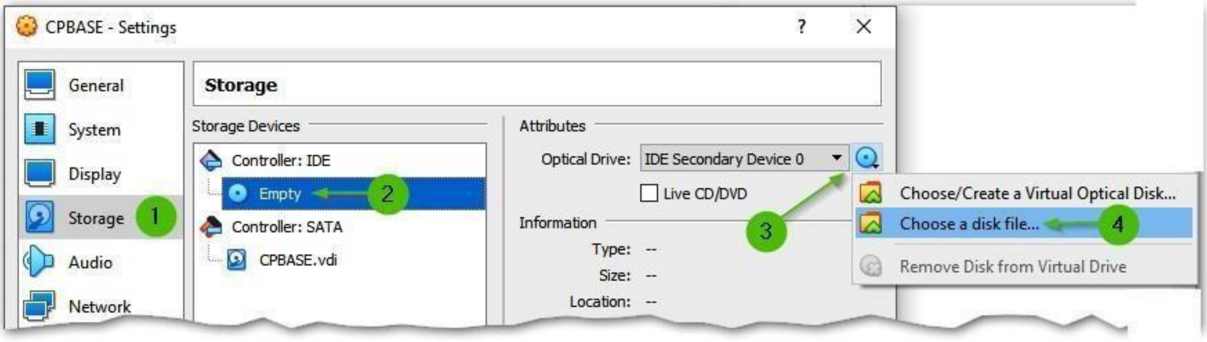


CPBASE1 - Settings

System

Paravirtualization Interface: None

Hardware Virtualization: ☑ Enable Nested Paging



CPBASE - Settings

Storage

Storage Devices

Controller: IDE
Empty
Controller: SATA
CPBASE.vdi

Attributes

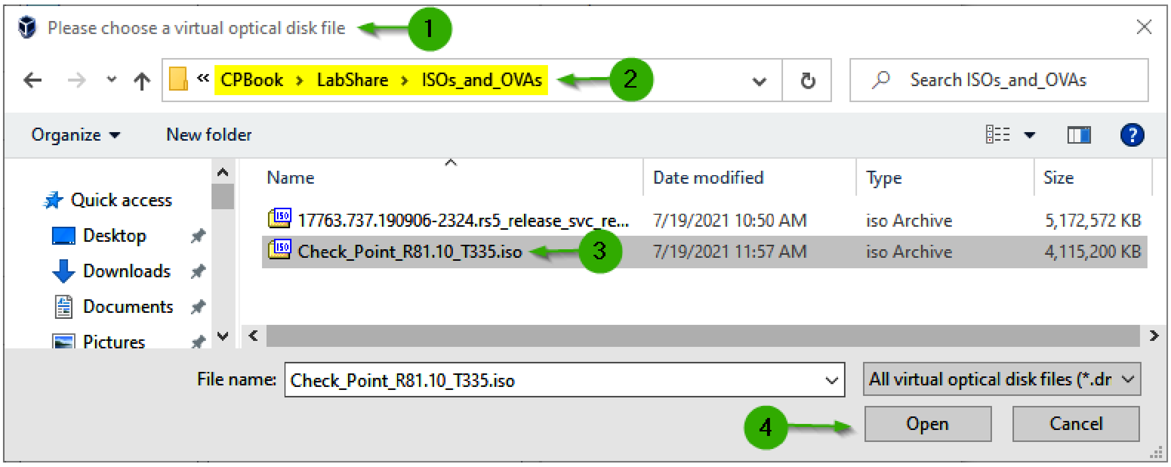
Optical Drive: IDE Secondary Device 0

□ Live CD/DVD

Information

Type: --
Size: --
Location: --

?
General
System
Display
Storage
Audio
Network
Choose/Create a Virtual Optical Disk...
Choose a disk file...
Remove Disk from Virtual Drive
1
2
3
4



Please choose a virtual optical disk file

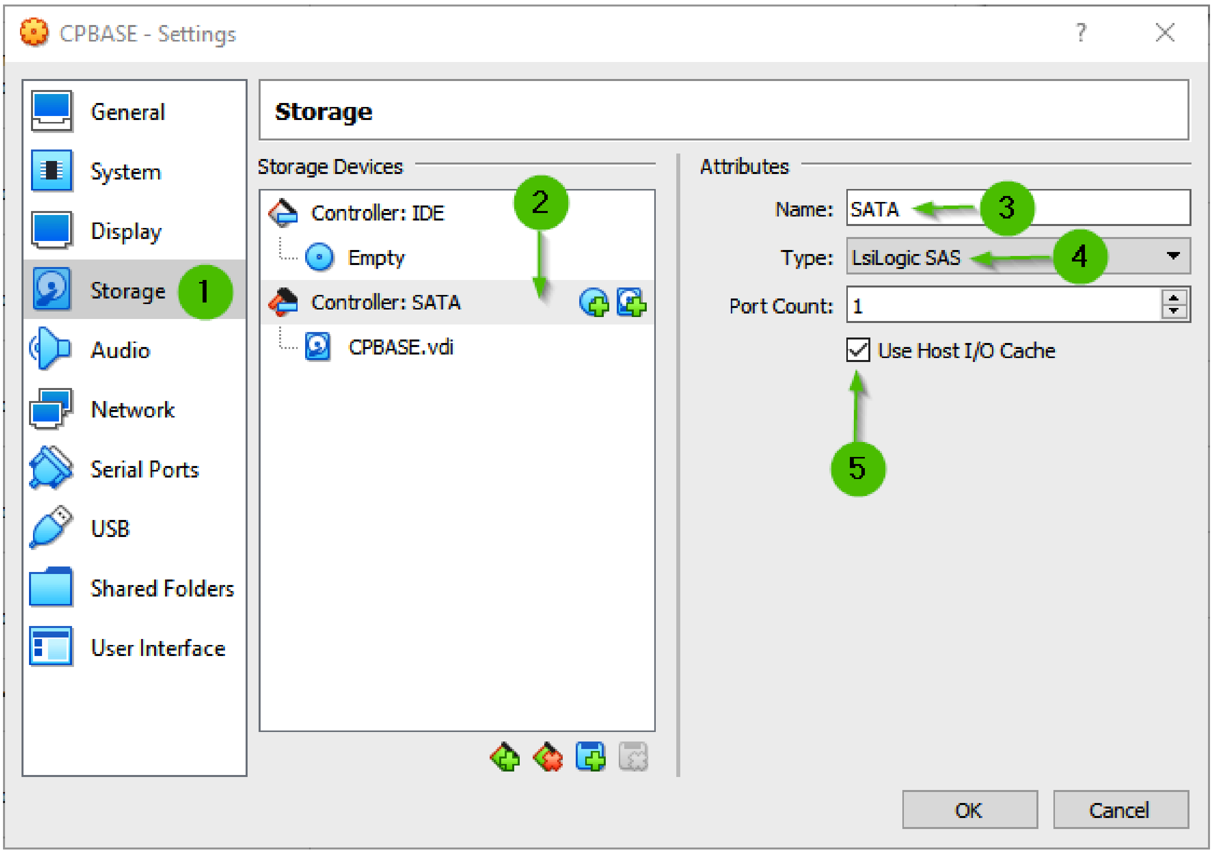
« CPBook › LabShare › ISOs_and_OVAs

Search ISOs_and_OVAs

Name	Date modified	Type	Size
17763.737.190906-2324.rs5_release_svc_re...	7/19/2021 10:50 AM	iso Archive	5,172,572 KB
Check_Point_R81.10_T335.iso	7/19/2021 11:57 AM	iso Archive	4,115,200 KB

File name: Check_Point_R81.10_T335.iso

All virtual optical disk files (*.dr



CPBASE - Settings

Storage

Storage Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - CPBASE.vdi

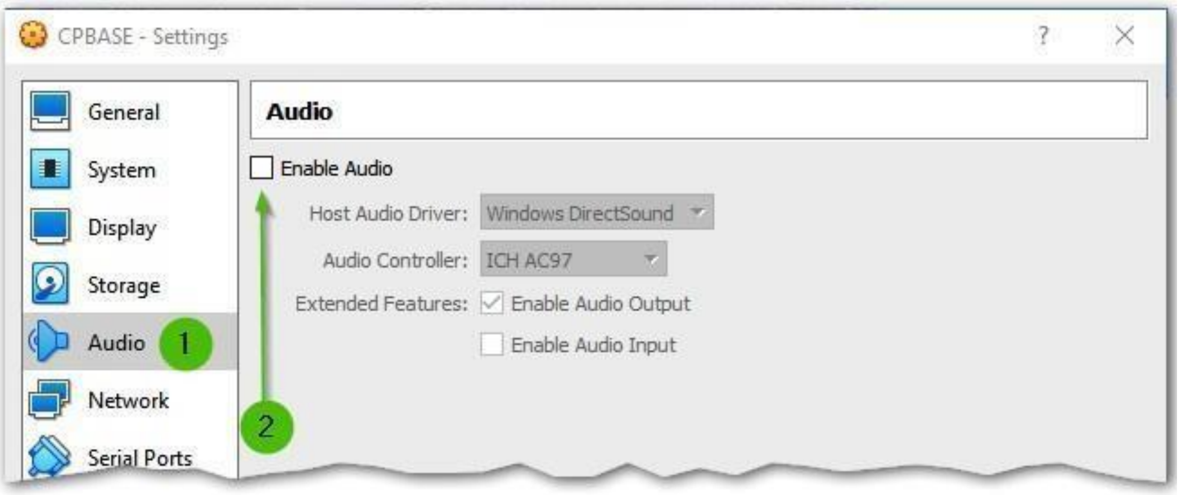
Attributes

Name: SATA

Type: LsiLogic SAS

Port Count: 1

☑ Use Host I/O Cache



CPBASE - Settings

Audio

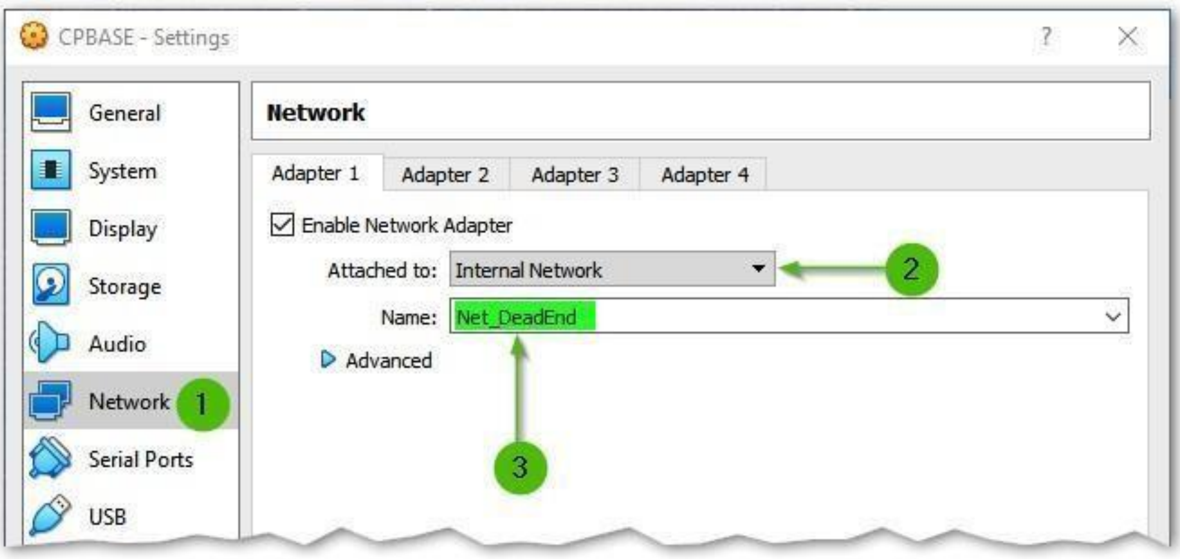
□ Enable Audio

Host Audio Driver: Windows DirectSound

Audio Controller: ICH AC97

Extended Features: ☑ Enable Audio Output

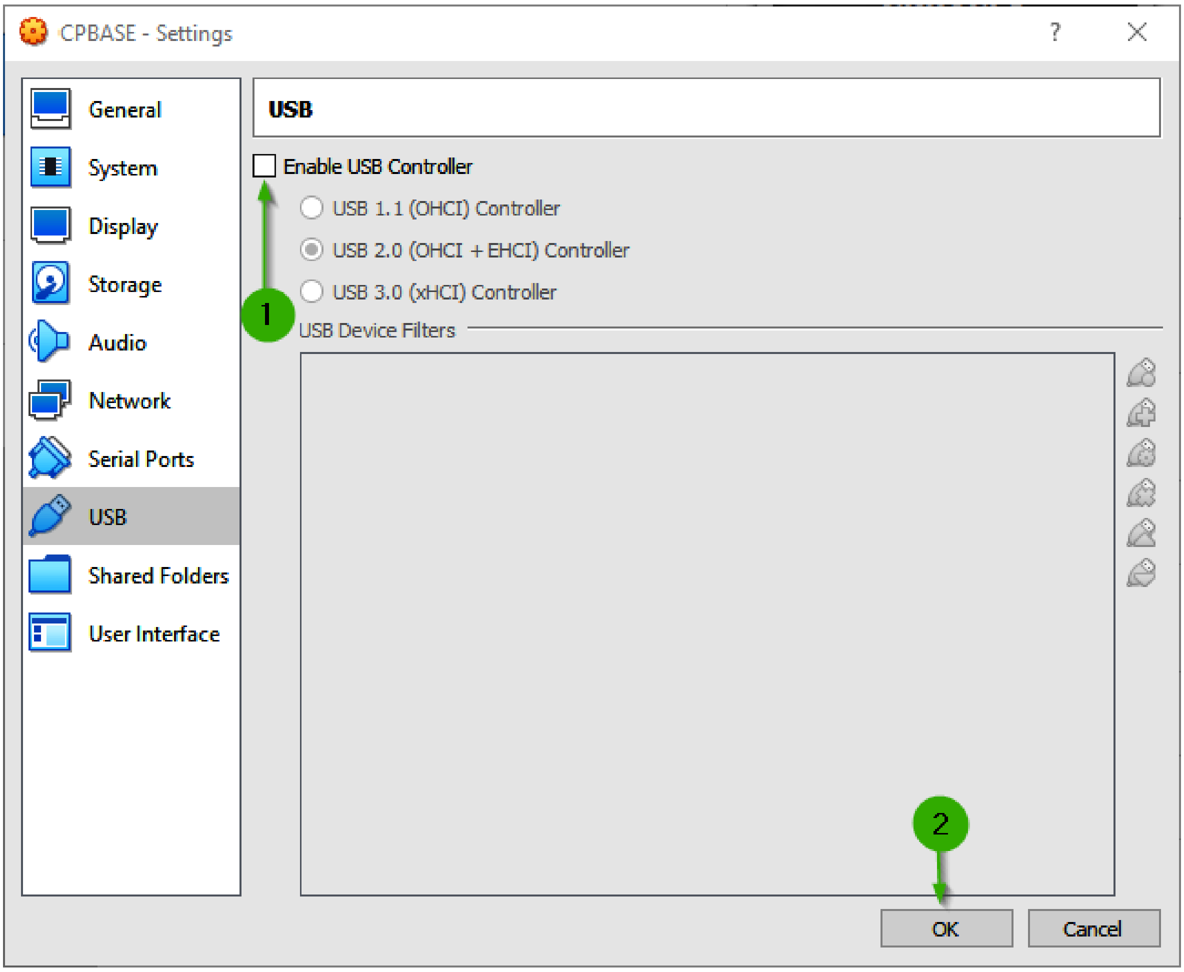
□ Enable Audio Input



☑ Enable Network Adapter

Attached to: Internal Network

Name: Net_DeadEnd

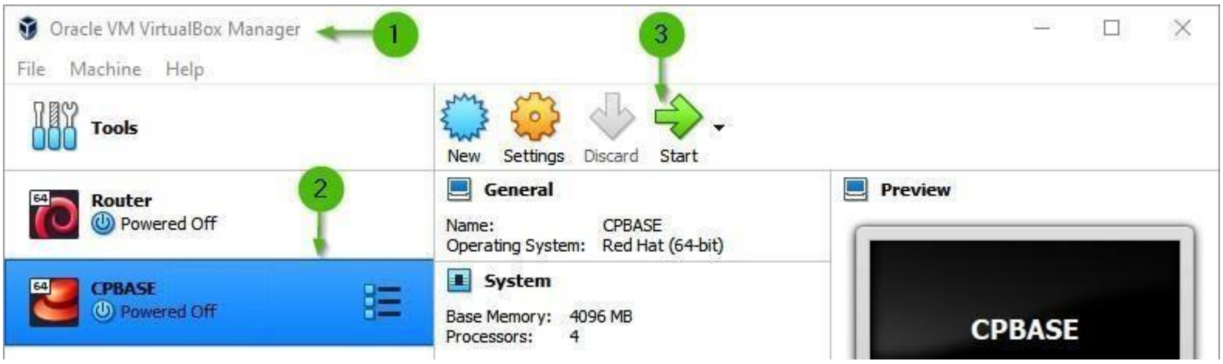


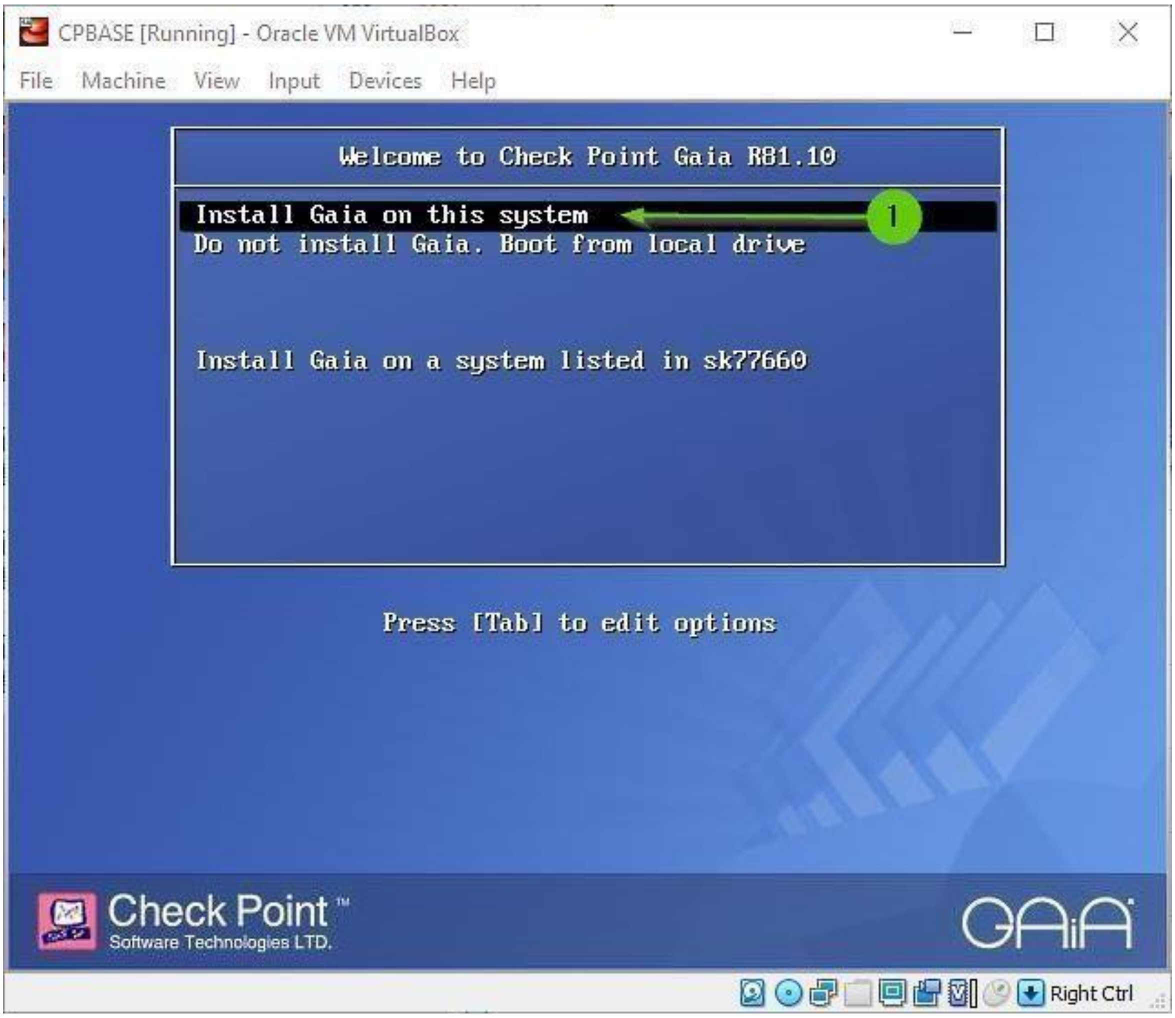
□ Enable USB Controller

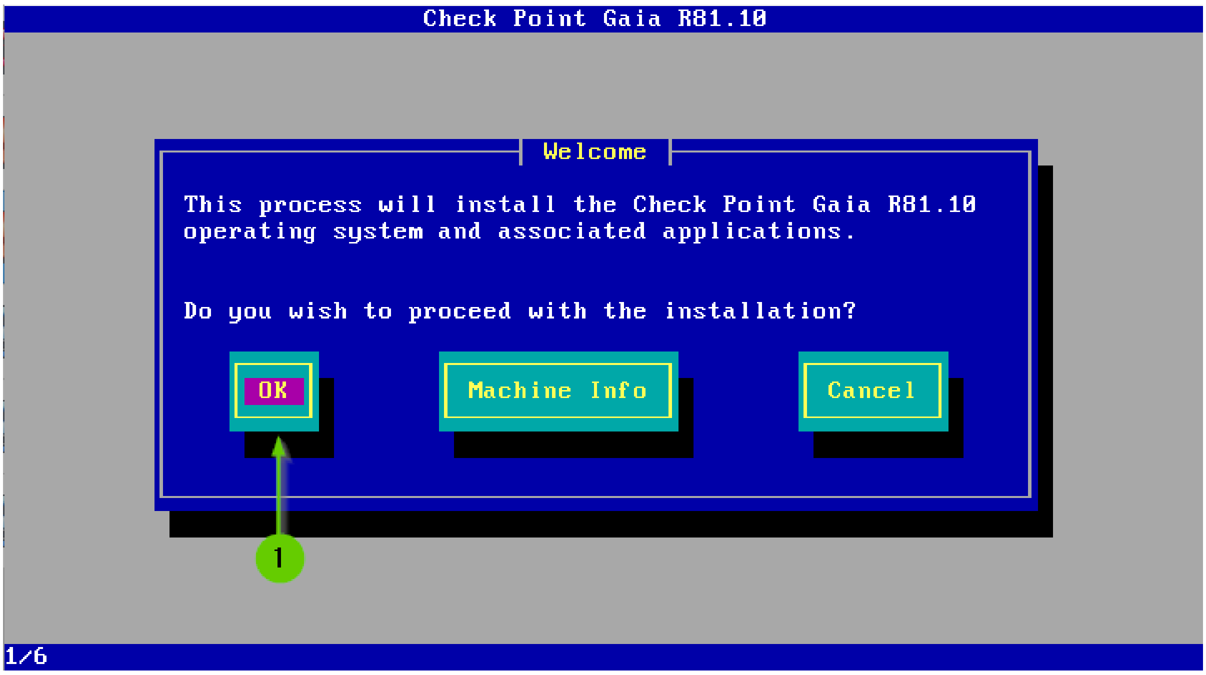
○ USB 1.1 (OHCI) Controller

● USB 2.0 (OHCI + EHCI) Controller

○ USB 3.0 (xHCI) Controller


Oracle VM VirtualBox Manager
1
File Machine Help
Tools
3
New Settings Discard Start
Router
Powered Off
2
CPBASE
Powered Off
General
Name: CPBASE
Operating System: Red Hat (64-bit)
System
Base Memory: 4096 MB
Processors: 4
Preview
CPBASE


CPBASE [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Welcome to Check Point Gaia R81.10
Install Gaia on this system
1
Do not install Gaia. Boot from local drive
Install Gaia on a system listed in sk77660
Press [Tab] to edit options
Check Point
Software Technologies LTD.
GAiA
Right Ctrl

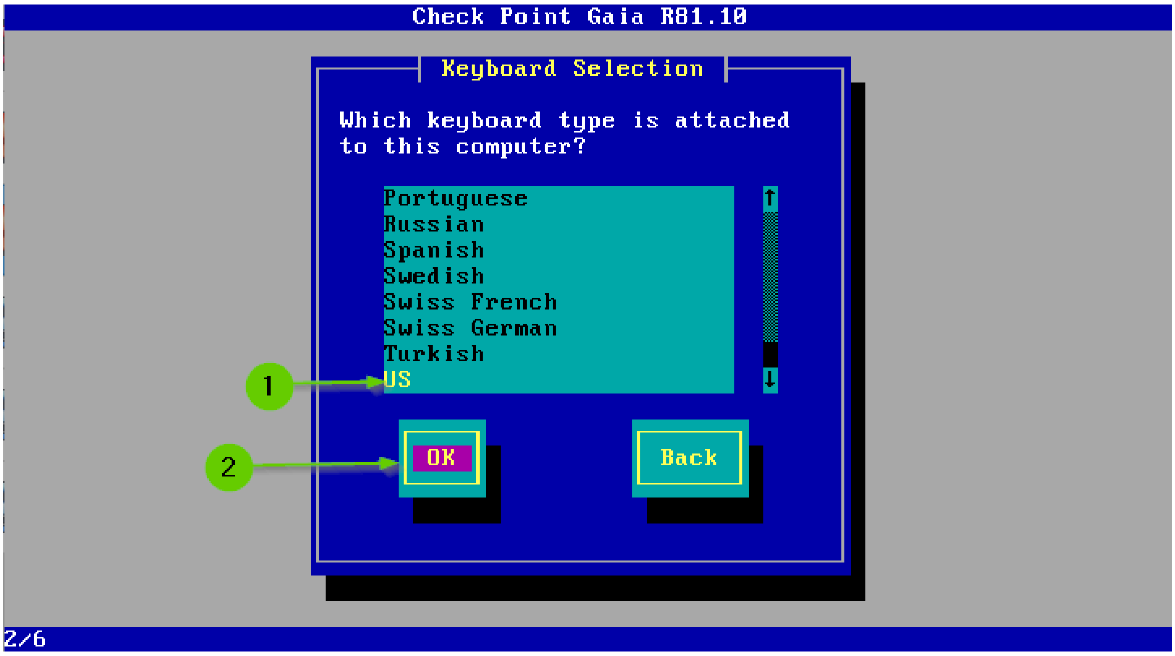


Check Point Gaia R81.10

Welcome

This process will install the Check Point Gaia R81.10 operating system and associated applications.

Do you wish to proceed with the installation?

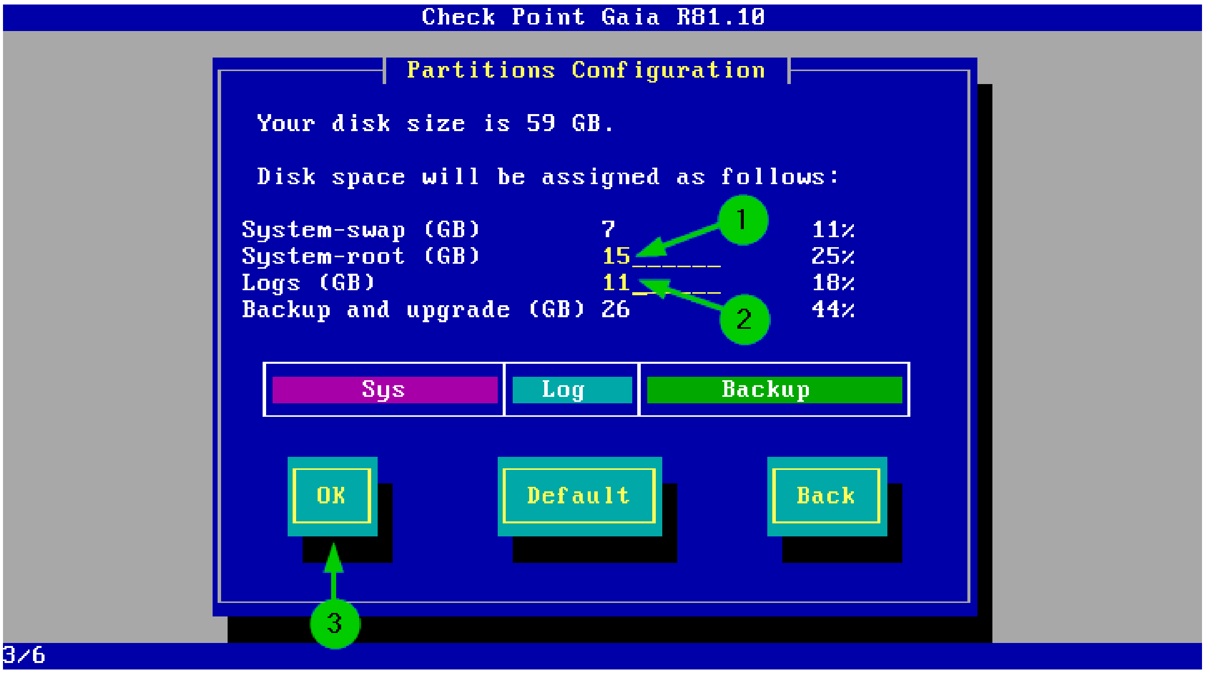


Check Point Gaia R81.10

Keyboard Selection

Which keyboard type is attached to this computer?

```
Portuguese
Russian
Spanish
Swedish
Swiss French
Swiss German
Turkish
US
```



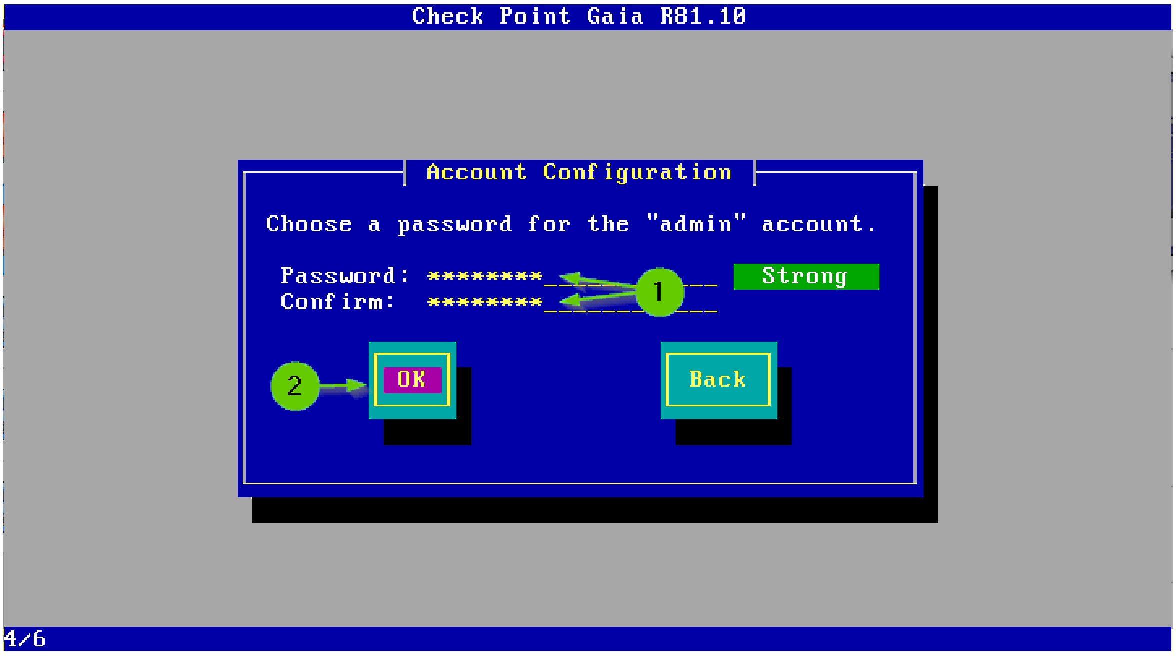
Check Point Gaia R81.10

Partitions Configuration

Your disk size is 59 GB.

Disk space will be assigned as follows:

```
System-swap (GB)           7            11%
System-root (GB)           15_______    25%
Logs (GB)                  11_______    18%
Backup and upgrade (GB) 26              44%
```

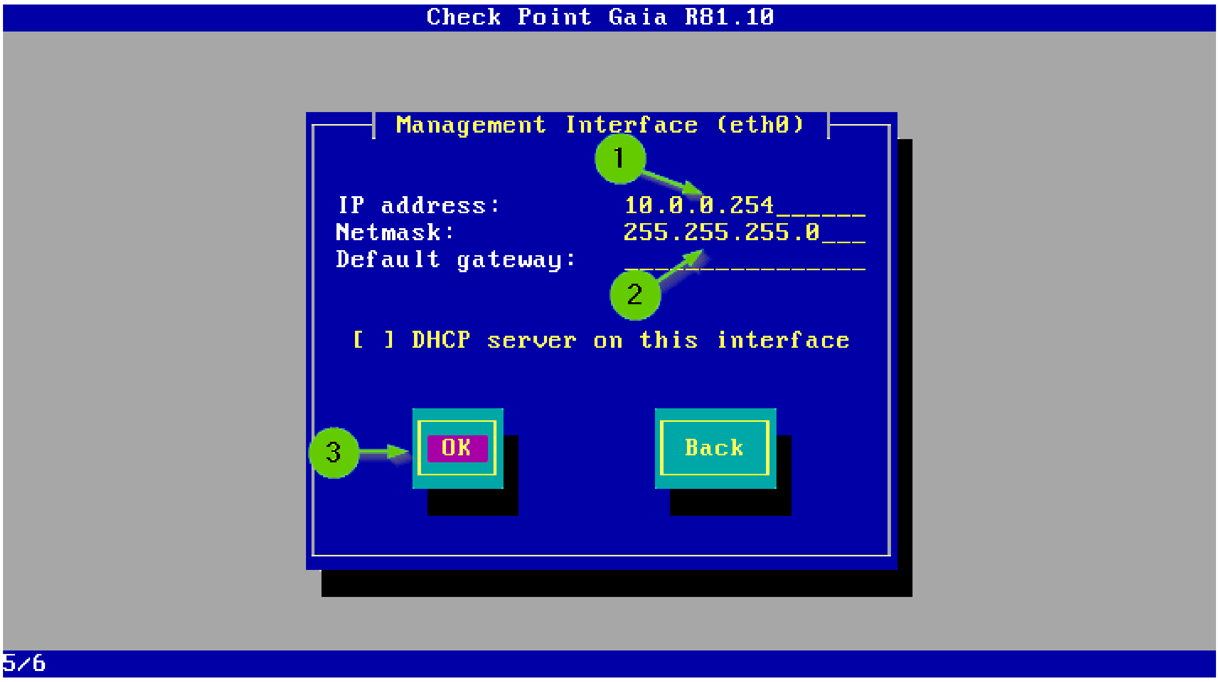


Check Point Gaia R81.10

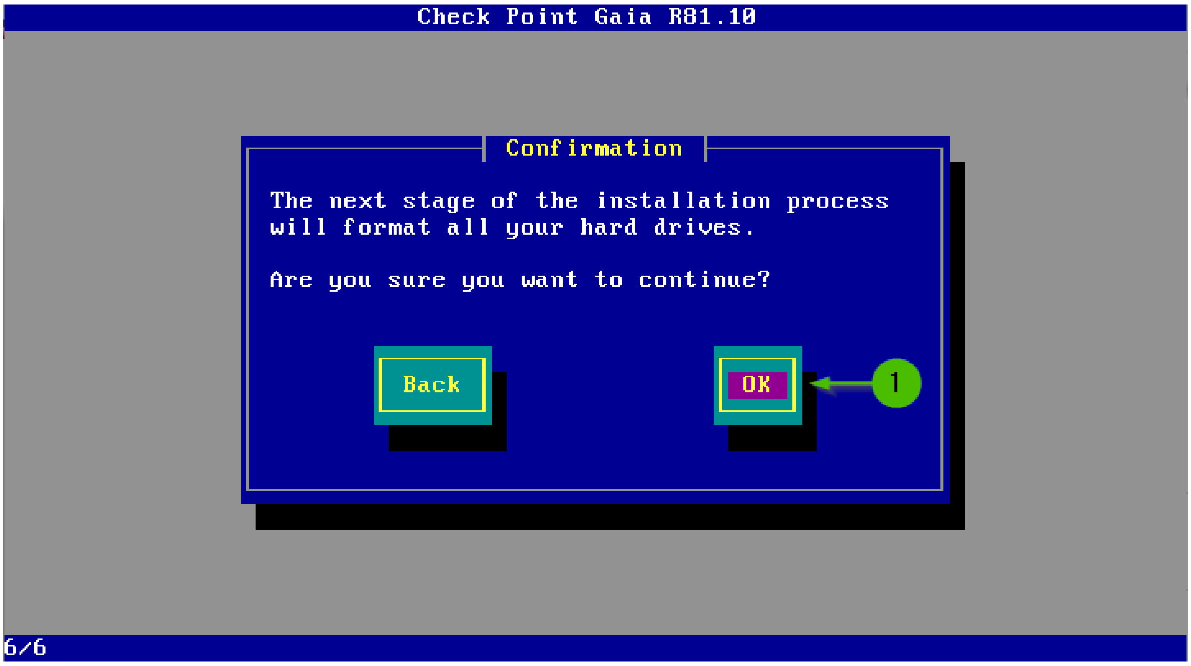
Account Configuration

Choose a password for the "admin" account.

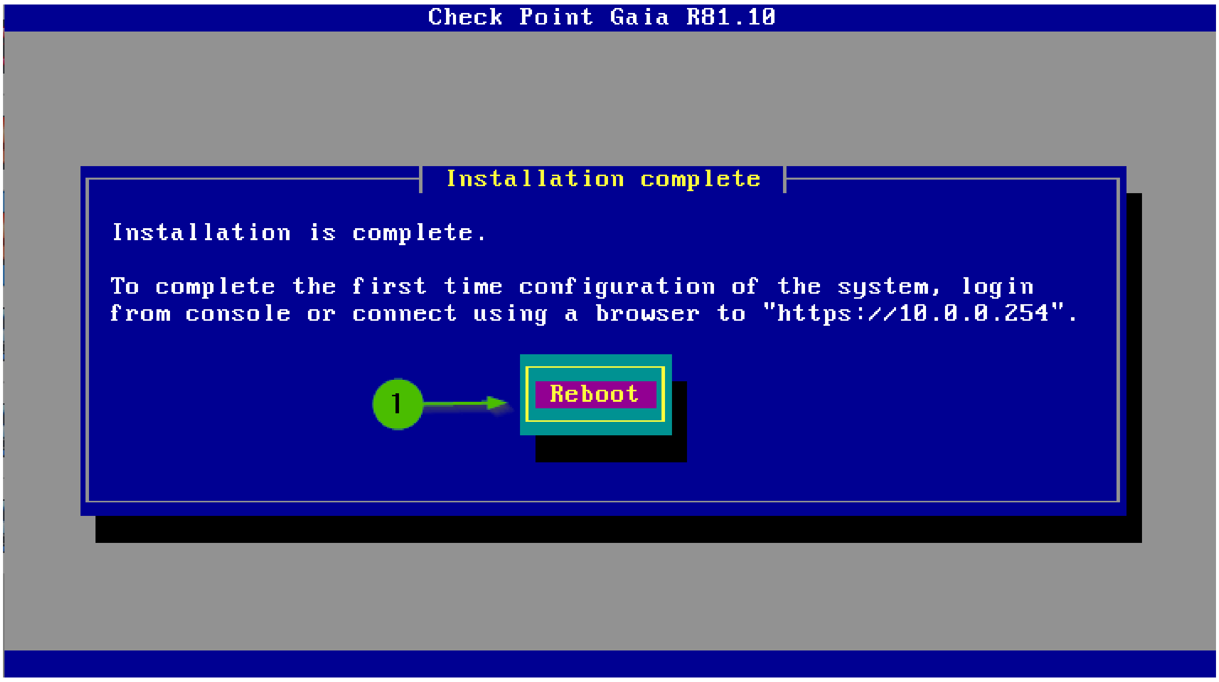
```
Password: ********_____________   Strong
Confirm:  ********_____________
```



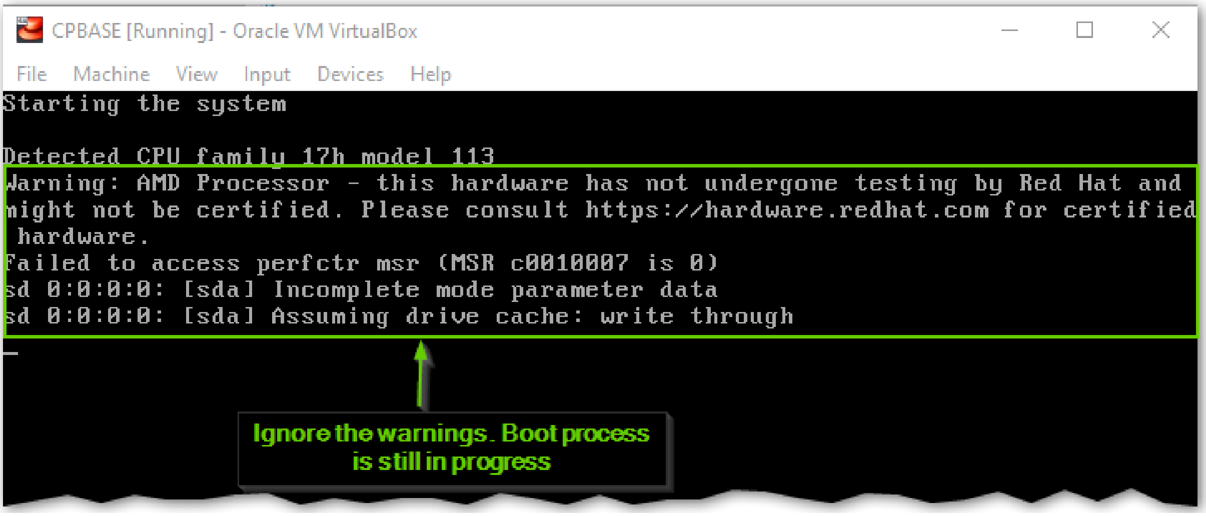
```
Check Point Gaia R81.10

Management Interface (eth0)

IP address:         10.0.0.254______
Netmask:            255.255.255.0___
Default gateway:    ________________

[ ] DHCP server on this interface

5/6
```



```
Check Point Gaia R81.10

Confirmation

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

Are you sure you want to continue?

6/6
```



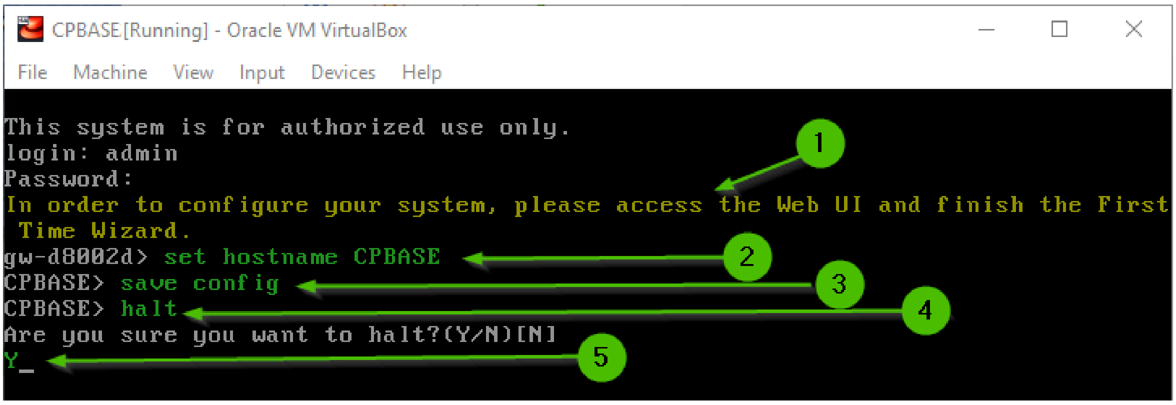
```
Check Point Gaia R81.10

Installation complete

Installation is complete.

To complete the first time configuration of the system, login
from console or connect using a browser to "https://10.0.0.254".
```



CPBASE [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

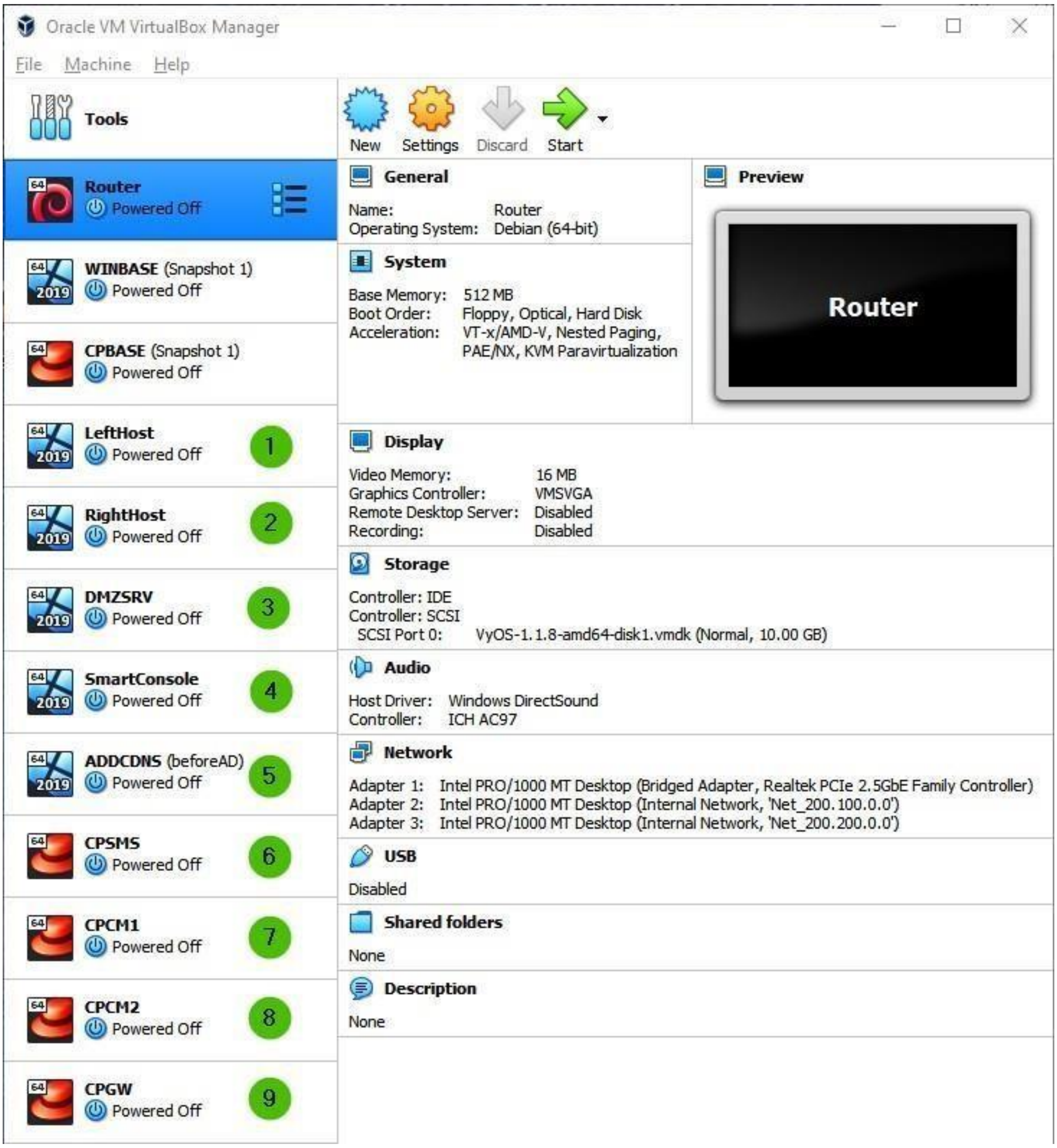
```
Starting the system

Detected CPU family 17h model 113
Warning: AMD Processor - this hardware has not undergone testing by Red Hat and
might not be certified. Please consult https://hardware.redhat.com for certified
 hardware.
Failed to access perfctr msr (MSR c0010007 is 0)
sd 0:0:0:0: [sda] Incomplete mode parameter data
sd 0:0:0:0: [sda] Assuming drive cache: write through
_
```

Ignore the warnings. Boot process is still in progress



CPBASE [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1
2
3
4
5

```
This system is for authorized use only.
login: admin
Password:
In order to configure your system, please access the Web UI and finish the First
 Time Wizard.
gw-d8002d> set hostname CPBASE
CPBASE> save config
CPBASE> halt
Are you sure you want to halt?(Y/N)[N]
Y_
```



Router Powered Off

WINBASE (Snapshot 1) Powered Off

CPBASE (Snapshot 1) Powered Off

LeftHost Powered Off 1

RightHost Powered Off 2

DMZSRV Powered Off 3

SmartConsole Powered Off 4

ADDCDNS (beforeAD) Powered Off 5

CPSMS Powered Off 6

CPCM1 Powered Off 7

CPCM2 Powered Off 8

CPGW Powered Off 9

General

```
Name:              Router
Operating System:  Debian (64-bit)
```

System

```
Base Memory:   512 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  VT-x/AMD-V, Nested Paging,
               PAE/NX, KVM Paravirtualization
```

Preview

Display

```
Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled
```

Storage

```
Controller: IDE
Controller: SCSI
 SCSI Port 0:    VyOS-1.1.8-amd64-disk1.vmdk (Normal, 10.00 GB)
```

Audio

```
Host Driver:   Windows DirectSound
Controller:    ICH AC97
```

Network

```
Adapter 1:  Intel PRO/1000 MT Desktop (Bridged Adapter, Realtek PCIe 2.5GbE Family Controller)
Adapter 2:  Intel PRO/1000 MT Desktop (Internal Network, 'Net_200.100.0.0')
Adapter 3:  Intel PRO/1000 MT Desktop (Internal Network, 'Net_200.200.0.0')
```

USB

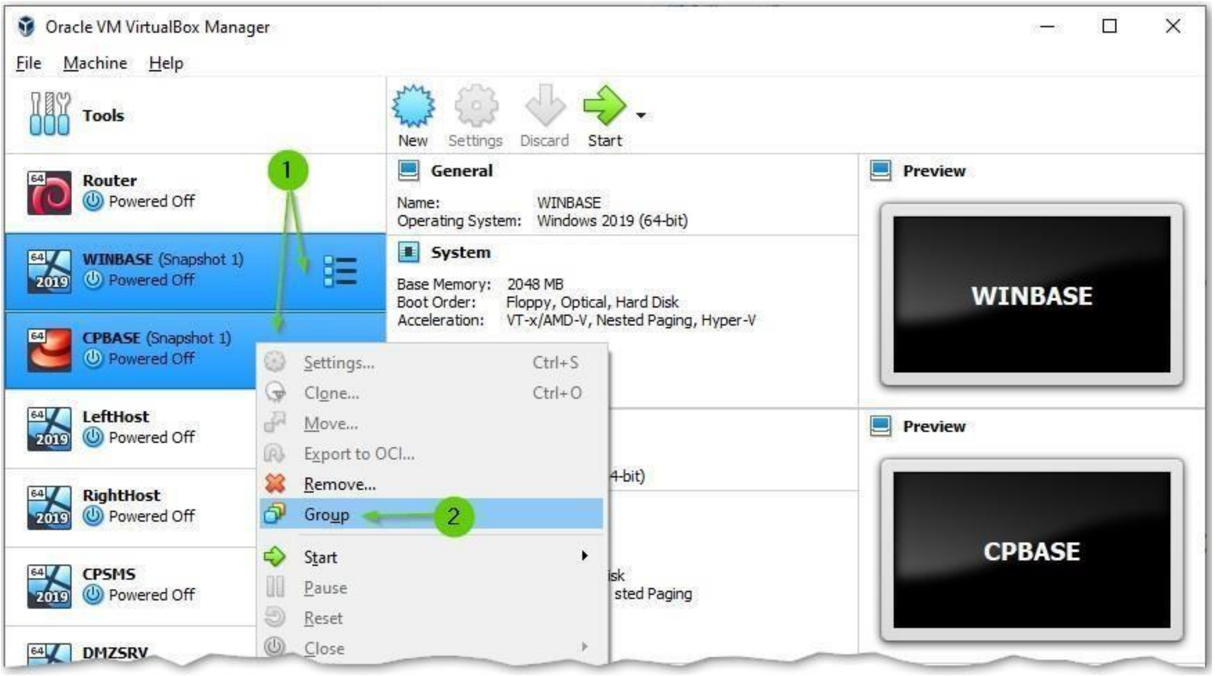
Disabled

Shared folders

None

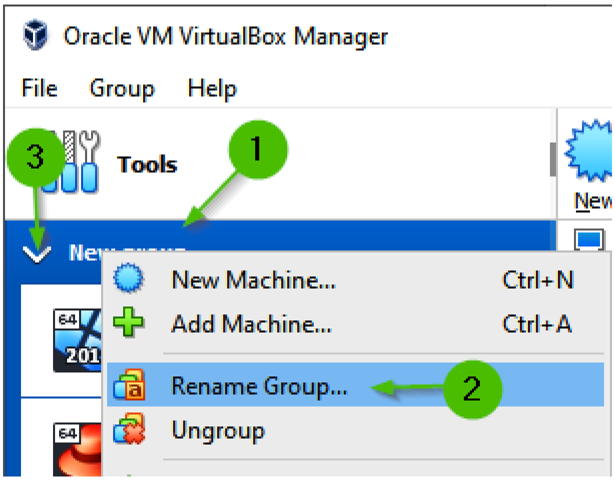
Description

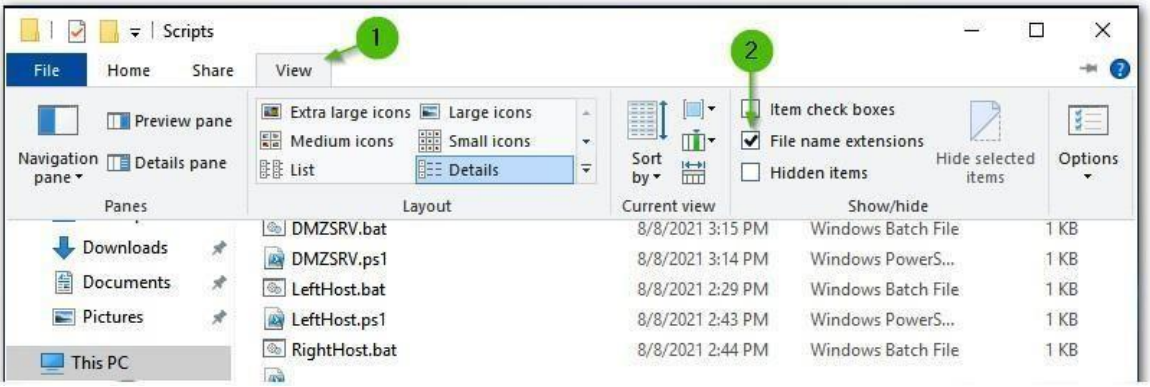
None



Name: WINBASE
Operating System: Windows 2019 (64-bit)

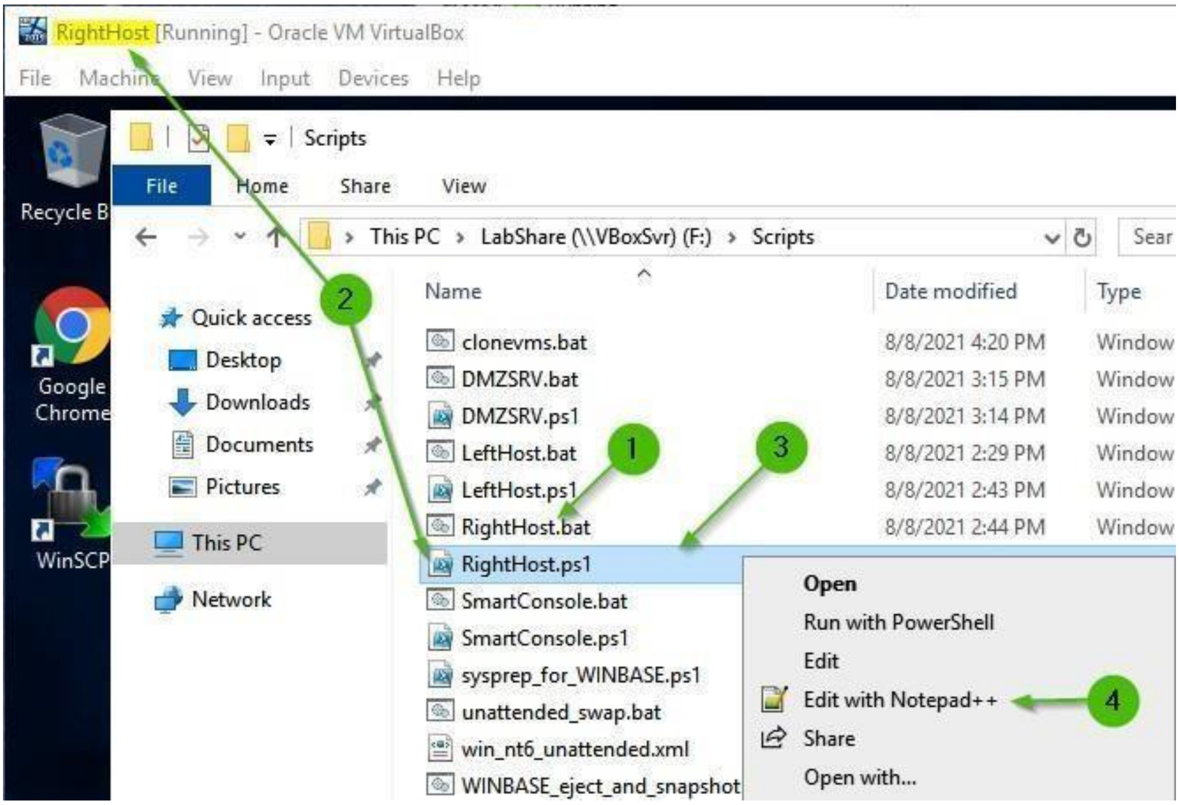
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V



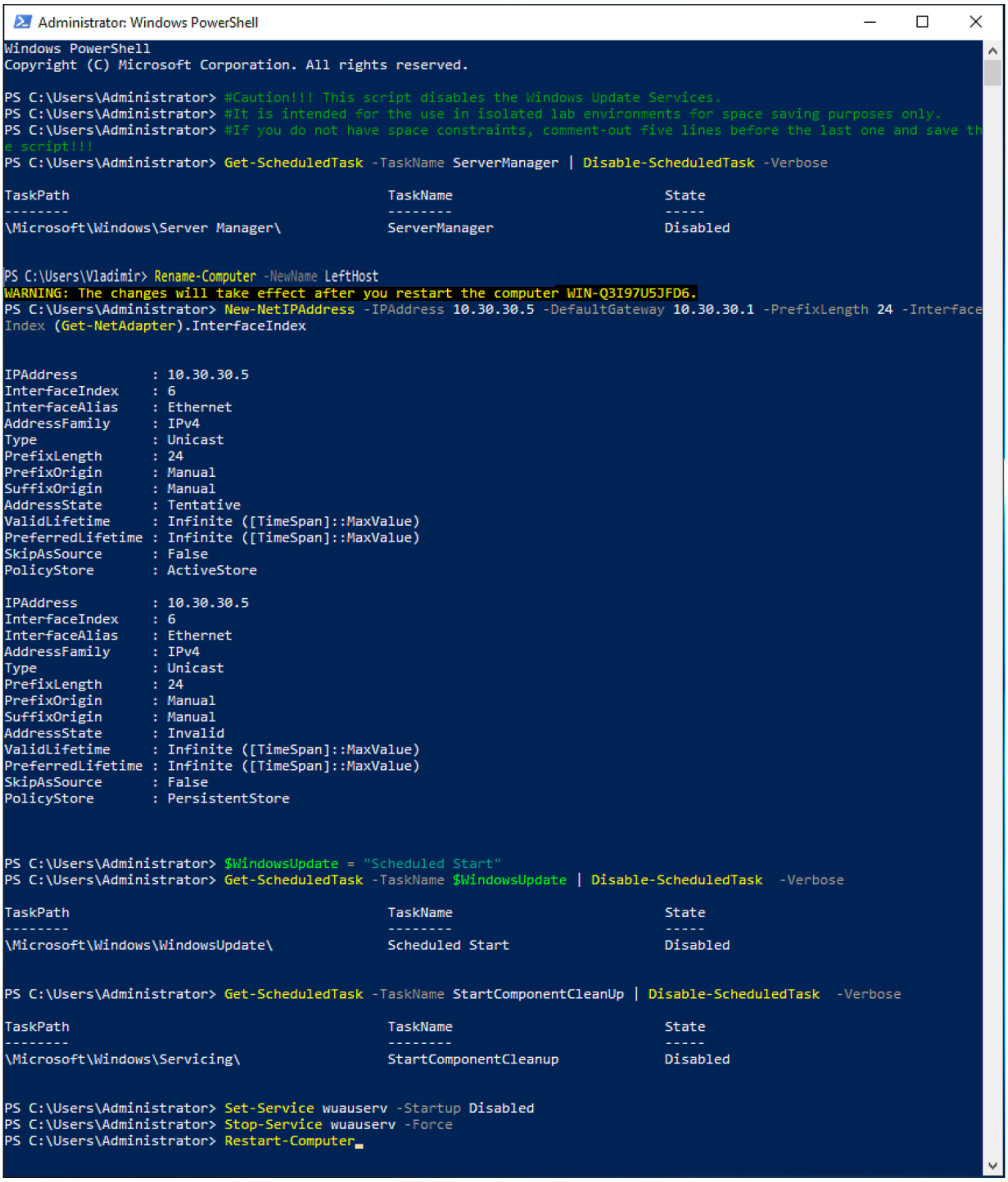


☐ Item check boxes
☑ File name extensions
☐ Hidden items

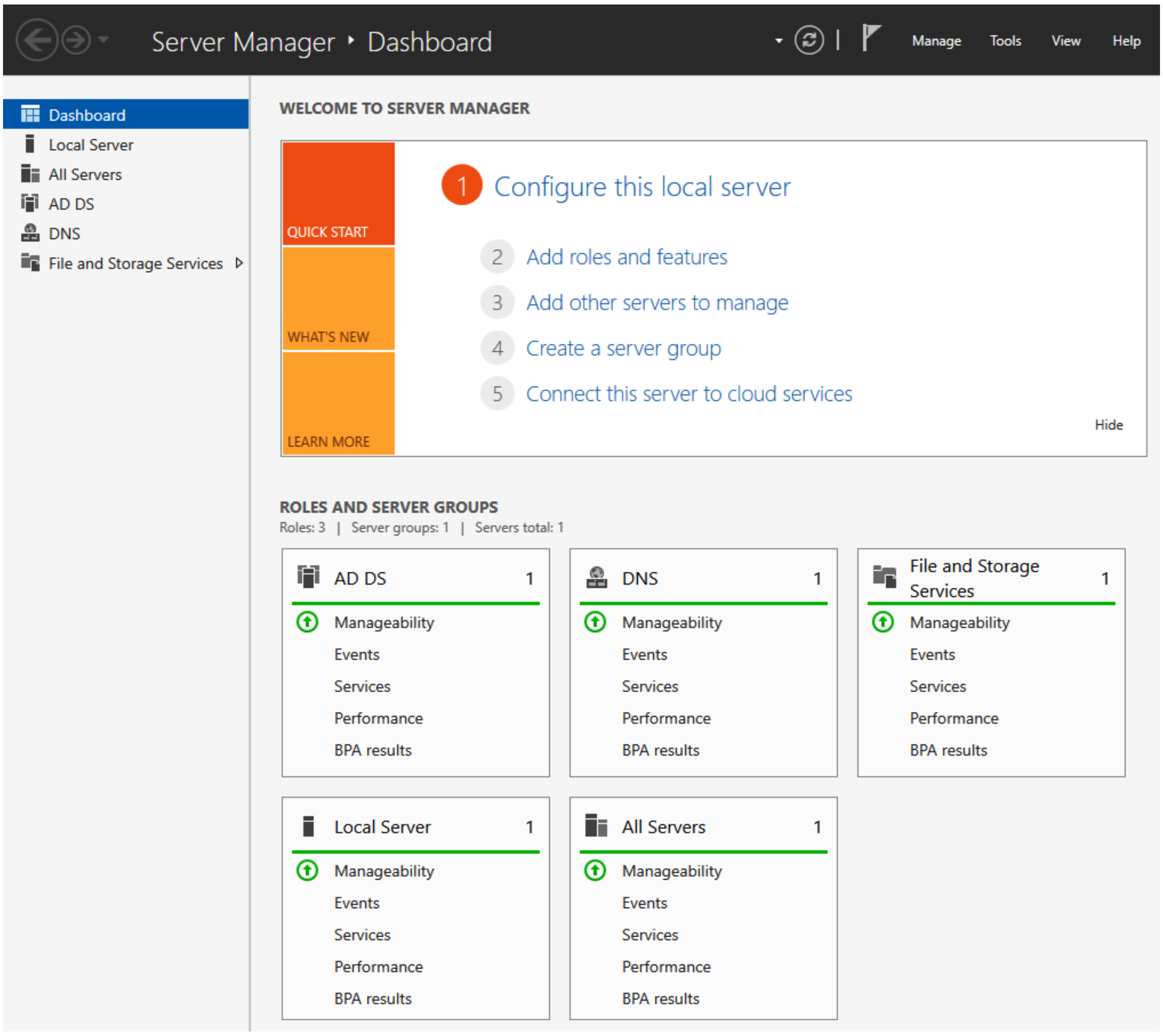
```
DMZSRV.bat      8/8/2021 3:15 PM   Windows Batch File   1 KB
DMZSRV.ps1      8/8/2021 3:14 PM   Windows PowerS...    1 KB
LeftHost.bat    8/8/2021 2:29 PM   Windows Batch File   1 KB
LeftHost.ps1    8/8/2021 2:43 PM   Windows PowerS...    1 KB
RightHost.bat   8/8/2021 2:44 PM   Windows Batch File   1 KB
```



Name	Date modified	Type
clonevms.bat	8/8/2021 4:20 PM	Window
DMZSRV.bat	8/8/2021 3:15 PM	Window
DMZSRV.ps1	8/8/2021 3:14 PM	Window
LeftHost.bat	8/8/2021 2:29 PM	Window
LeftHost.ps1	8/8/2021 2:43 PM	Window
RightHost.bat	8/8/2021 2:44 PM	Window
RightHost.ps1		
SmartConsole.bat		
SmartConsole.ps1		
sysprep_for_WINBASE.ps1		
unattended_swap.bat		
win_nt6_unattended.xml		
WINBASE_eject_and_snapshot		



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> #Caution!!! This script disables the Windows Update Services.
PS C:\Users\Administrator> #It is intended for the use in isolated lab environments for space saving purposes only.
PS C:\Users\Administrator> #If you do not have space constraints, comment-out five lines before the last one and save th
e script!!!
PS C:\Users\Administrator> Get-ScheduledTask -TaskName ServerManager | Disable-ScheduledTask -Verbose

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\Microsoft\Windows\Server Manager\             ServerManager                     Disabled


PS C:\Users\Vladimir> Rename-Computer -NewName LeftHost
WARNING: The changes will take effect after you restart the computer WIN-Q3I97U5JFD6.
PS C:\Users\Administrator> New-NetIPAddress -IPAddress 10.30.30.5 -DefaultGateway 10.30.30.1 -PrefixLength 24 -Interface
Index (Get-NetAdapter).InterfaceIndex


IPAddress         : 10.30.30.5
InterfaceIndex    : 6
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 10.30.30.5
InterfaceIndex    : 6
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore



PS C:\Users\Administrator> $WindowsUpdate = "Scheduled Start"
PS C:\Users\Administrator> Get-ScheduledTask -TaskName $WindowsUpdate | Disable-ScheduledTask  -Verbose

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\Microsoft\Windows\WindowsUpdate\              Scheduled Start                   Disabled


PS C:\Users\Administrator> Get-ScheduledTask -TaskName StartComponentCleanUp | Disable-ScheduledTask  -Verbose

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\Microsoft\Windows\Servicing\                  StartComponentCleanup             Disabled


PS C:\Users\Administrator> Set-Service wuauserv -Startup Disabled
PS C:\Users\Administrator> Stop-Service wuauserv -Force
PS C:\Users\Administrator> Restart-Computer_
```



WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

Hide

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

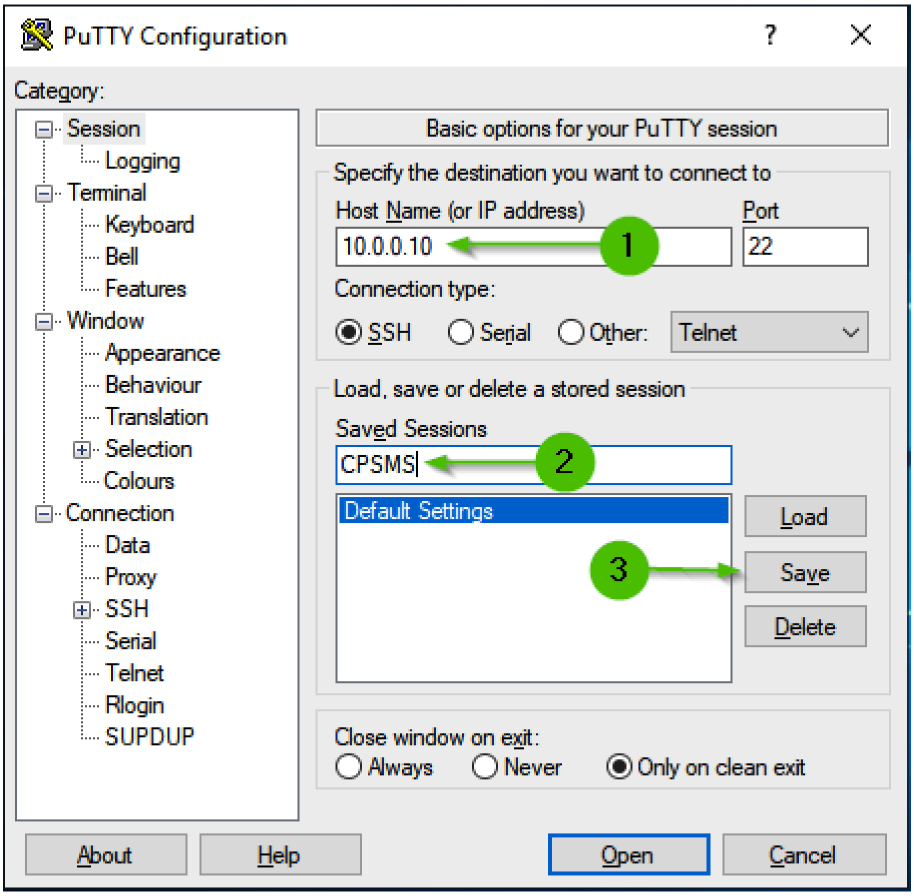
AD DS 1
- Manageability
- Events
- Services
- Performance
- BPA results

DNS 1
- Manageability
- Events
- Services
- Performance
- BPA results

File and Storage Services 1
- Manageability
- Events
- Services
- Performance
- BPA results

Local Server 1
- Manageability
- Events
- Services
- Performance
- BPA results

All Servers 1
- Manageability
- Events
- Services
- Performance
- BPA results



Specify the destination you want to connect to

Host Name (or IP address): 10.0.0.10 ← 1

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

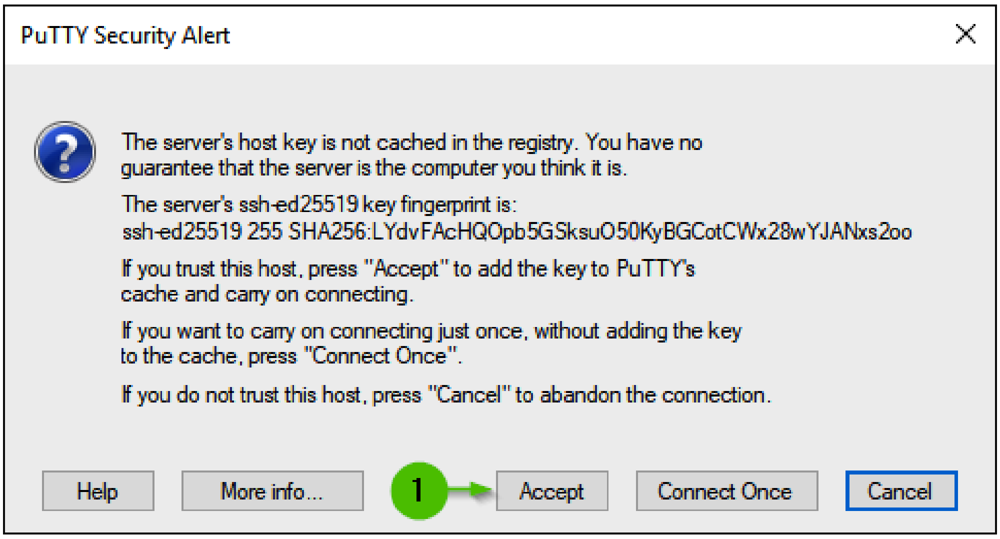
Load, save or delete a stored session

Saved Sessions: CPSMS ← 2

Default Settings

3 → Save

Close window on exit: ○ Always ○ Never ● Only on clean exit



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

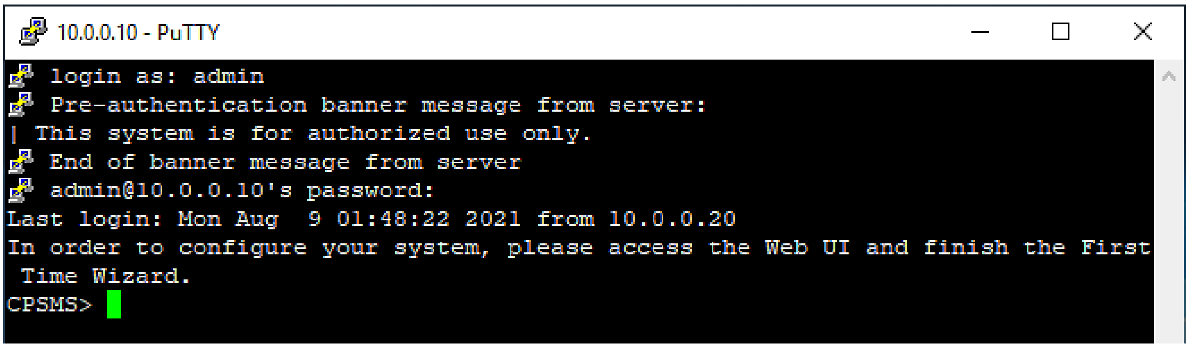
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:LYdvFAcHQOpb5GSksuO50KyBGCotCWx28wYJANxs2oo

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

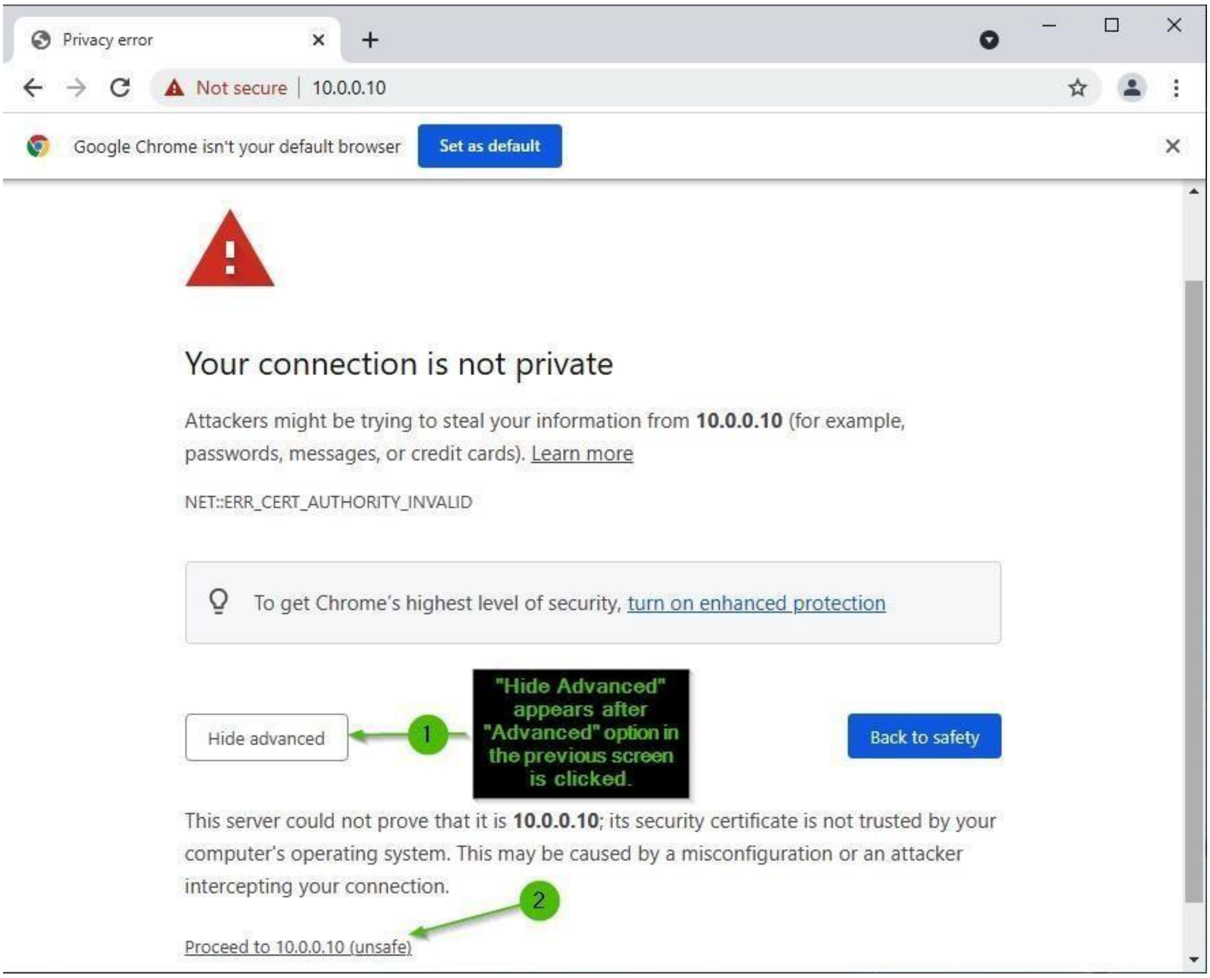
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

1 → Accept



```
login as: admin
Pre-authentication banner message from server:
| This system is for authorized use only.
End of banner message from server
admin@10.0.0.10's password:
Last login: Mon Aug  9 01:48:22 2021 from 10.0.0.20
In order to configure your system, please access the Web UI and finish the First
 Time Wizard.
CPSMS>
```


Privacy error
Not secure | 10.0.0.10
Google Chrome isn't your default browser
Set as default

Your connection is not private

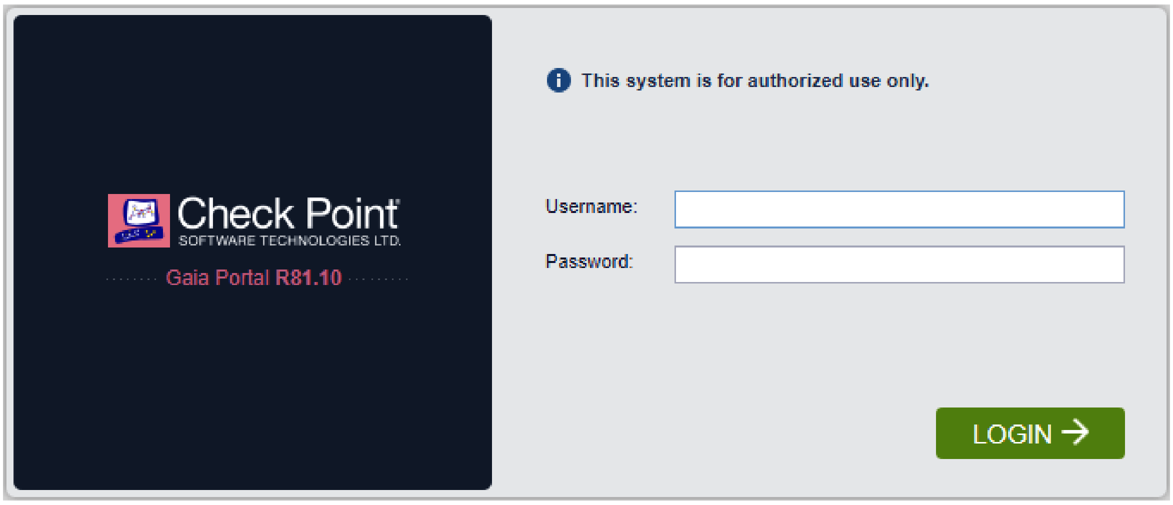
Attackers might be trying to steal your information from **10.0.0.10** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

Hide advanced
1
"Hide Advanced" appears after "Advanced" option in the previous screen is clicked.
Back to safety

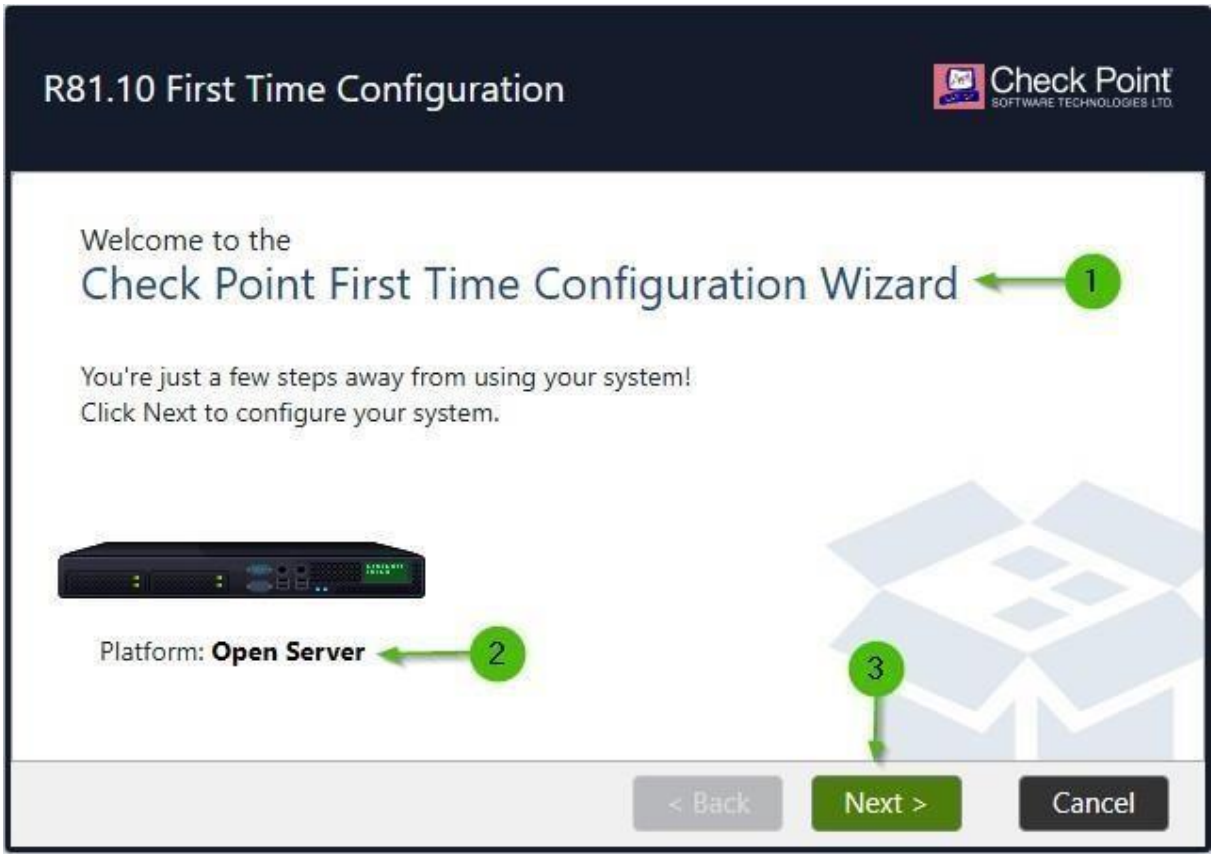
This server could not prove that it is **10.0.0.10**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.



This system is for authorized use only.

Username:

Password:



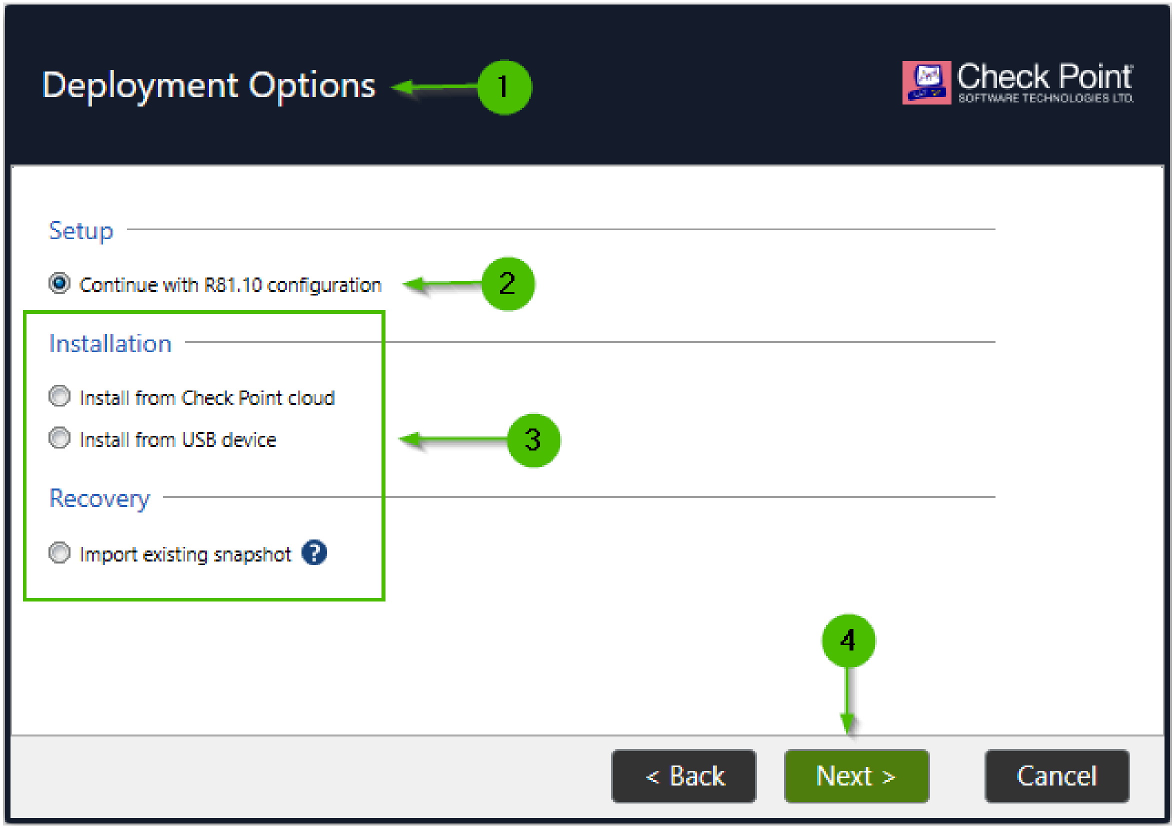
R81.10 First Time Configuration

Welcome to the

Check Point First Time Configuration Wizard

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

Platform: **Open Server**



Deployment Options

Setup

● Continue with R81.10 configuration

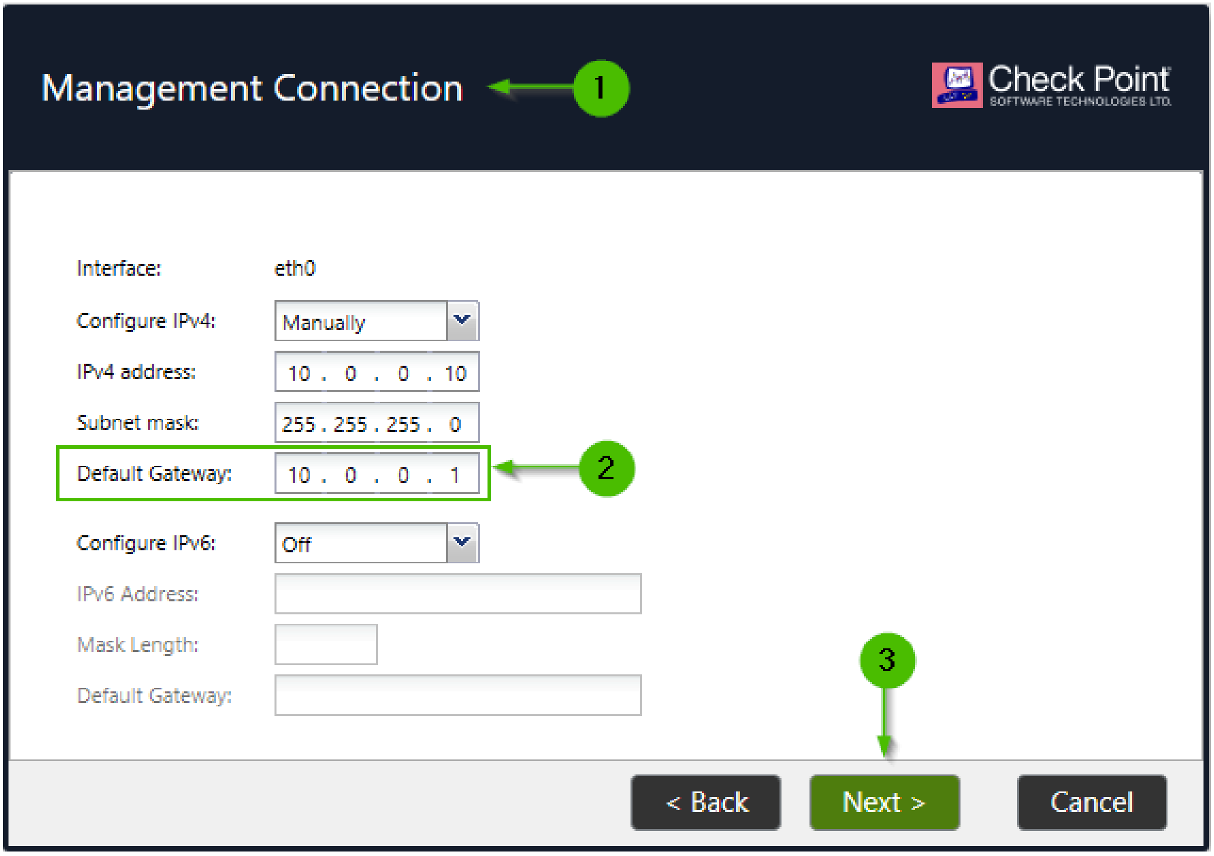
Installation

○ Install from Check Point cloud

○ Install from USB device

Recovery

○ Import existing snapshot ?



Management Connection

Interface: eth0

Configure IPv4: Manually

IPv4 address: 10 . 0 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

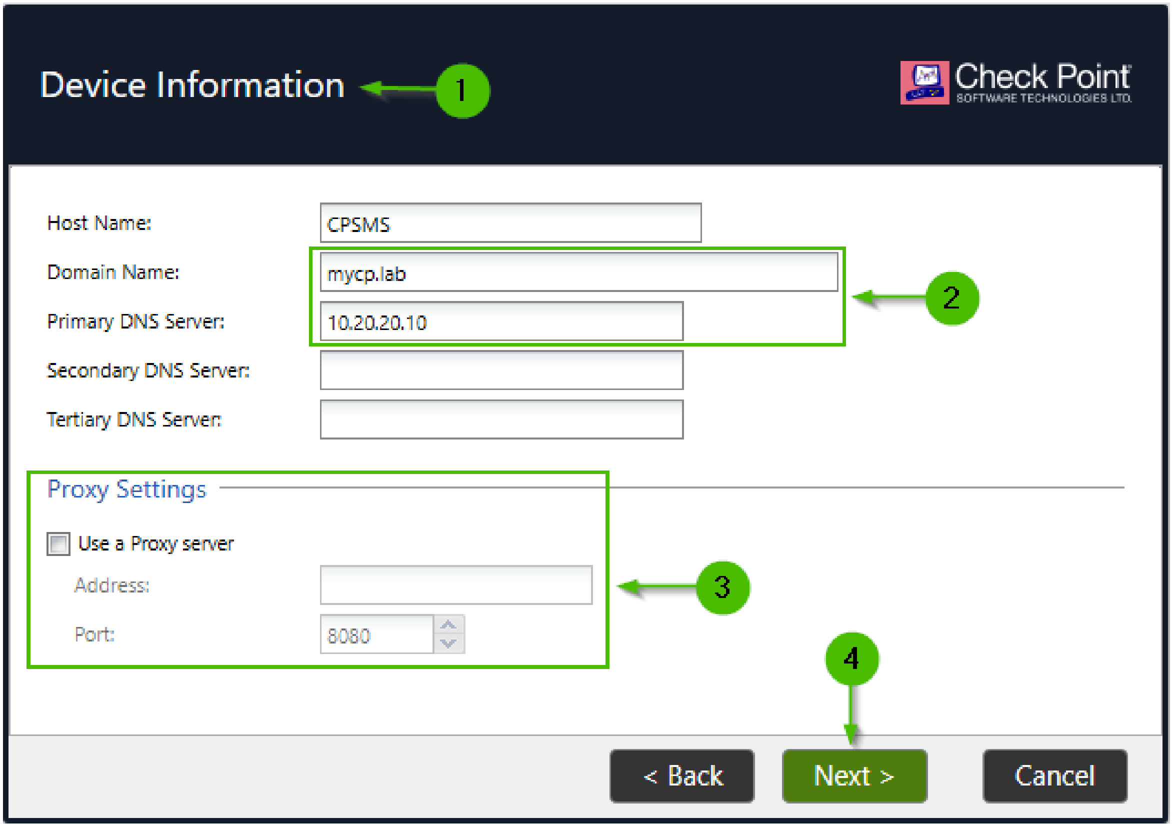
Default Gateway: 10 . 0 . 0 . 1

Configure IPv6: Off

IPv6 Address:

Mask Length:

Default Gateway:



Device Information

Host Name: CPSMS

Domain Name: mycp.lab

Primary DNS Server: 10.20.20.10

Secondary DNS Server:

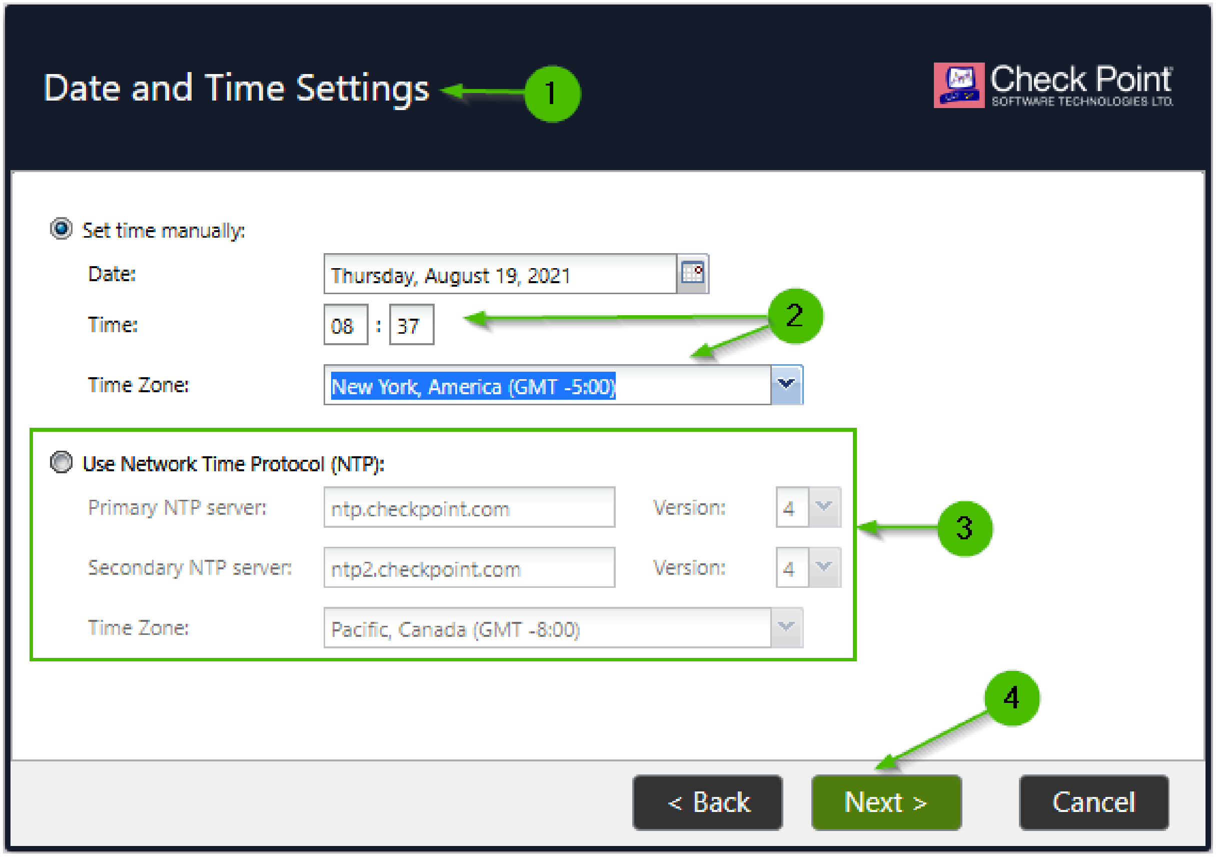
Tertiary DNS Server:

Proxy Settings

□ Use a Proxy server

Address:

Port: 8080



Date and Time Settings

● Set time manually:

Date: Thursday, August 19, 2021

Time: 08 : 37

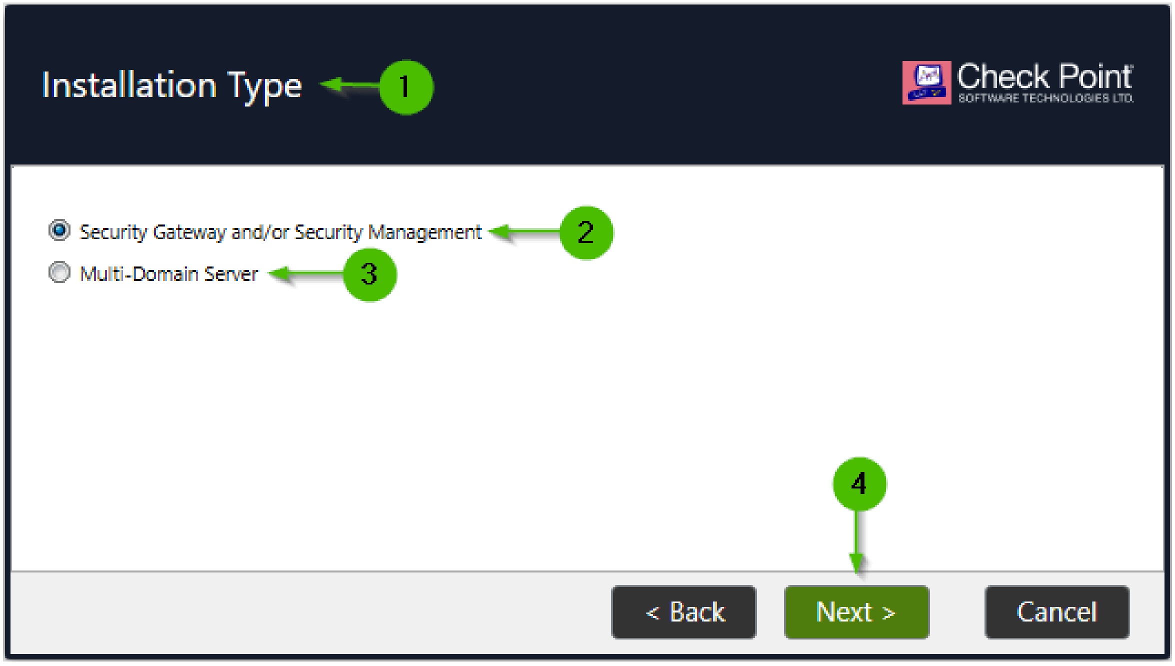
Time Zone: New York, America (GMT -5:00)

○ Use Network Time Protocol (NTP):

Primary NTP server: ntp.checkpoint.com Version: 4

Secondary NTP server: ntp2.checkpoint.com Version: 4

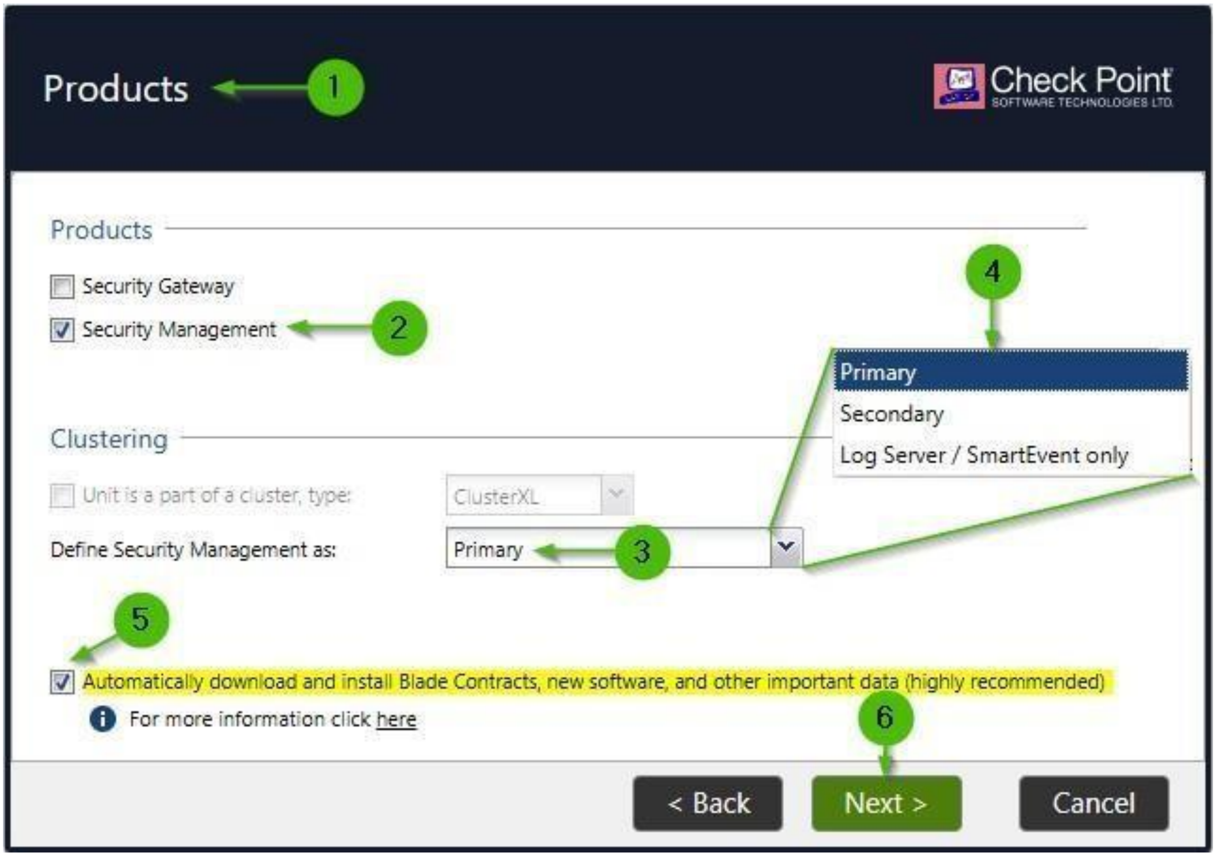
Time Zone: Pacific, Canada (GMT -8:00)



Installation Type

● Security Gateway and/or Security Management

○ Multi-Domain Server



Products

Products

☐ Security Gateway

☑ Security Management

Clustering

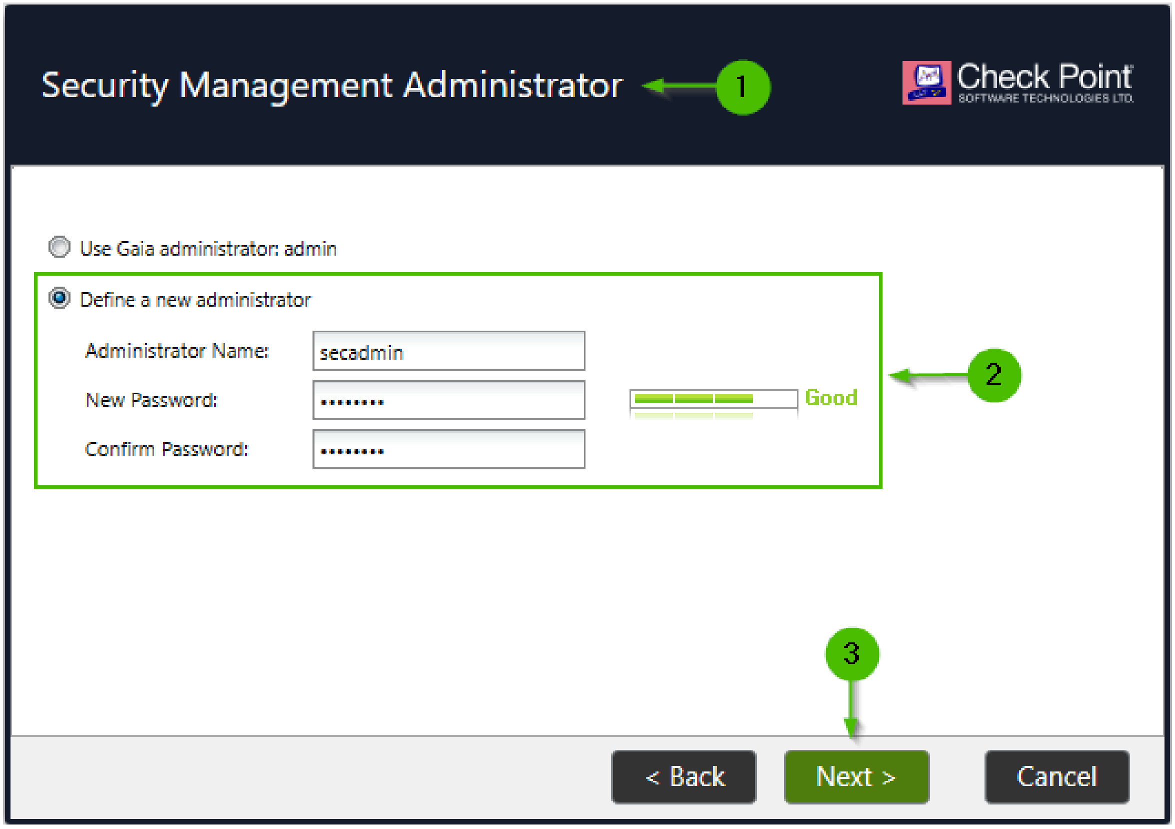
☐ Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

☑ Automatically download and install Blade Contracts, new software, and other important data (highly recommended)

For more information click here

1
2
3
4
5
6
Check Point SOFTWARE TECHNOLOGIES LTD.
Primary
Secondary
Log Server / SmartEvent only
< Back
Next >
Cancel



Security Management Administrator

○ Use Gaia administrator: admin

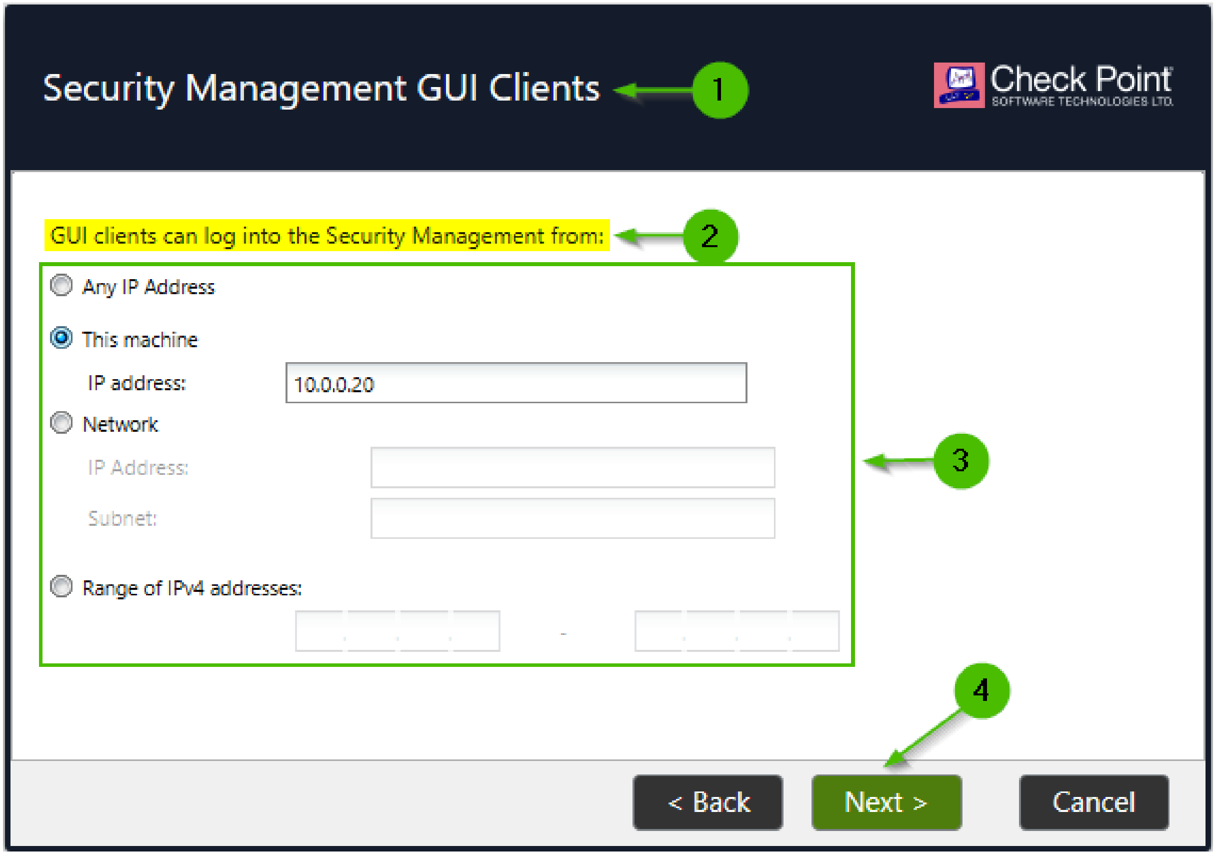
● Define a new administrator

Administrator Name: secadmin

New Password: ••••••••

Confirm Password: ••••••••

Good



Security Management GUI Clients

GUI clients can log into the Security Management from:

○ Any IP Address

● This machine

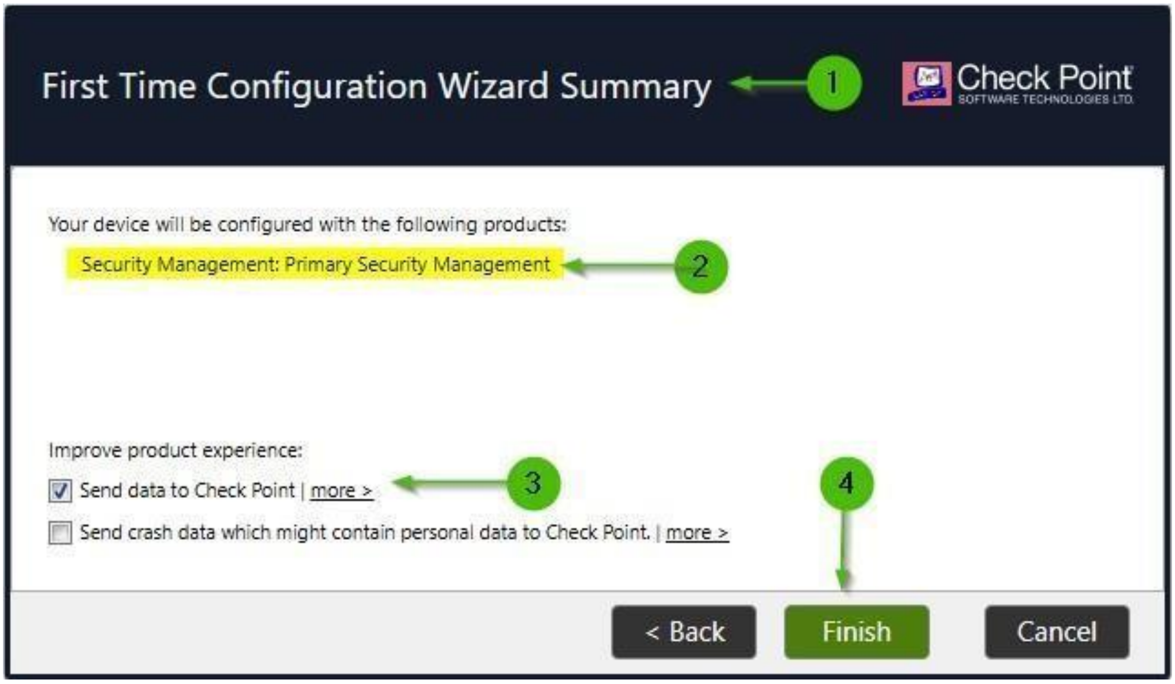
IP address: 10.0.0.20

○ Network

IP Address:

Subnet:

○ Range of IPv4 addresses:



First Time Configuration Wizard Summary

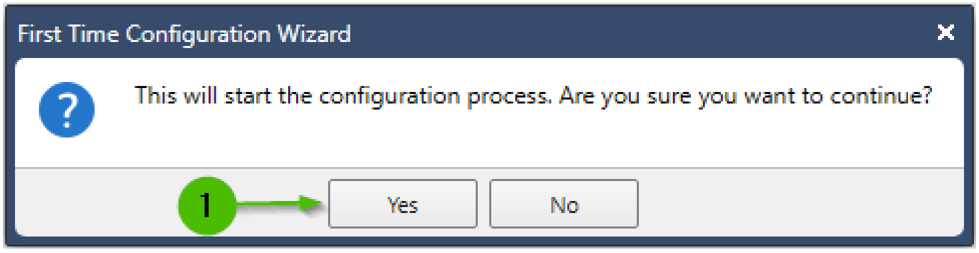
Your device will be configured with the following products:

Security Management: Primary Security Management

Improve product experience:

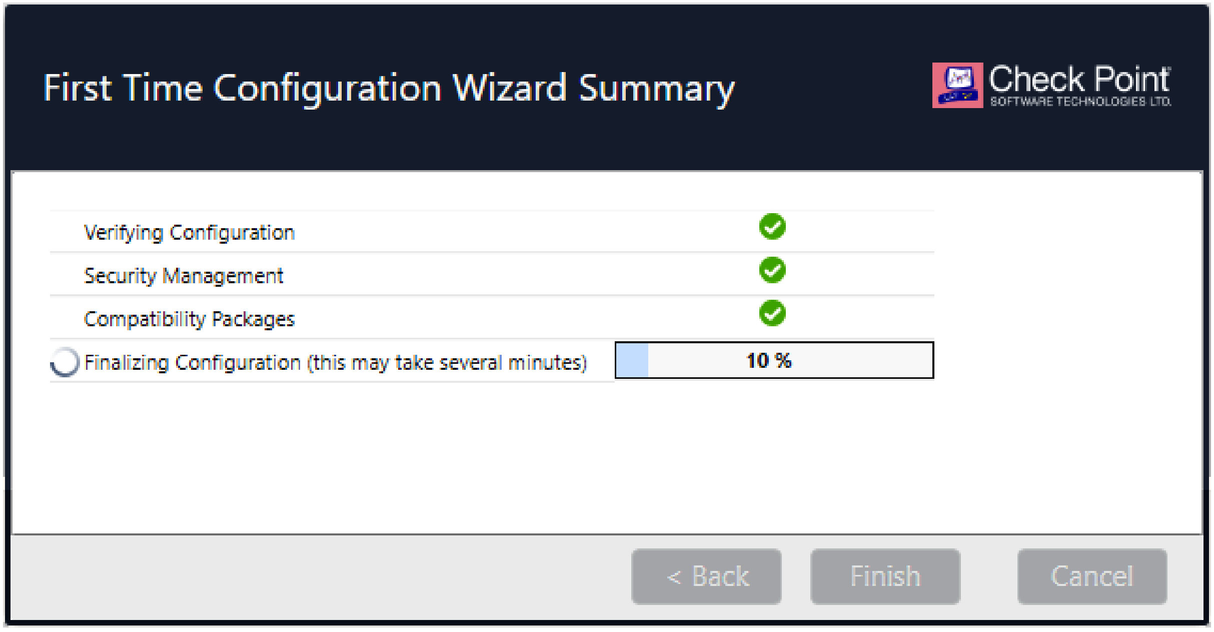
☑ Send data to Check Point | more >

□ Send crash data which might contain personal data to Check Point. | more >



First Time Configuration Wizard

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



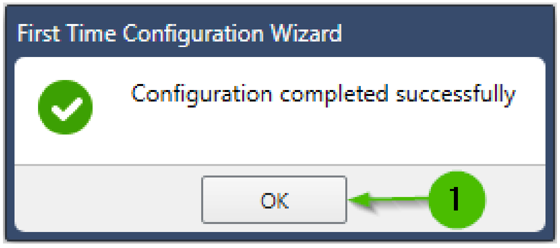
First Time Configuration Wizard Summary

Verifying Configuration ✓

Security Management ✓

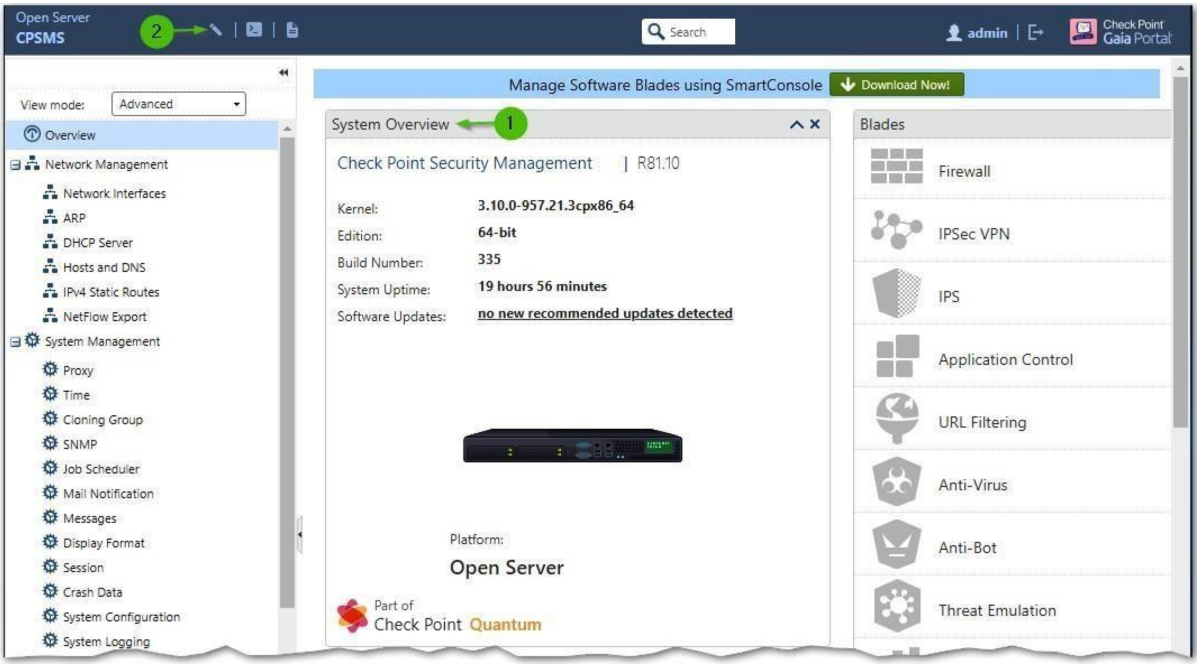
Compatibility Packages ✓

Finalizing Configuration (this may take several minutes) 10 %



First Time Configuration Wizard

Configuration completed successfully



Check Point Security Management | R81.10

Kernel: 3.10.0-957.21.3cpx86_64

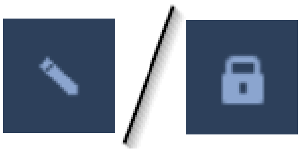
Edition: 64-bit

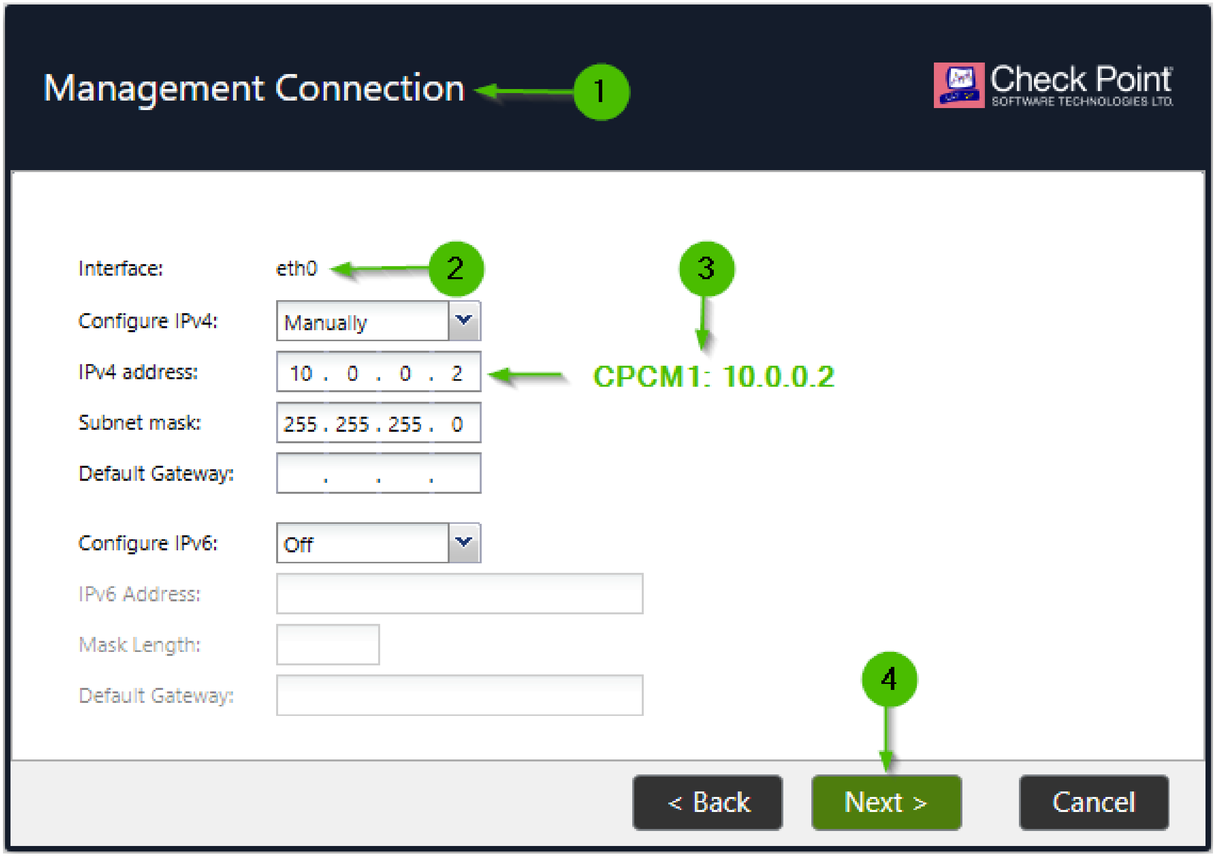
Build Number: 335

System Uptime: 19 hours 56 minutes

Software Updates: no new recommended updates detected

Platform:
Open Server





Management Connection

Interface: eth0

Configure IPv4: Manually

IPv4 address: 10 . 0 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

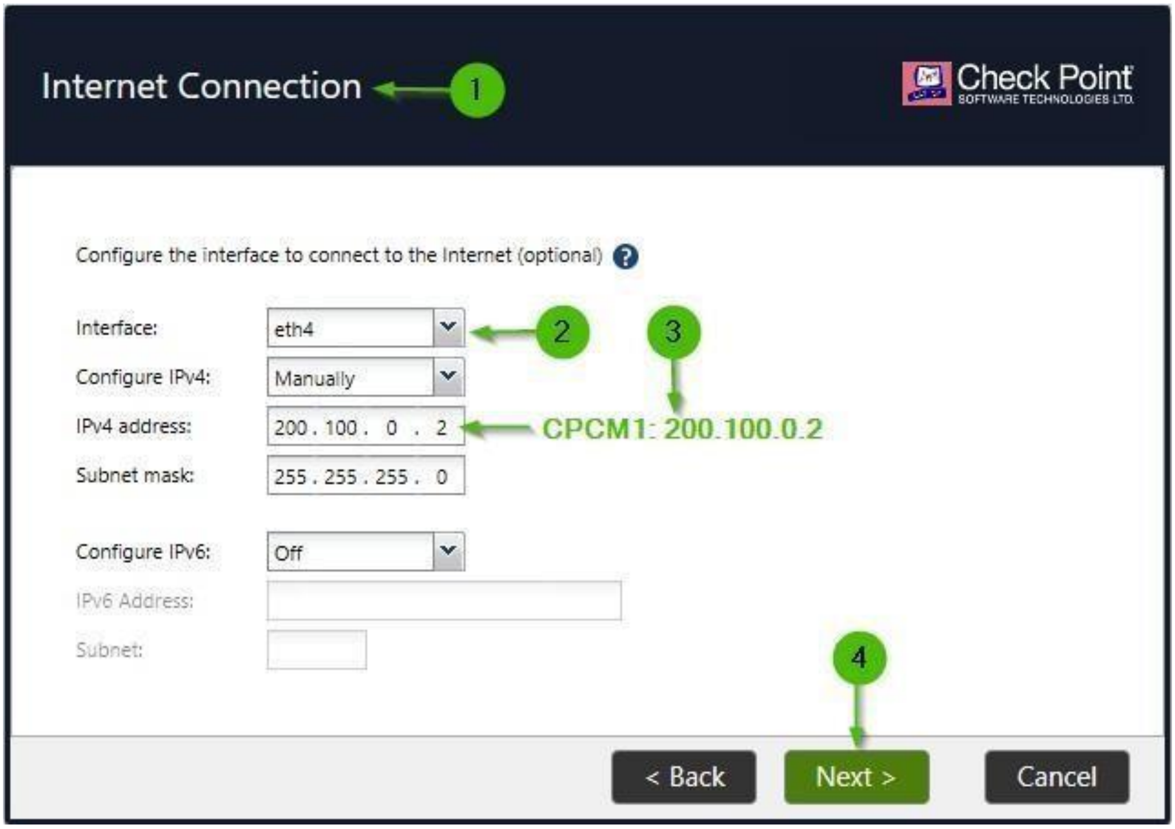
Default Gateway: . . .

Configure IPv6: Off

IPv6 Address:

Mask Length:

Default Gateway:



Internet Connection

Configure the interface to connect to the Internet (optional)

Interface: eth4

Configure IPv4: Manually

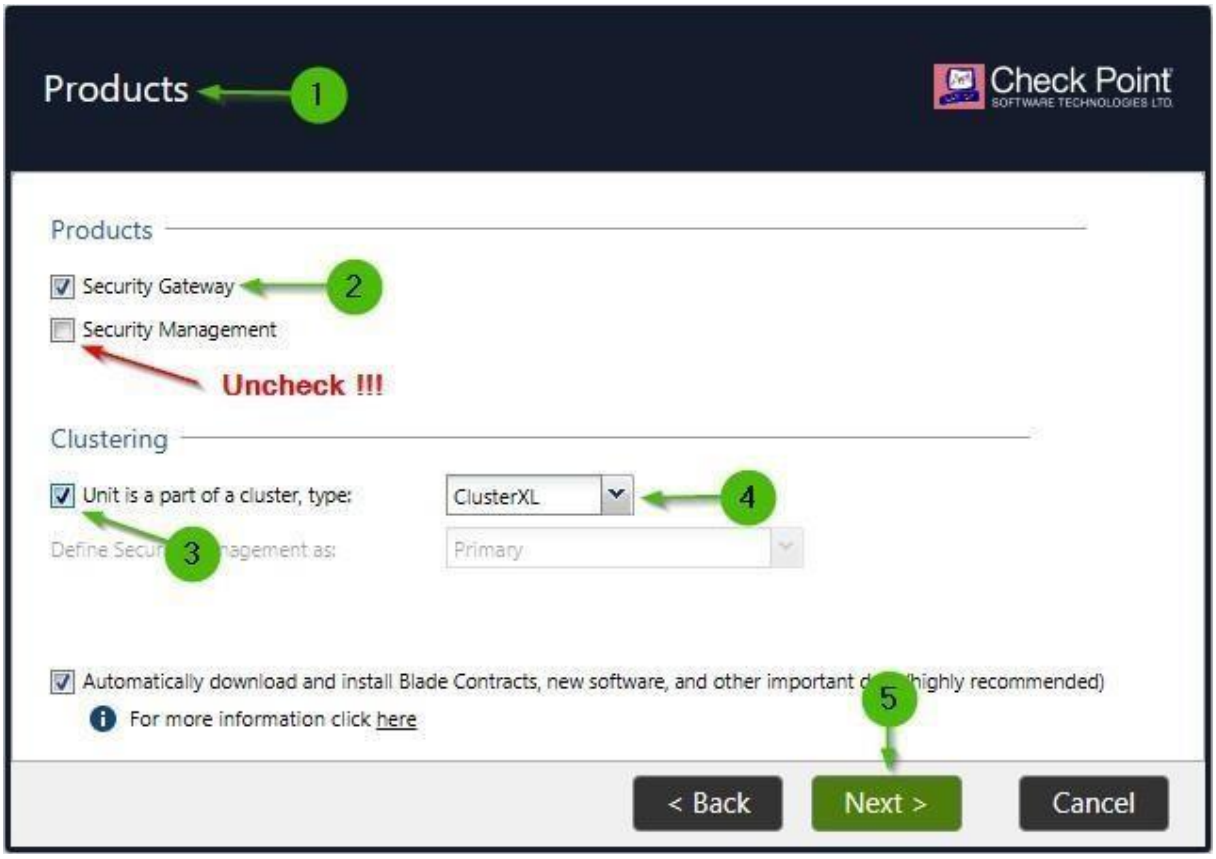
IPv4 address: 200 . 100 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Configure IPv6: Off

IPv6 Address:

Subnet:



Products

Products

☑ Security Gateway

□ Security Management

Uncheck !!!

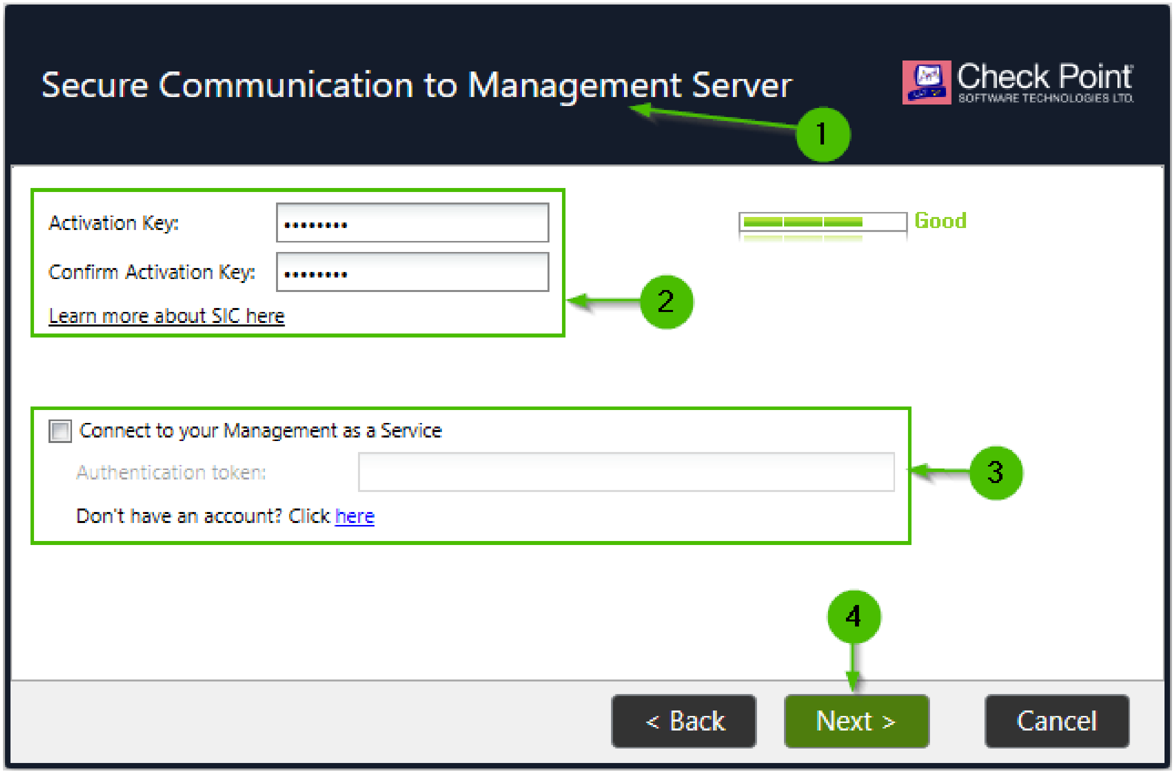
Clustering

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

Define Secur agement as: Primary

☑ Automatically download and install Blade Contracts, new software, and other important d highly recommended)

For more information click here



Secure Communication to Management Server

Activation Key: ••••••••

Confirm Activation Key: ••••••••

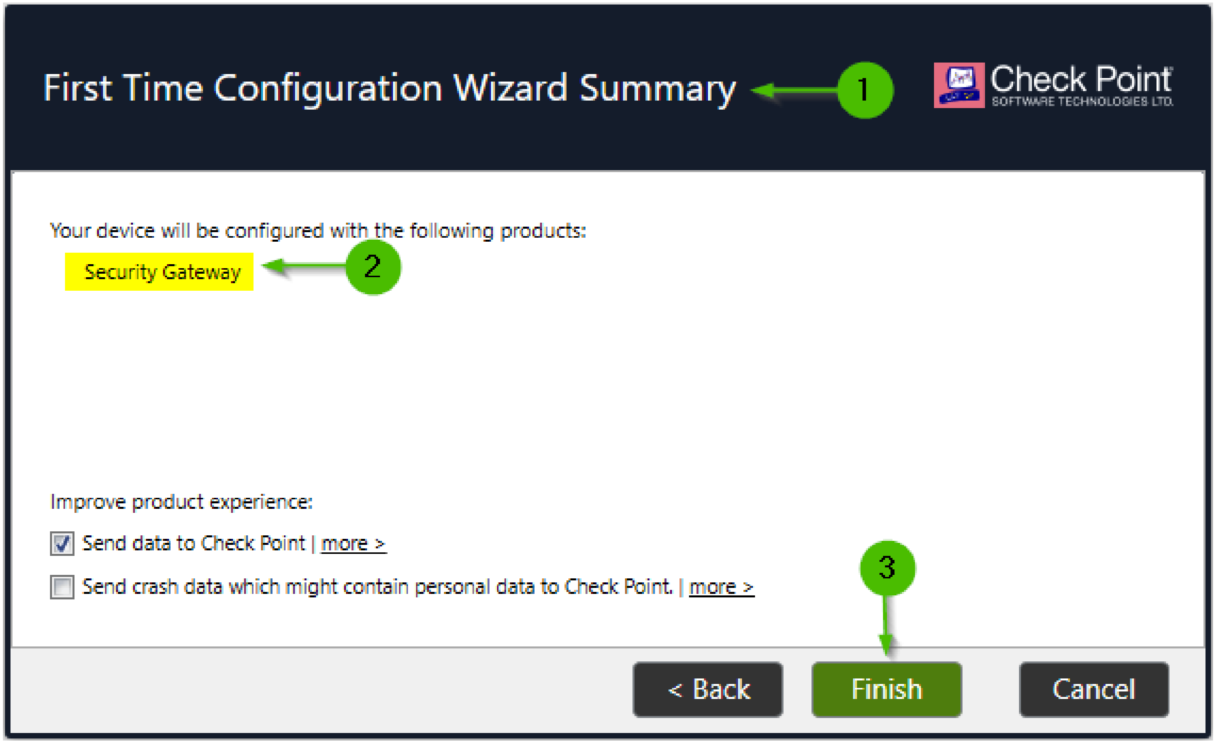
Good

Learn more about SIC here

□ Connect to your Management as a Service

Authentication token:

Don't have an account? Click here



First Time Configuration Wizard Summary

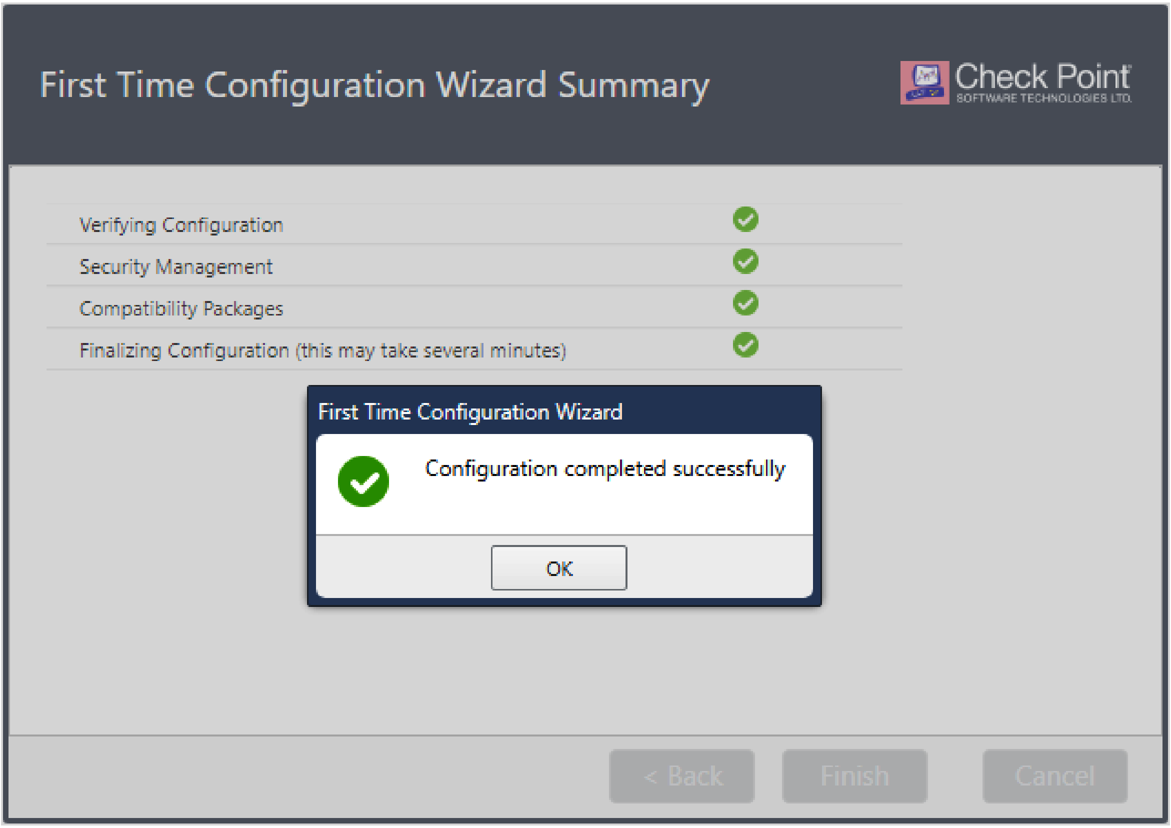
Your device will be configured with the following products:

Security Gateway

Improve product experience:

☑ Send data to Check Point | more >

□ Send crash data which might contain personal data to Check Point. | more >

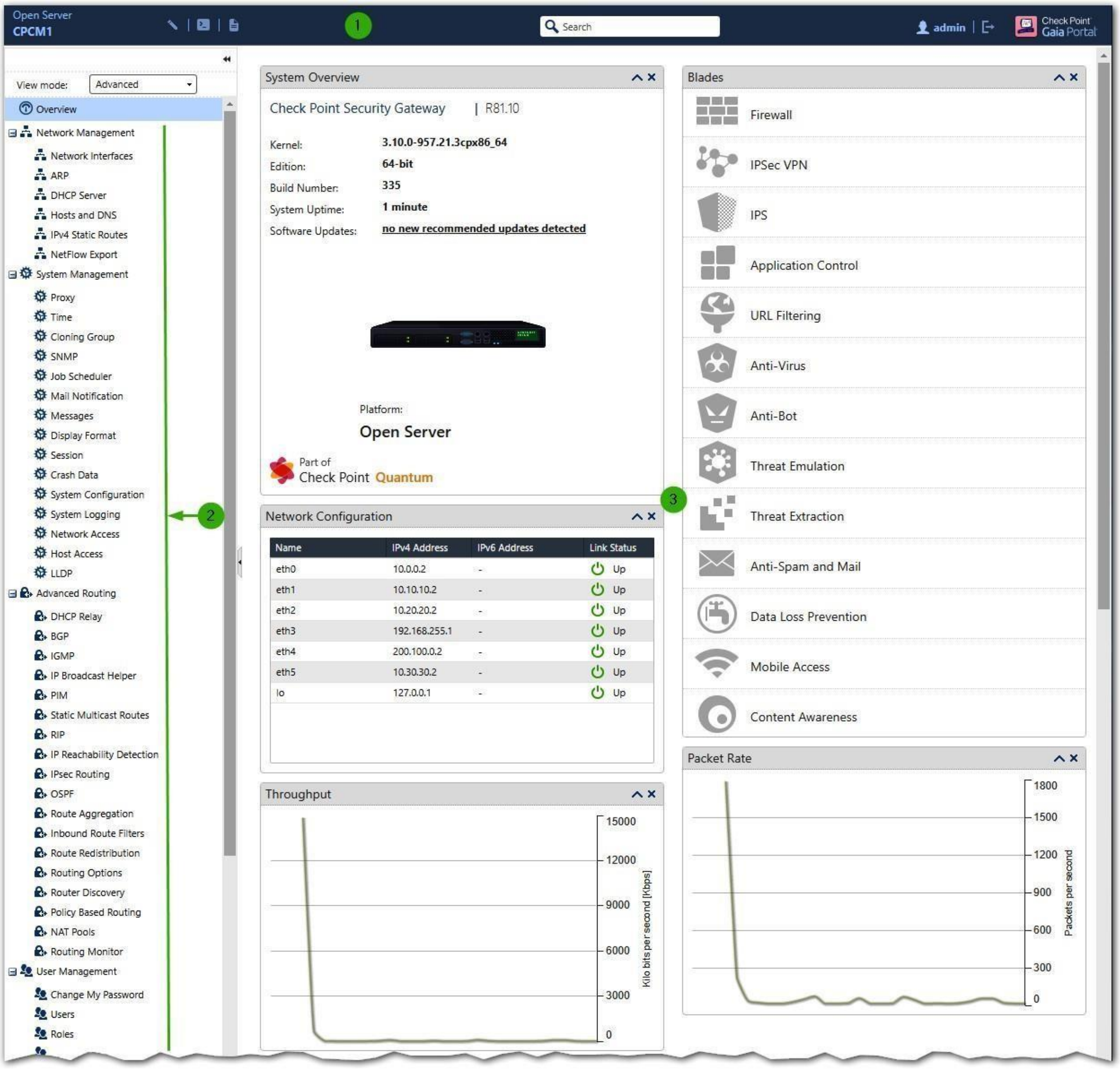


First Time Configuration Wizard Summary

Verifying Configuration	✓
Security Management	✓
Compatibility Packages	✓
Finalizing Configuration (this may take several minutes)	✓

First Time Configuration Wizard

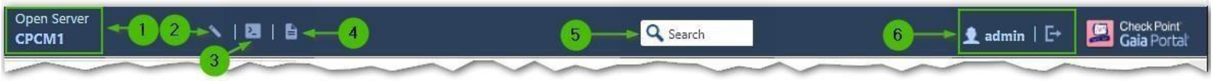
✓ Configuration completed successfully

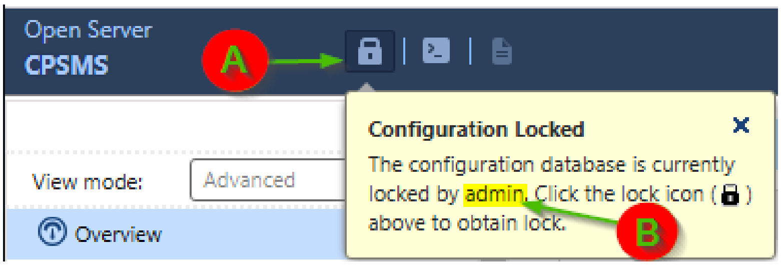


Check Point Security Gateway | R81.10

Kernel: 3.10.0-957.21.3cpx86_64
Edition: 64-bit
Build Number: 335
System Uptime: 1 minute
Software Updates: no new recommended updates detected

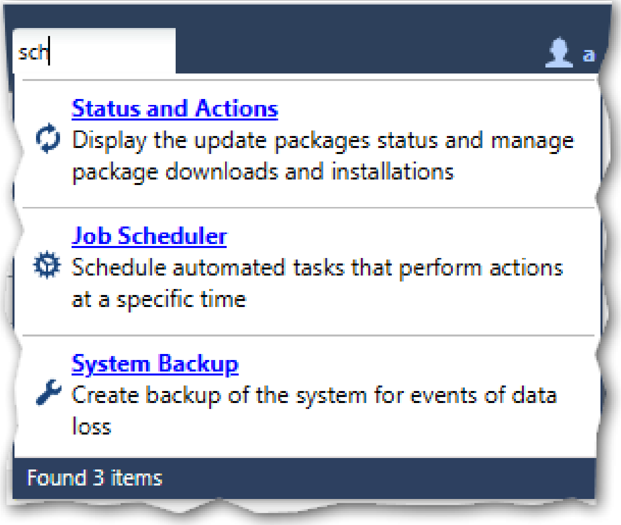
Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.0.0.2	-	Up
eth1	10.10.10.2	-	Up
eth2	10.20.20.2	-	Up
eth3	192.168.255.1	-	Up
eth4	200.100.0.2	-	Up
eth5	10.30.30.2	-	Up
lo	127.0.0.1	-	Up





Configuration Locked

The configuration database is currently locked by admin. Click the lock icon (🔒) above to obtain lock.

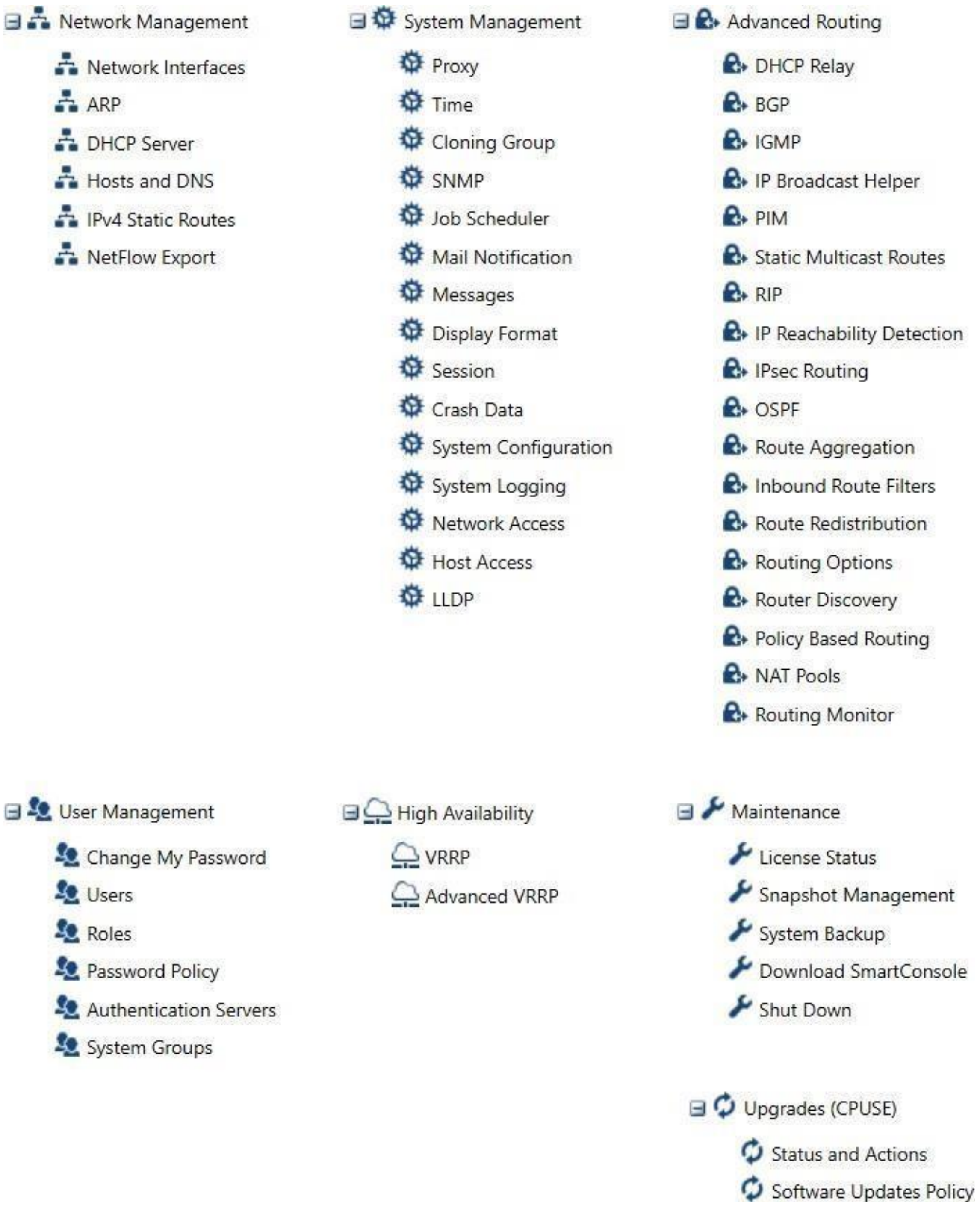


Status and Actions
Display the update packages status and manage package downloads and installations

Job Scheduler
Schedule automated tasks that perform actions at a specific time

System Backup
Create backup of the system for events of data loss

Found 3 items



- Network Management
  - Network Interfaces
  - ARP
  - DHCP Server
  - Hosts and DNS
  - IPv4 Static Routes
  - NetFlow Export

- System Management
  - Proxy
  - Time
  - Cloning Group
  - SNMP
  - Job Scheduler
  - Mail Notification
  - Messages
  - Display Format
  - Session
  - Crash Data
  - System Configuration
  - System Logging
  - Network Access
  - Host Access
  - LLDP

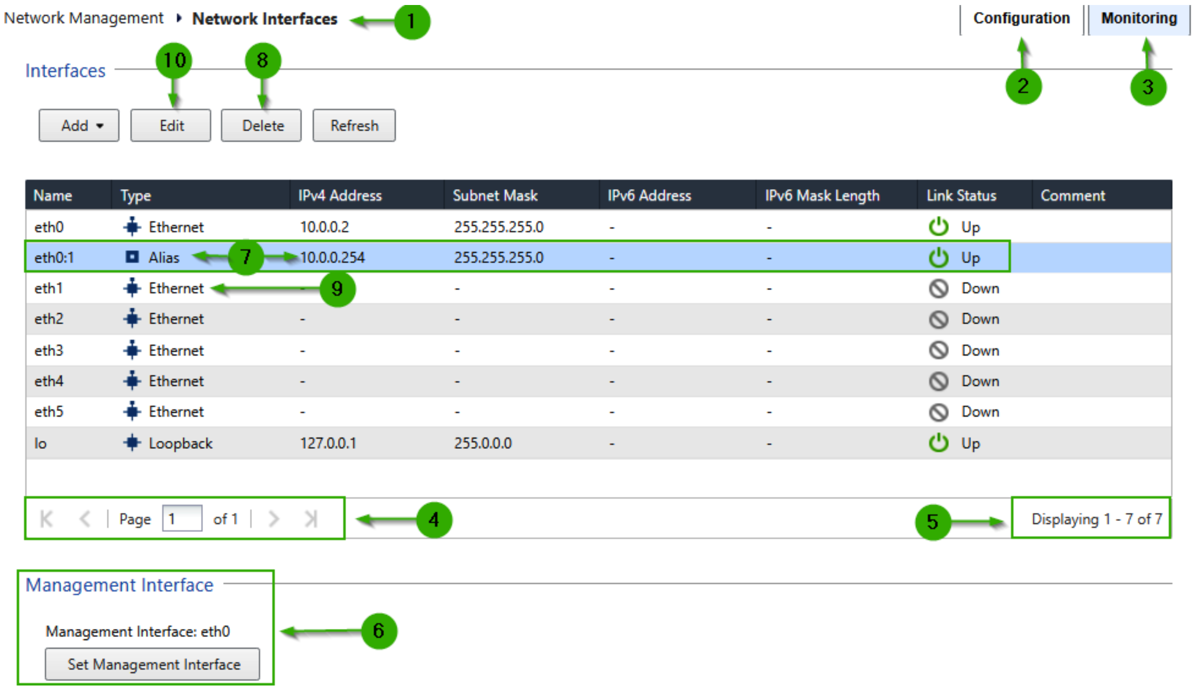
- Advanced Routing
  - DHCP Relay
  - BGP
  - IGMP
  - IP Broadcast Helper
  - PIM
  - Static Multicast Routes
  - RIP
  - IP Reachability Detection
  - IPsec Routing
  - OSPF
  - Route Aggregation
  - Inbound Route Filters
  - Route Redistribution
  - Routing Options
  - Router Discovery
  - Policy Based Routing
  - NAT Pools
  - Routing Monitor

- User Management
  - Change My Password
  - Users
  - Roles
  - Password Policy
  - Authentication Servers
  - System Groups

- High Availability
  - VRRP
  - Advanced VRRP

- Maintenance
  - License Status
  - Snapshot Management
  - System Backup
  - Download SmartConsole
  - Shut Down

- Upgrades (CPUSE)
  - Status and Actions
  - Software Updates Policy



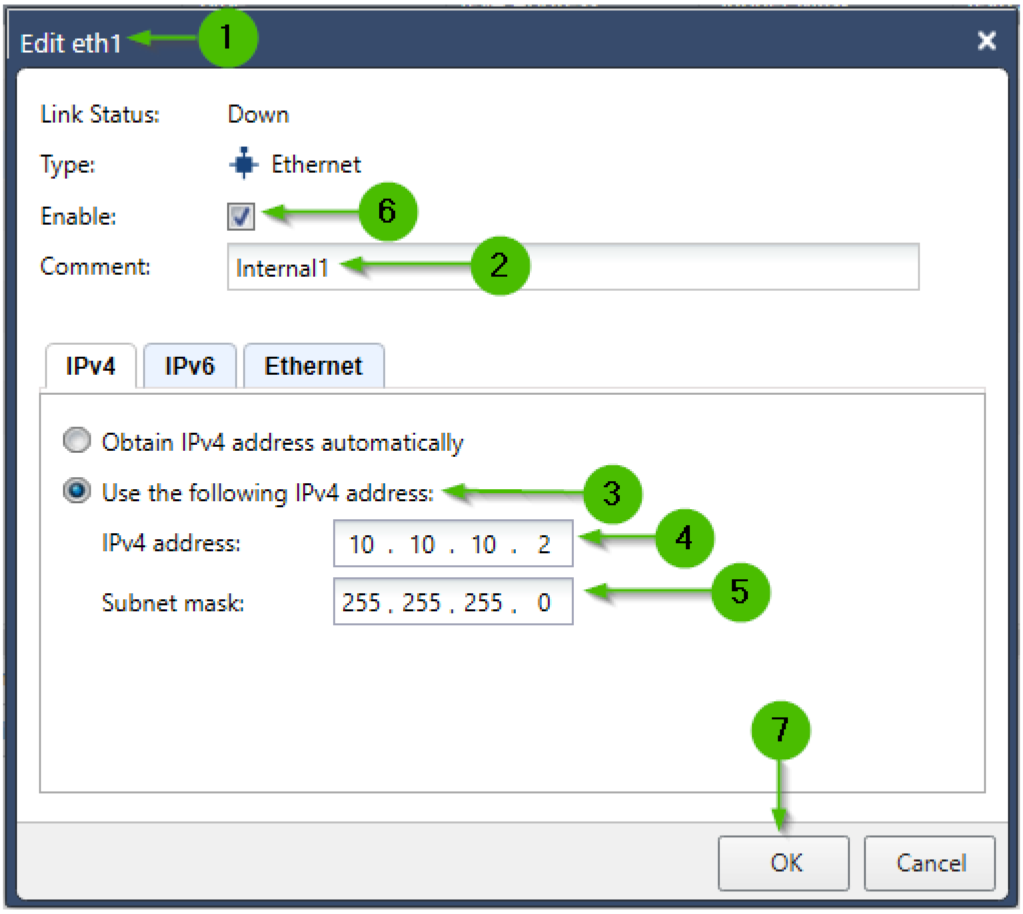
Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	10.0.0.2	255.255.255.0	-	-	Up	
eth0:1	Alias	10.0.0.254	255.255.255.0	-	-	Up	
eth1	Ethernet	-	-	-	-	Down	
eth2	Ethernet	-	-	-	-	Down	
eth3	Ethernet	-	-	-	-	Down	
eth4	Ethernet	-	-	-	-	Down	
eth5	Ethernet	-	-	-	-	Down	
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

Page 1 of 1

Displaying 1 - 7 of 7

Management Interface

Management Interface: eth0



Link Status: Down

Type: Ethernet

Enable: ☑

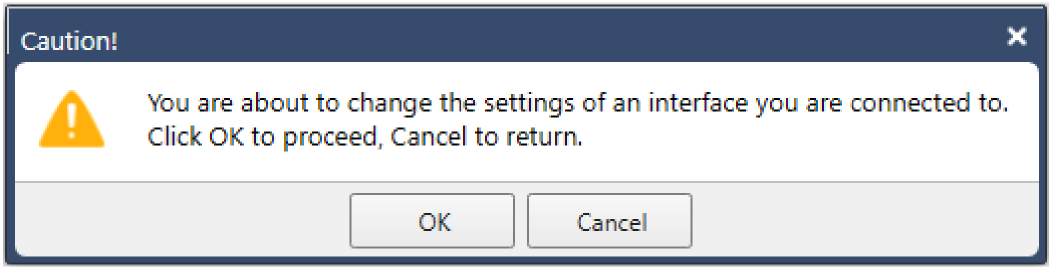
Comment: Internal1

○ Obtain IPv4 address automatically

● Use the following IPv4 address:

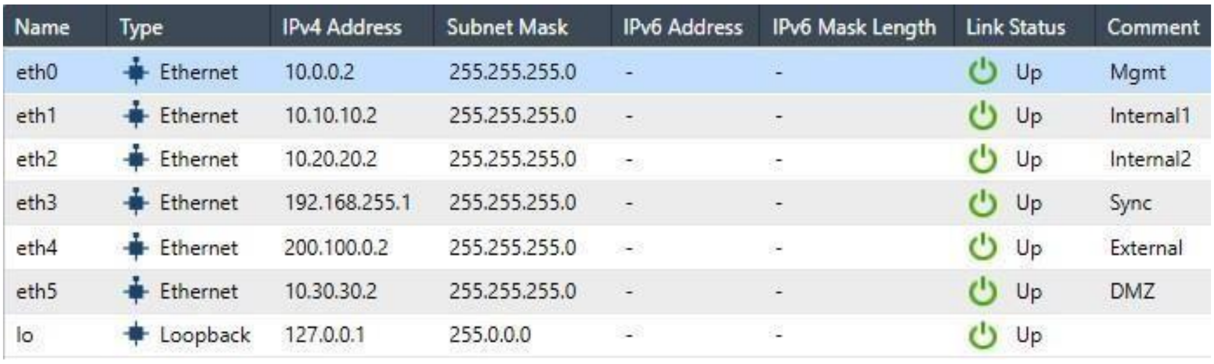
IPv4 address: 10 . 10 . 10 . 2

Subnet mask: 255 . 255 . 255 . 0

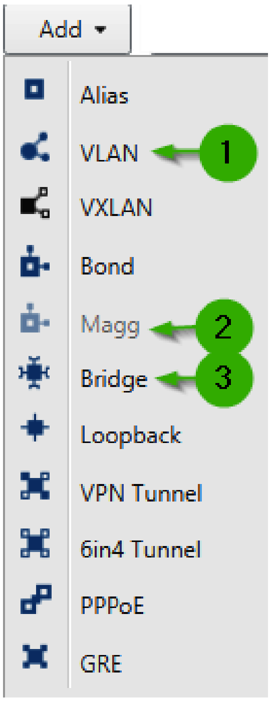


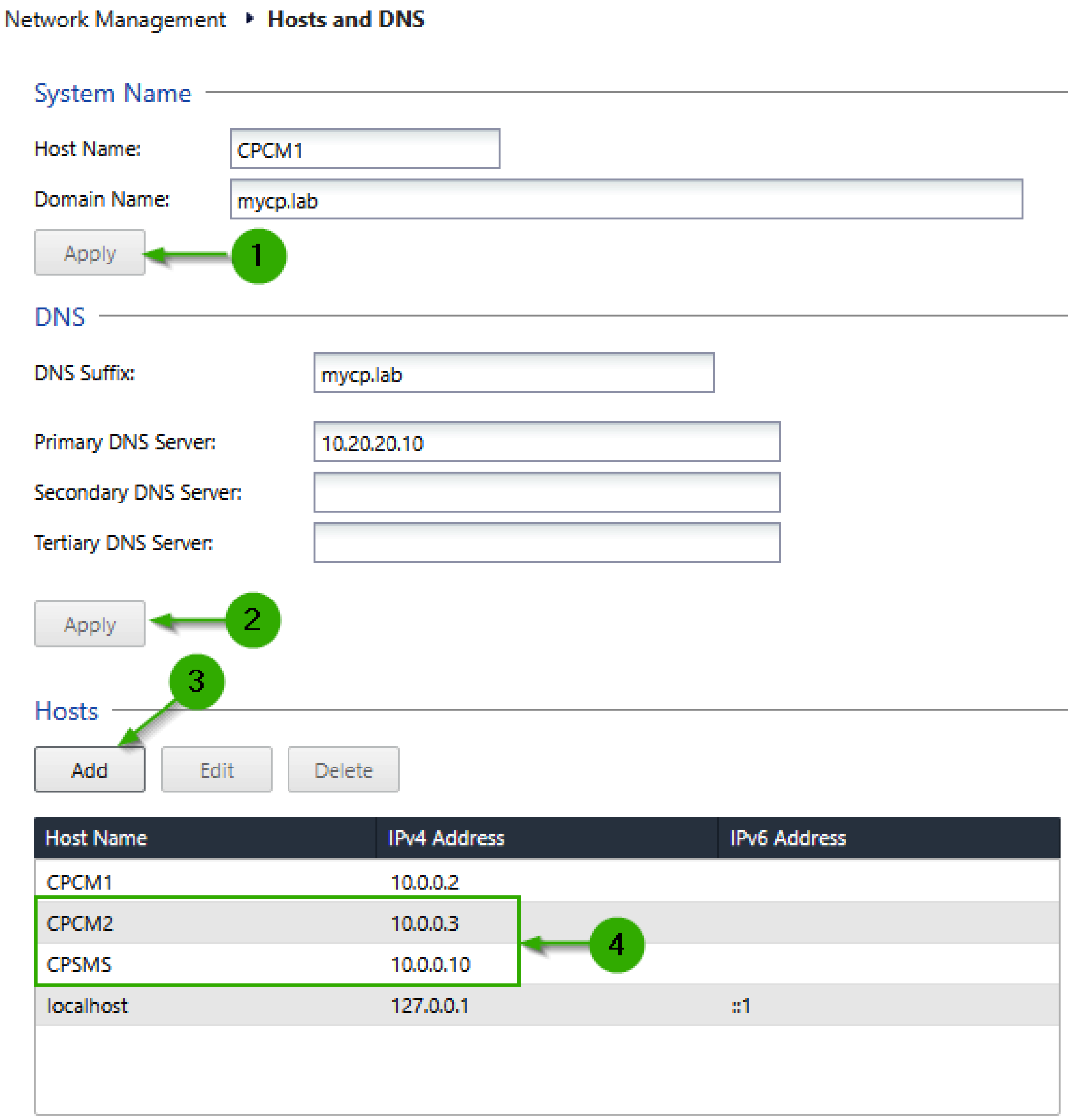
Caution!

You are about to change the settings of an interface you are connected to. Click OK to proceed, Cancel to return.



Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	10.0.0.2	255.255.255.0	-	-	Up	Mgmt
eth1	Ethernet	10.10.10.2	255.255.255.0	-	-	Up	Internal1
eth2	Ethernet	10.20.20.2	255.255.255.0	-	-	Up	Internal2
eth3	Ethernet	192.168.255.1	255.255.255.0	-	-	Up	Sync
eth4	Ethernet	200.100.0.2	255.255.255.0	-	-	Up	External
eth5	Ethernet	10.30.30.2	255.255.255.0	-	-	Up	DMZ
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	





Network Management ▸ **Hosts and DNS**

System Name

Host Name: CPCM1

Domain Name: mycp.lab

DNS

DNS Suffix: mycp.lab

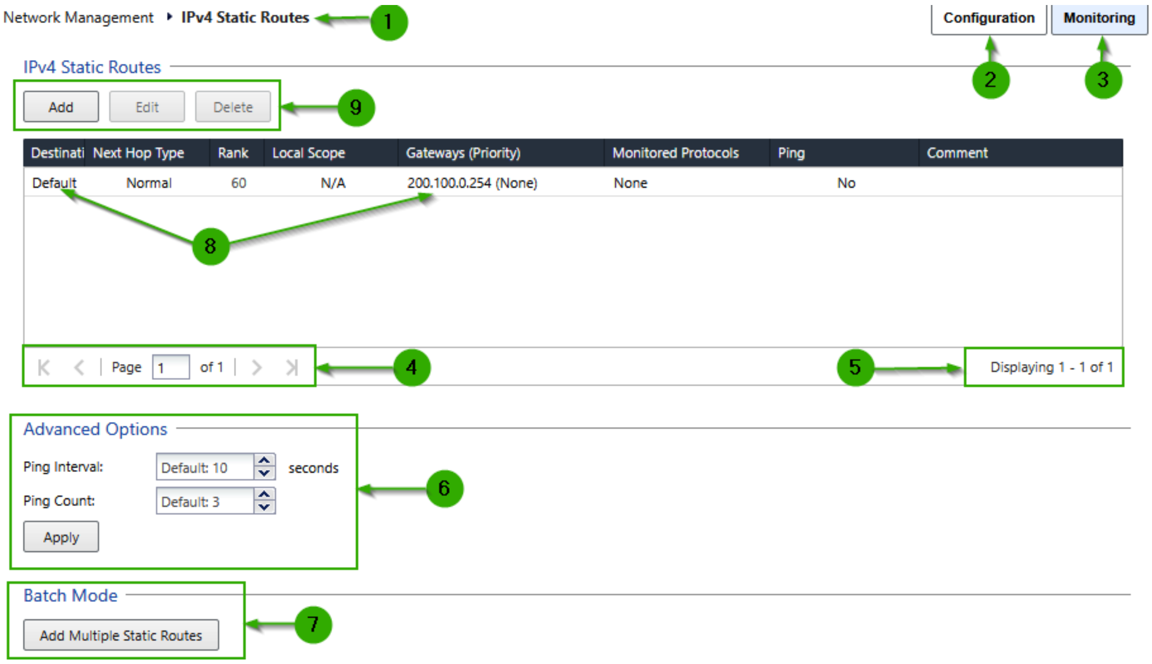
Primary DNS Server: 10.20.20.10

Secondary DNS Server:

Tertiary DNS Server:

Hosts

Host Name	IPv4 Address	IPv6 Address
CPCM1	10.0.0.2	
CPCM2	10.0.0.3	
CPSMS	10.0.0.10	
localhost	127.0.0.1	::1



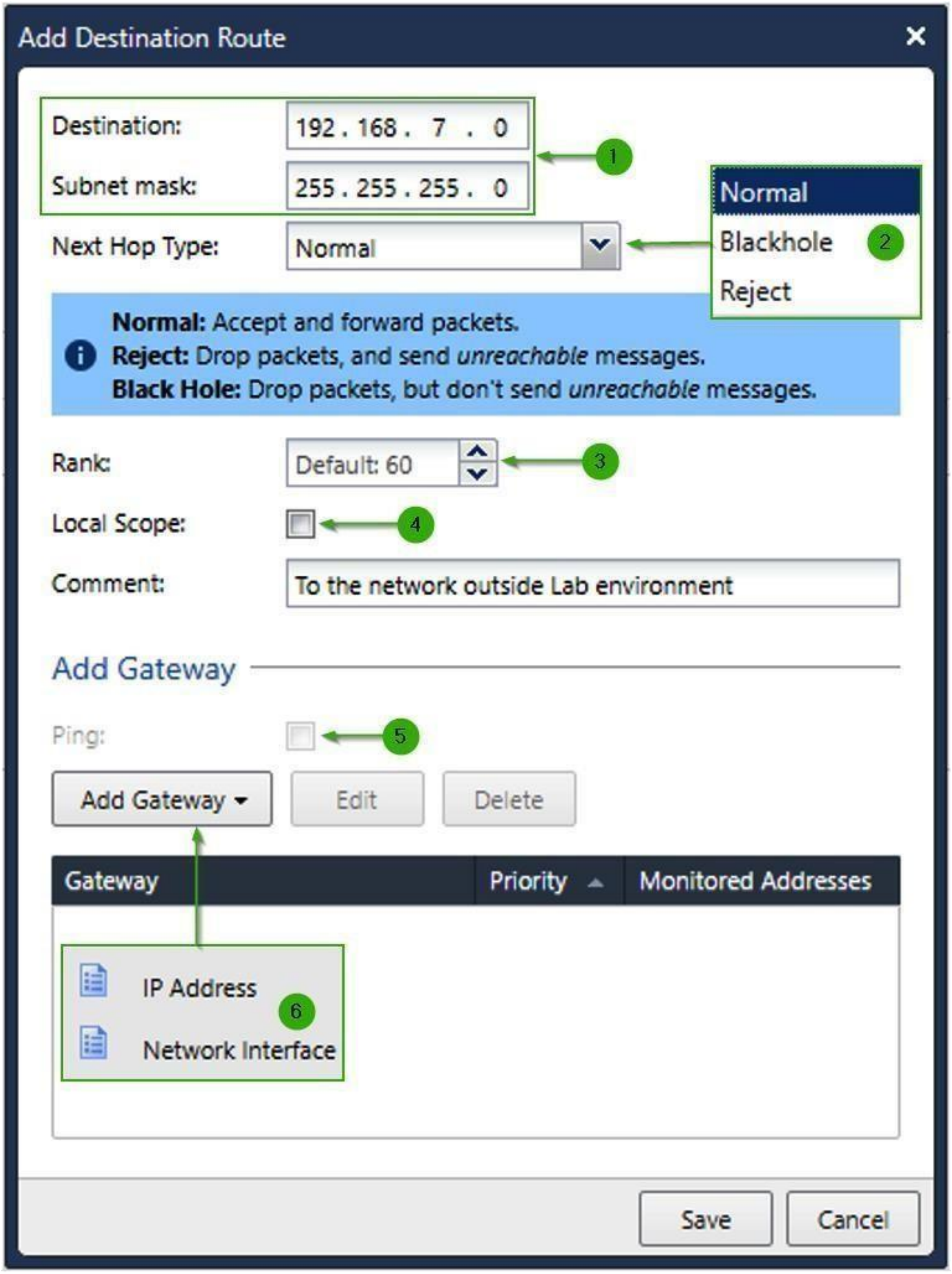
Destinati	Next Hop Type	Rank	Local Scope	Gateways (Priority)	Monitored Protocols	Ping	Comment
Default	Normal	60	N/A	200.100.0.254 (None)	None	No	

Page 1 of 1

Displaying 1 - 1 of 1

Ping Interval: Default: 10 seconds

Ping Count: Default: 3



Add Destination Route

Destination: 192 . 168 . 7 . 0

Subnet mask: 255 . 255 . 255 . 0

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send *unreachable* messages.
Black Hole: Drop packets, but don't send *unreachable* messages.

Rank: Default: 60

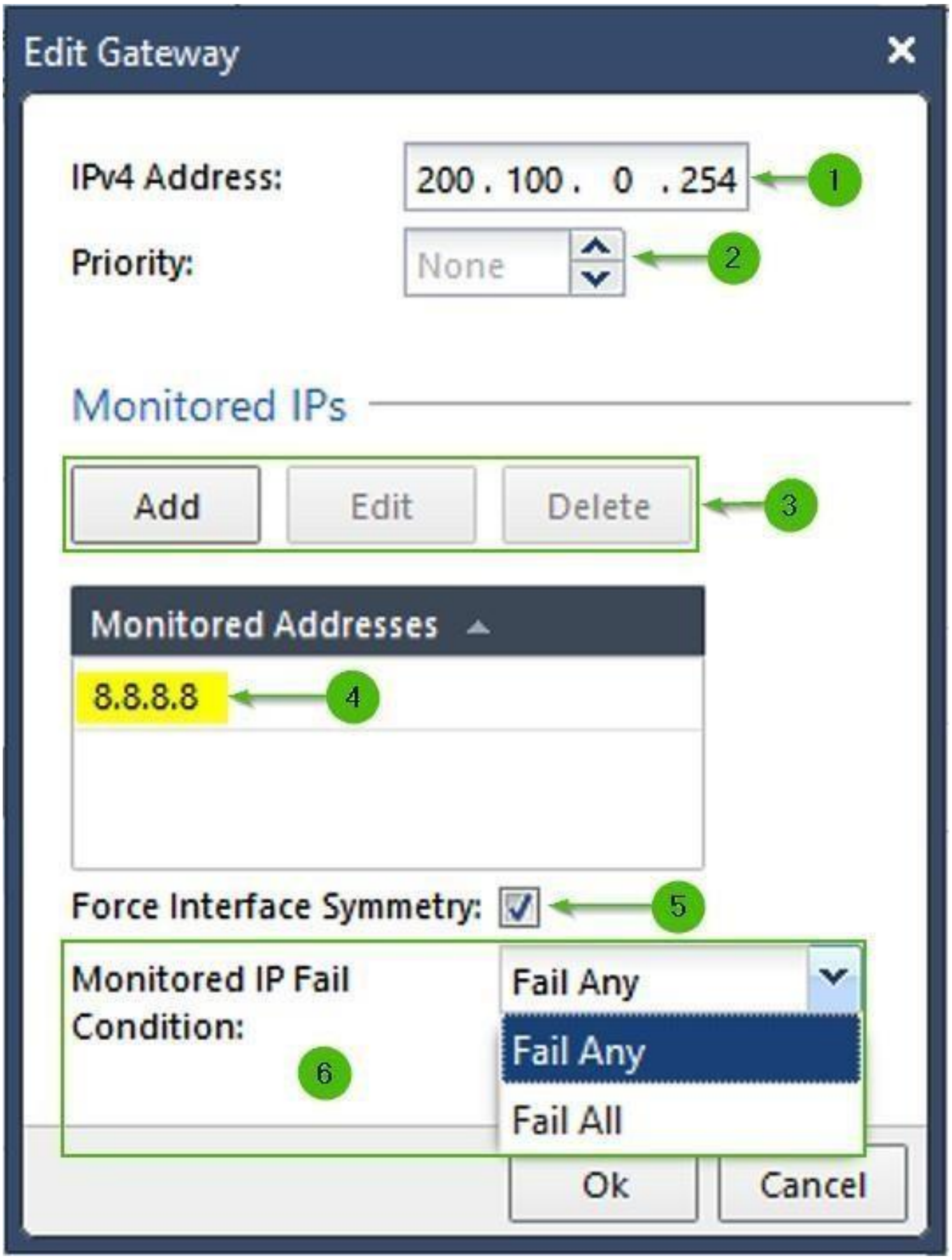
Local Scope: □

Comment: To the network outside Lab environment

Add Gateway

Ping: □

Gateway	Priority	Monitored Addresses



Edit Gateway

IPv4 Address: 200 . 100 . 0 . 254

Priority: None

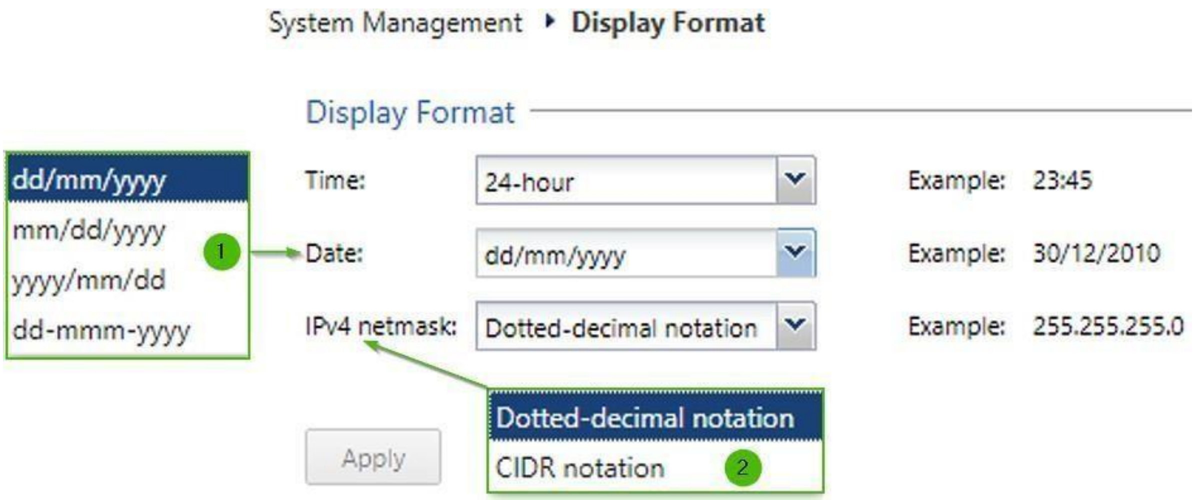
Monitored IPs

Monitored Addresses

8.8.8.8

Force Interface Symmetry: ☑

Monitored IP Fail Condition: Fail Any



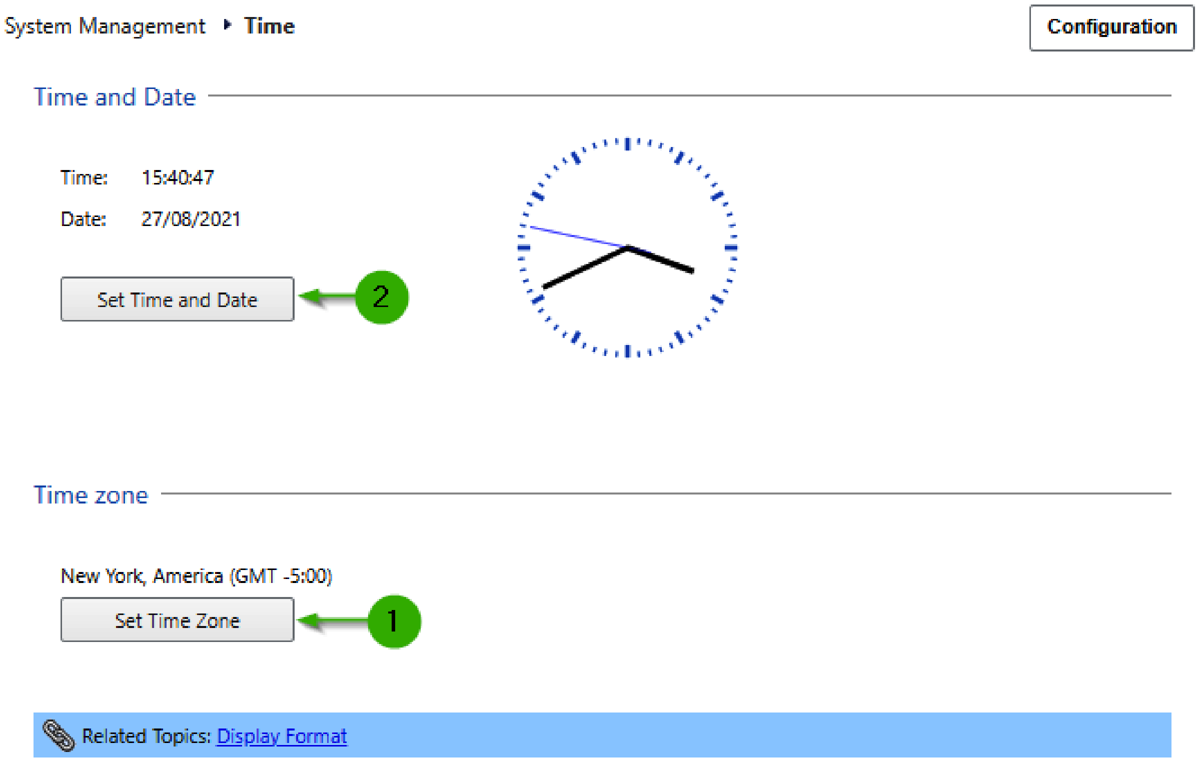
System Management ▸ **Display Format**

Display Format

Time: 24-hour — Example: 23:45

Date: dd/mm/yyyy — Example: 30/12/2010

IPv4 netmask: Dotted-decimal notation — Example: 255.255.255.0



System Management ▸ **Time**

Time and Date

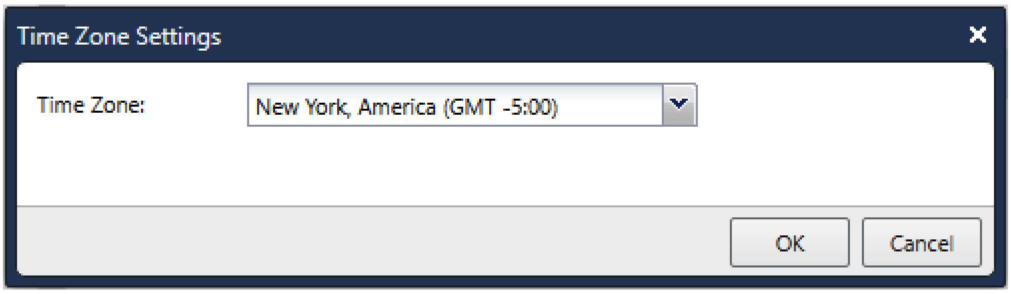
Time: 15:40:47

Date: 27/08/2021

Time zone

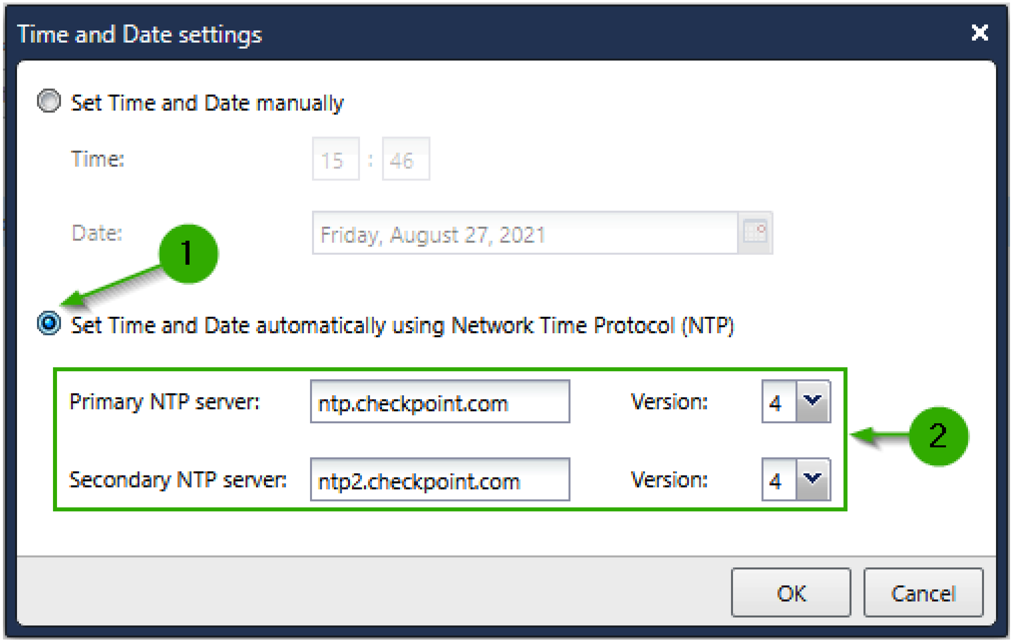
New York, America (GMT -5:00)

Related Topics: Display Format



Time Zone Settings

Time Zone: New York, America (GMT -5:00)



Time and Date settings

○ Set Time and Date manually

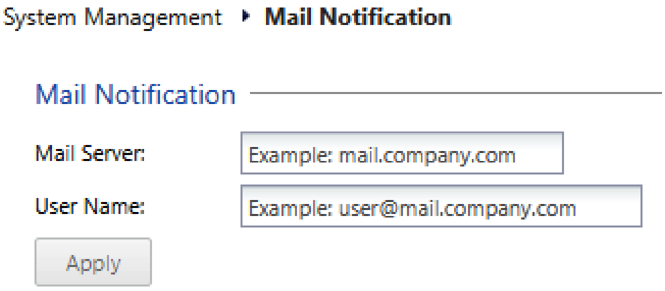
Time: 15 : 46

Date: Friday, August 27, 2021

● Set Time and Date automatically using Network Time Protocol (NTP)

Primary NTP server: ntp.checkpoint.com Version: 4

Secondary NTP server: ntp2.checkpoint.com Version: 4

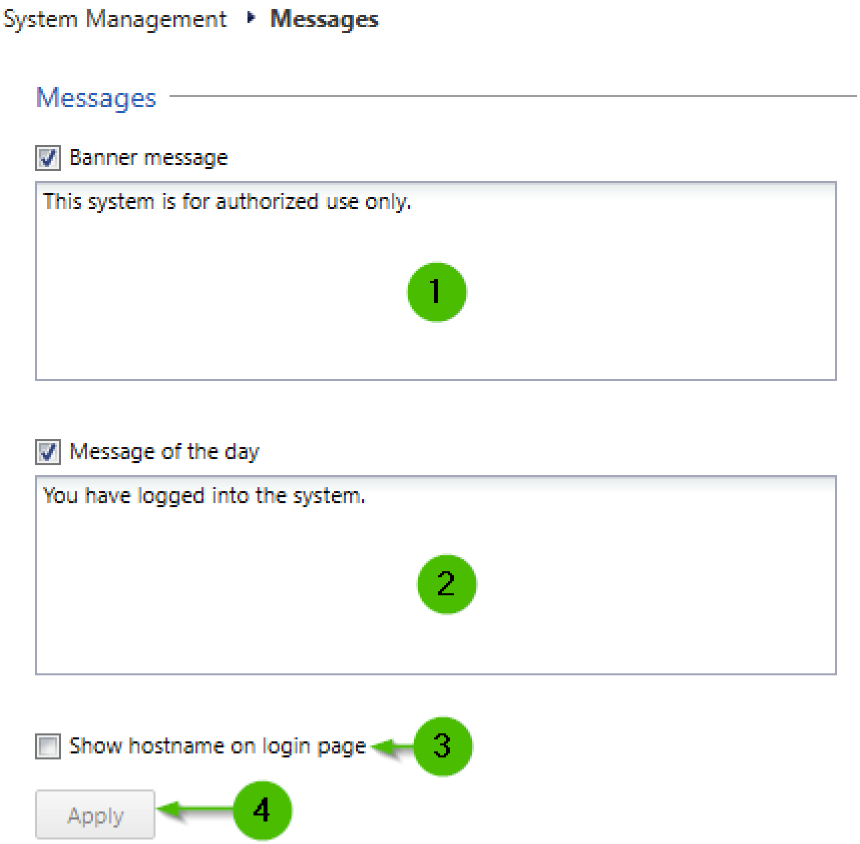


System Management ▸ **Mail Notification**

Mail Notification

Mail Server: Example: mail.company.com

User Name: Example: user@mail.company.com



System Management ▸ **Messages**

Messages

☑ Banner message

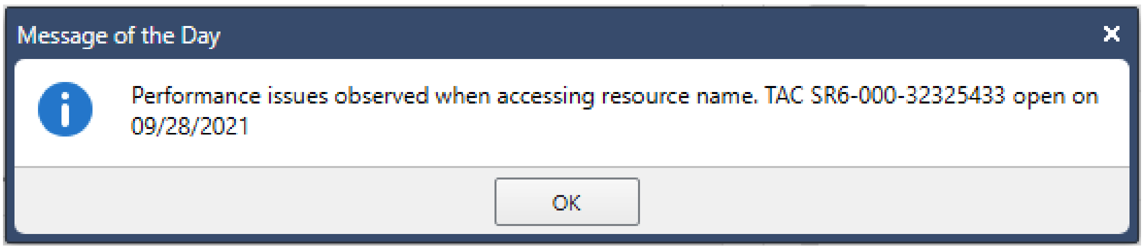
This system is for authorized use only.

☑ Message of the day

You have logged into the system.

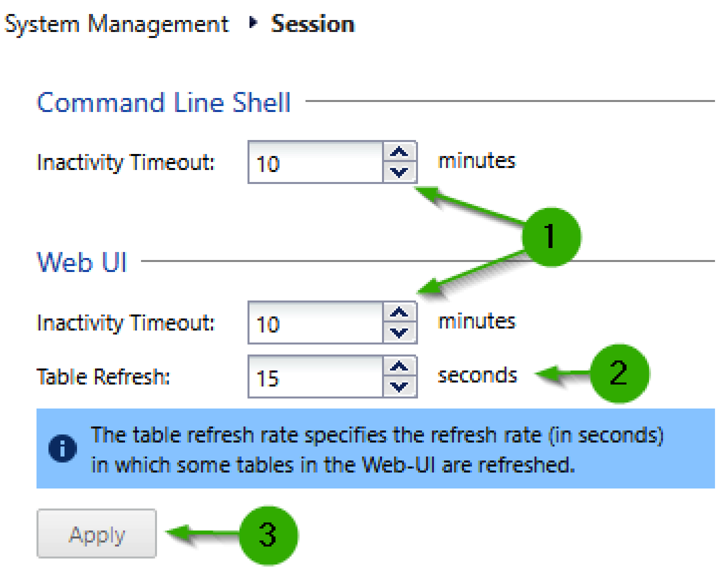
☐ Show hostname on login page

Apply



Message of the Day

Performance issues observed when accessing resource name. TAC SR6-000-32325433 open on 09/28/2021



System Management ▸ **Session**

Command Line Shell

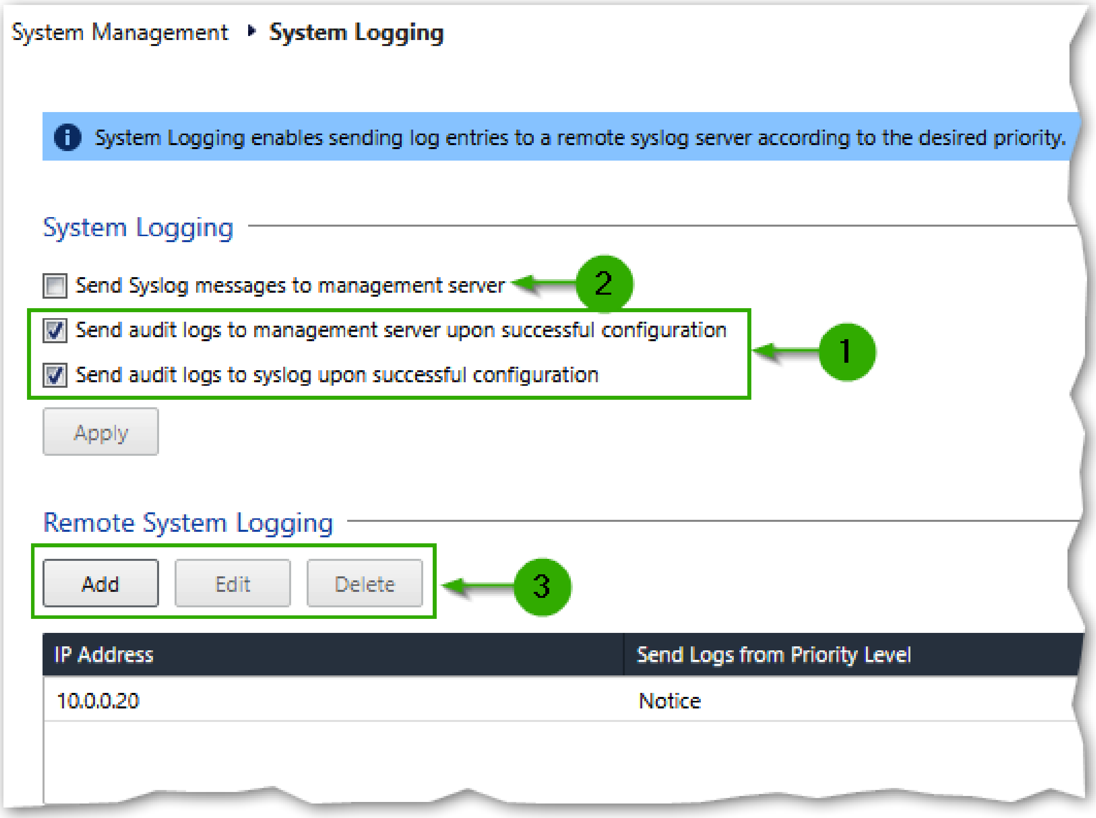
Inactivity Timeout: 10 minutes

Web UI

Inactivity Timeout: 10 minutes

Table Refresh: 15 seconds

The table refresh rate specifies the refresh rate (in seconds) in which some tables in the Web-UI are refreshed.



System Management ▸ **System Logging**

System Logging enables sending log entries to a remote syslog server according to the desired priority.

System Logging

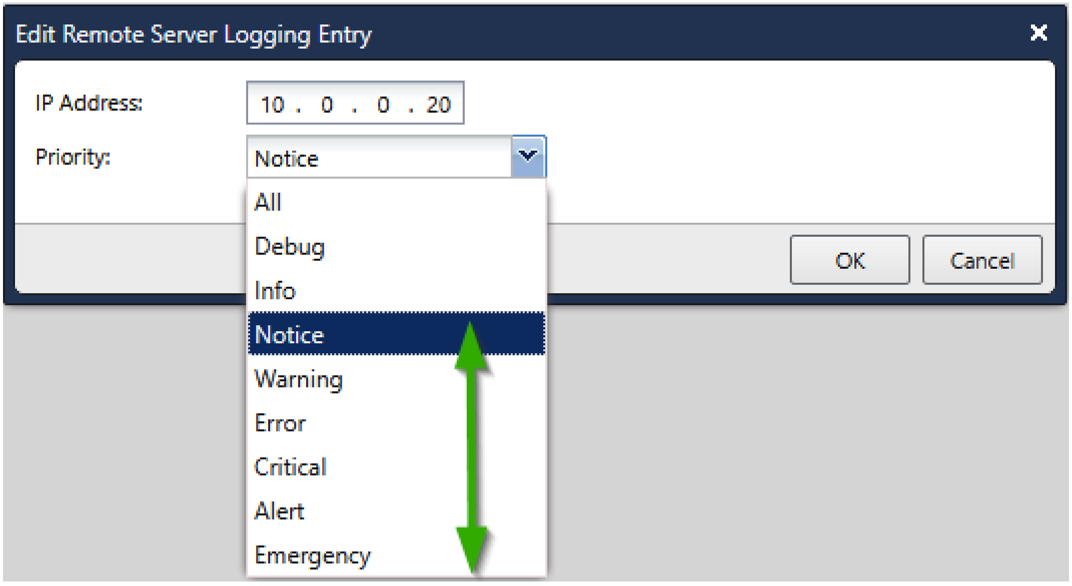
□ Send Syslog messages to management server

☑ Send audit logs to management server upon successful configuration

☑ Send audit logs to syslog upon successful configuration

Remote System Logging

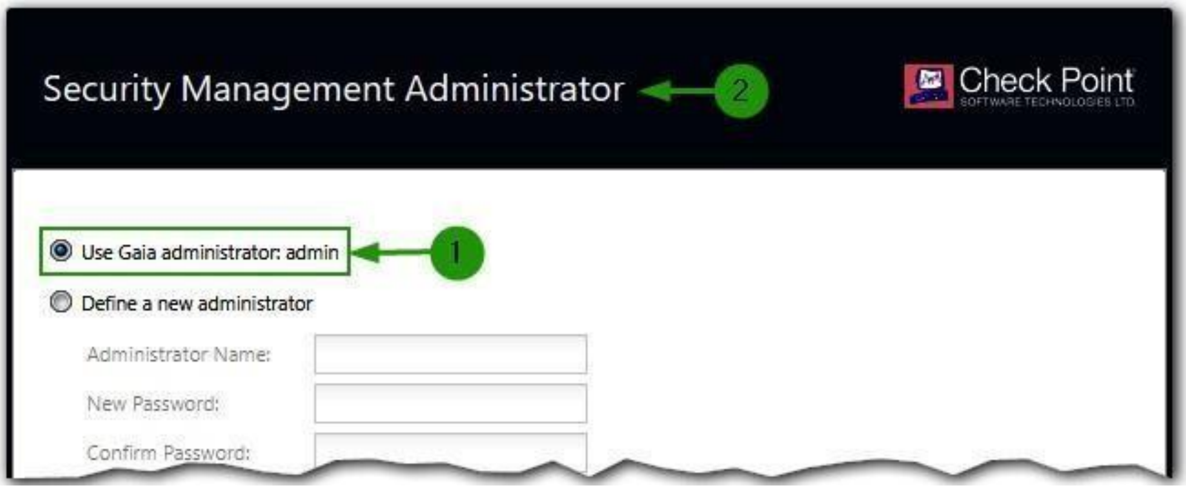
IP Address	Send Logs from Priority Level
10.0.0.20	Notice



Edit Remote Server Logging Entry

IP Address: 10 . 0 . 0 . 20

Priority: Notice



Security Management Administrator

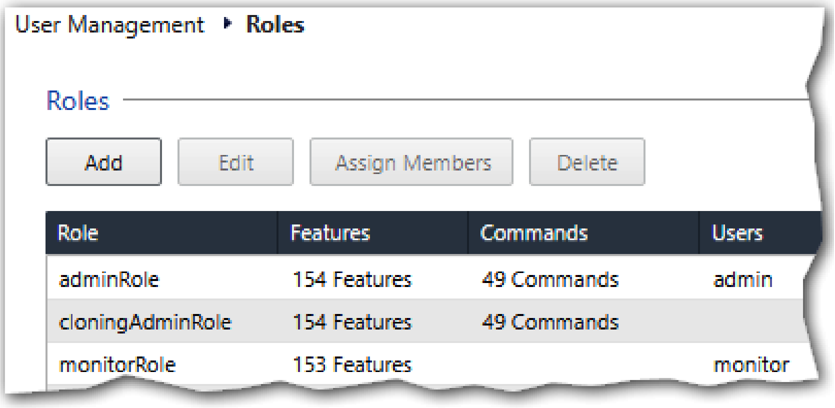
● Use Gaia administrator: admin

○ Define a new administrator

Administrator Name:

New Password:

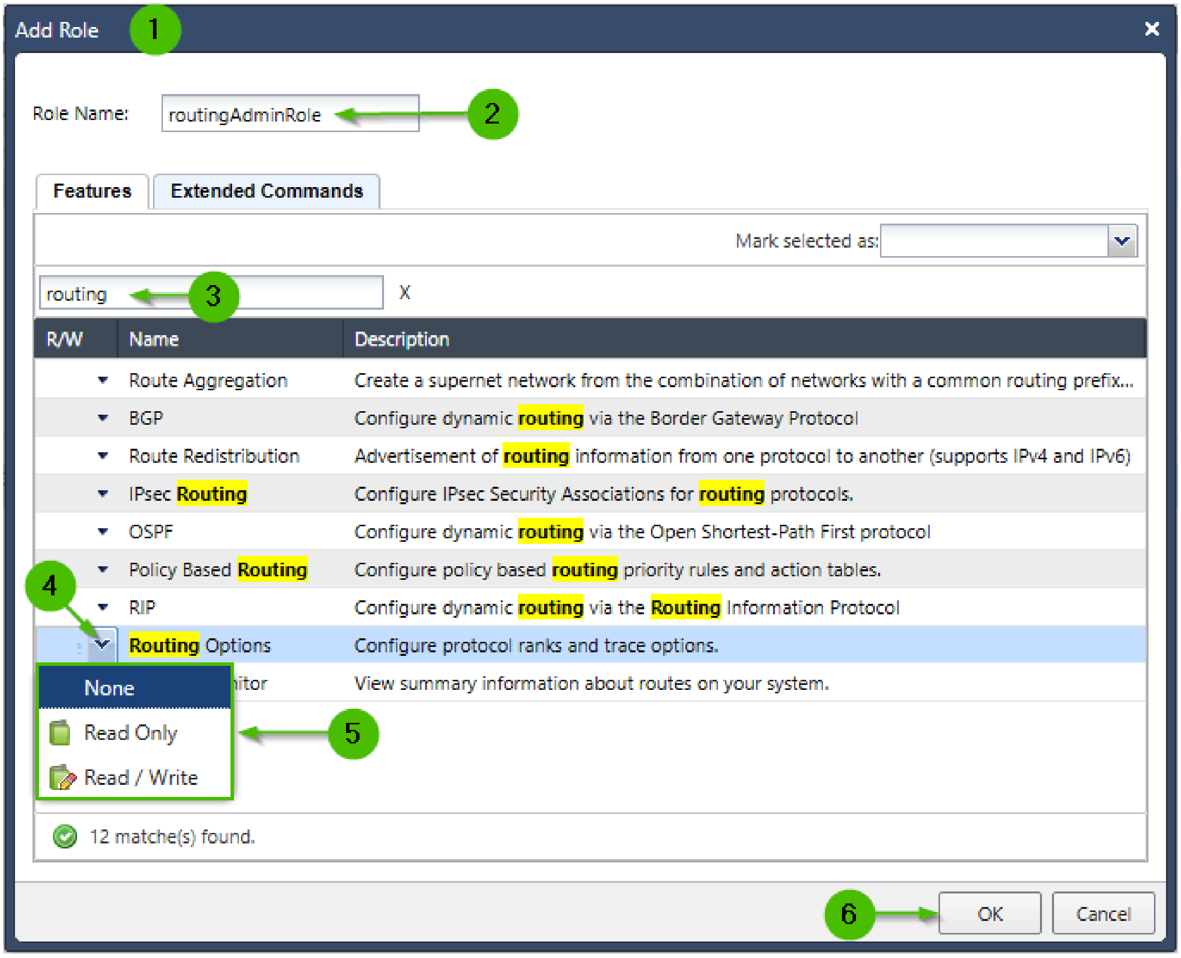
Confirm Password:



User Management ▸ **Roles**

Roles

Role	Features	Commands	Users
adminRole	154 Features	49 Commands	admin
cloningAdminRole	154 Features	49 Commands	
monitorRole	153 Features		monitor



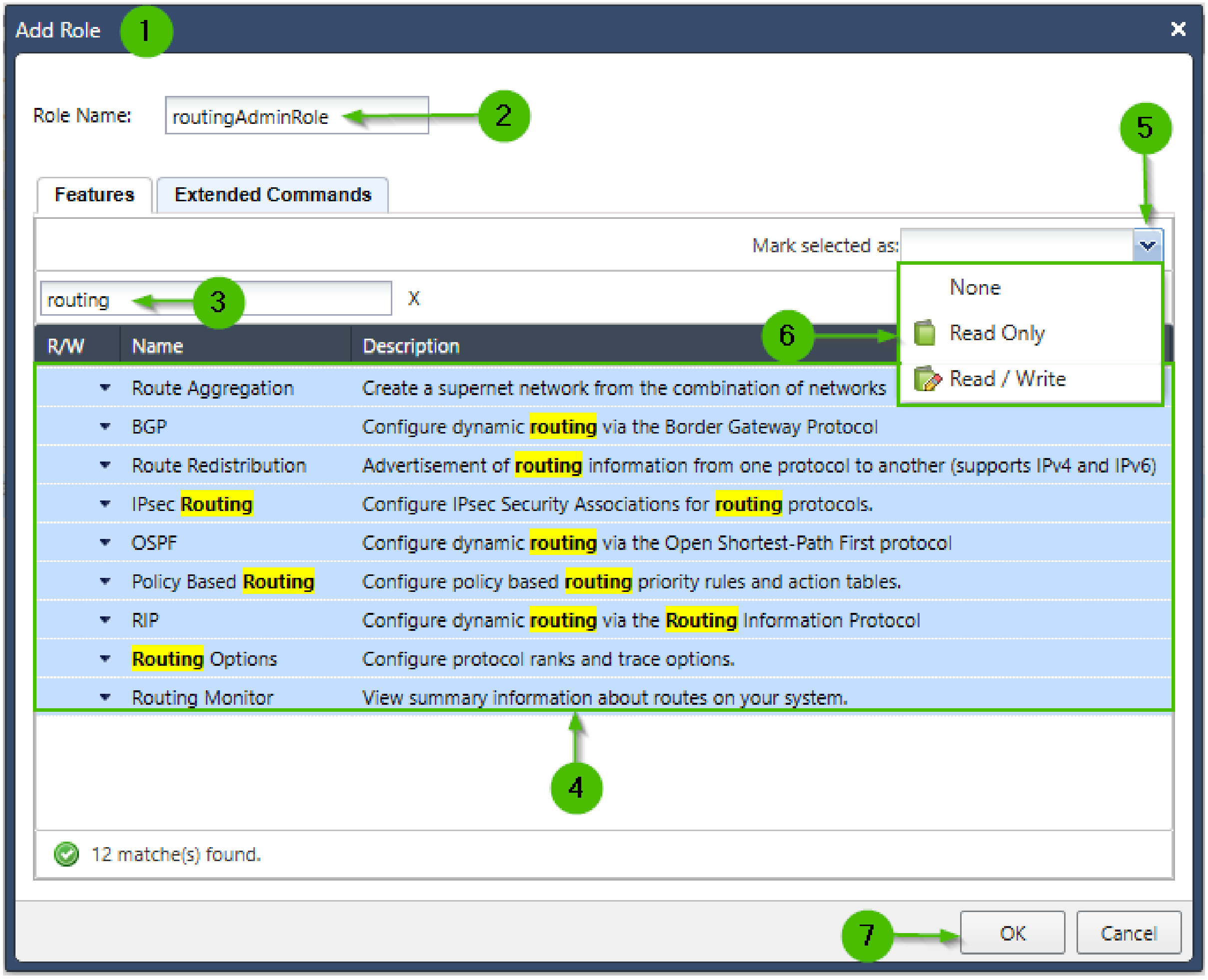
Role Name: routingAdminRole

Mark selected as:

routing

R/W	Name	Description
▾	Route Aggregation	Create a supernet network from the combination of networks with a common routing prefix...
▾	BGP	Configure dynamic routing via the Border Gateway Protocol
▾	Route Redistribution	Advertisement of routing information from one protocol to another (supports IPv4 and IPv6)
▾	IPsec Routing	Configure IPsec Security Associations for routing protocols.
▾	OSPF	Configure dynamic routing via the Open Shortest-Path First protocol
▾	Policy Based Routing	Configure policy based routing priority rules and action tables.
▾	RIP	Configure dynamic routing via the Routing Information Protocol
▾	Routing Options	Configure protocol ranks and trace options.
	itor	View summary information about routes on your system.

✓ 12 matche(s) found.

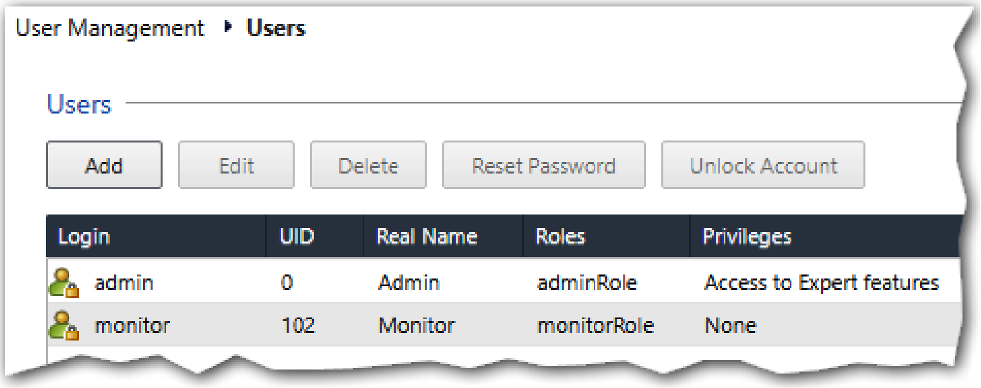


Role Name: routingAdminRole

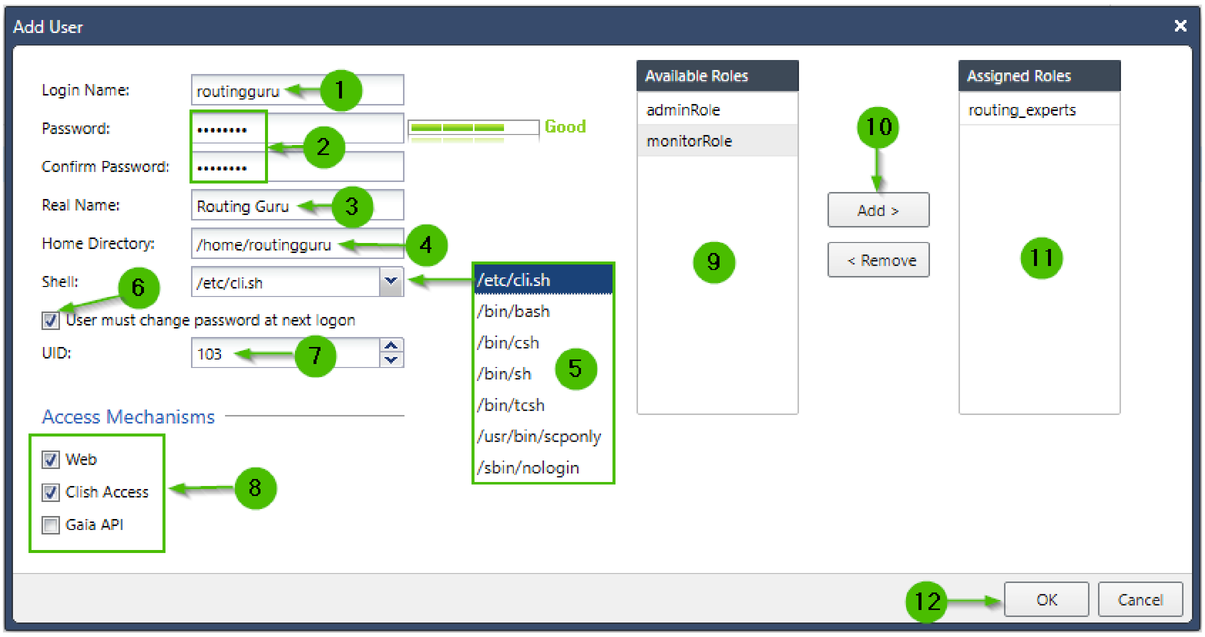
routing

R/W	Name	Description
▾	Route Aggregation	Create a supernet network from the combination of networks
▾	BGP	Configure dynamic routing via the Border Gateway Protocol
▾	Route Redistribution	Advertisement of routing information from one protocol to another (supports IPv4 and IPv6)
▾	IPsec Routing	Configure IPsec Security Associations for routing protocols.
▾	OSPF	Configure dynamic routing via the Open Shortest-Path First protocol
▾	Policy Based Routing	Configure policy based routing priority rules and action tables.
▾	RIP	Configure dynamic routing via the Routing Information Protocol
▾	Routing Options	Configure protocol ranks and trace options.
▾	Routing Monitor	View summary information about routes on your system.

✓ 12 match(s) found.



Login	UID	Real Name	Roles	Privileges
admin	0	Admin	adminRole	Access to Expert features
monitor	102	Monitor	monitorRole	None



Add User

Login Name: routingguru

Password: •••••••• Good

Confirm Password: ••••••••

Real Name: Routing Guru

Home Directory: /home/routingguru

Shell: /etc/cli.sh

☑ User must change password at next logon

UID: 103

Access Mechanisms

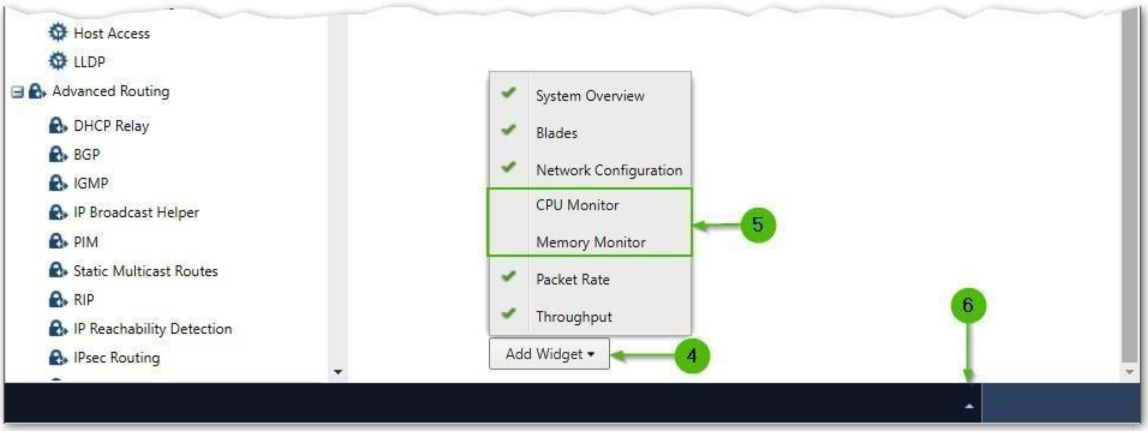
☑ Web

☑ Clish Access

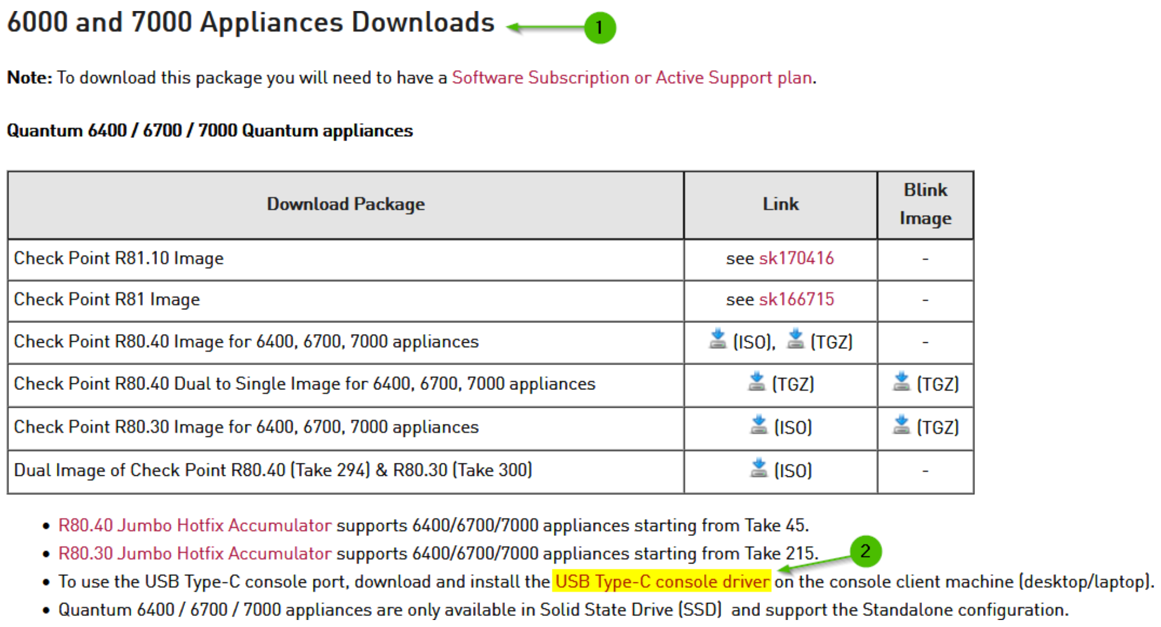
☐ Gaia API

Available Roles: adminRole, monitorRole

Assigned Roles: routing_experts



Chapter 6: Check Point Gaia Command-Line Interface; Backup and Recovery Methods; CPUSE



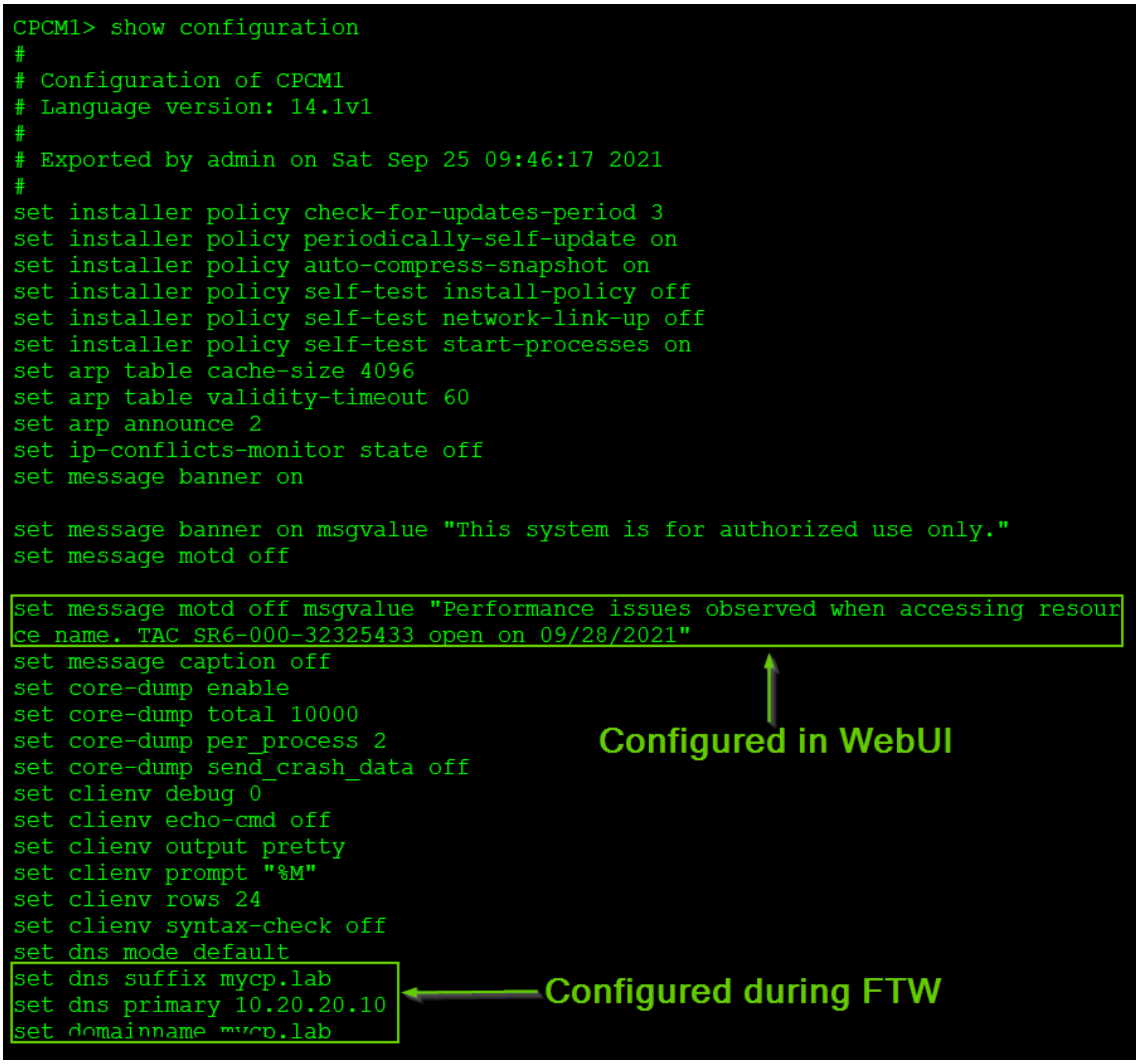
6000 and 7000 Appliances Downloads

Note: To download this package you will need to have a Software Subscription or Active Support plan.

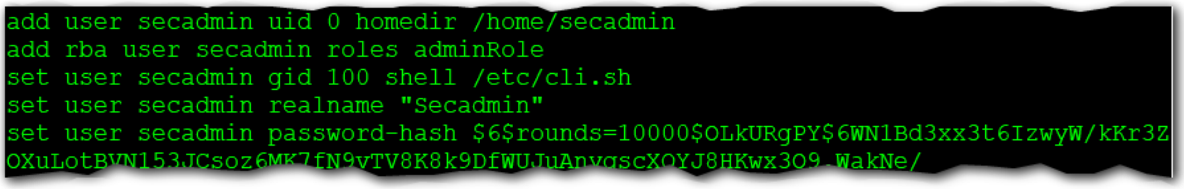
Quantum 6400 / 6700 / 7000 Quantum appliances

Download Package	Link	Blink Image
Check Point R81.10 Image	see sk170416	-
Check Point R81 Image	see sk166715	-
Check Point R80.40 Image for 6400, 6700, 7000 appliances	⬇ (ISO), ⬇ (TGZ)	-
Check Point R80.40 Dual to Single Image for 6400, 6700, 7000 appliances	⬇ (TGZ)	⬇ (TGZ)
Check Point R80.30 Image for 6400, 6700, 7000 appliances	⬇ (ISO)	⬇ (TGZ)
Dual Image of Check Point R80.40 (Take 294) & R80.30 (Take 300)	⬇ (ISO)	-

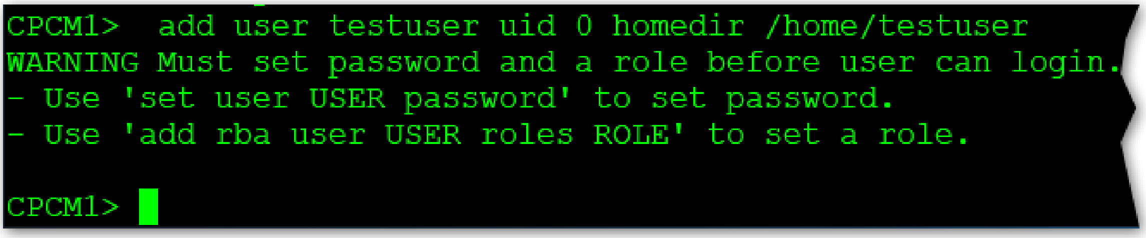
- R80.40 Jumbo Hotfix Accumulator supports 6400/6700/7000 appliances starting from Take 45.
- R80.30 Jumbo Hotfix Accumulator supports 6400/6700/7000 appliances starting from Take 215.
- To use the USB Type-C console port, download and install the USB Type-C console driver on the console client machine (desktop/laptop).
- Quantum 6400 / 6700 / 7000 appliances are only available in Solid State Drive (SSD) and support the Standalone configuration.



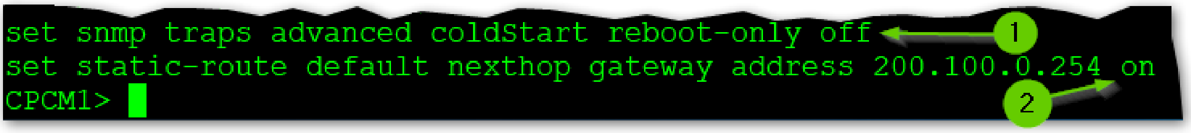
```
CPCM1> show configuration
#
# Configuration of CPCM1
# Language version: 14.1v1
#
# Exported by admin on Sat Sep 25 09:46:17 2021
#
set installer policy check-for-updates-period 3
set installer policy periodically-self-update on
set installer policy auto-compress-snapshot on
set installer policy self-test install-policy off
set installer policy self-test network-link-up off
set installer policy self-test start-processes on
set arp table cache-size 4096
set arp table validity-timeout 60
set arp announce 2
set ip-conflicts-monitor state off
set message banner on

set message banner on msgvalue "This system is for authorized use only."
set message motd off

set message motd off msgvalue "Performance issues observed when accessing resour
ce name. TAC SR6-000-32325433 open on 09/28/2021"
set message caption off
set core-dump enable
set core-dump total 10000
set core-dump per_process 2
set core-dump send_crash_data off
set clienv debug 0
set clienv echo-cmd off
set clienv output pretty
set clienv prompt "%M"
set clienv rows 24
set clienv syntax-check off
set dns mode default
set dns suffix mycp.lab
set dns primary 10.20.20.10
set domainname mycp.lab
```



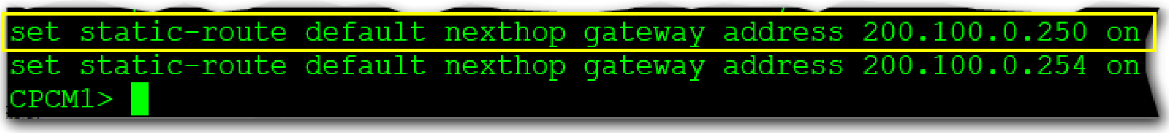
```
add user secadmin uid 0 homedir /home/secadmin
add rba user secadmin roles adminRole
set user secadmin gid 100 shell /etc/cli.sh
set user secadmin realname "Secadmin"
set user secadmin password-hash $6$rounds=10000$OLkURgPY$6WN1Bd3xx3t6IzwyW/kKr3Z
OXuLotBVN153JCsoz6MK7fN9vTV8K8k9DfWUJuAnvgscXOYJ8HKwx3O9.WakNe/
```



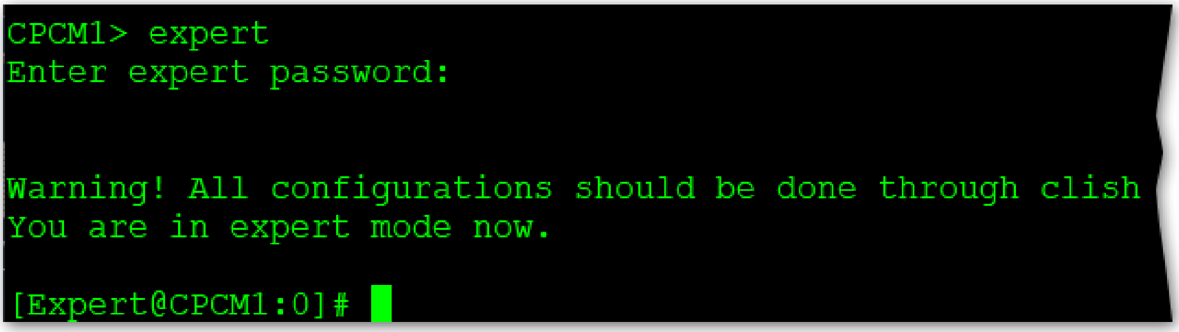
```
CPCM1>  add user testuser uid 0 homedir /home/testuser
WARNING Must set password and a role before user can login.
- Use 'set user USER password' to set password.
- Use 'add rba user USER roles ROLE' to set a role.

CPCM1>
```



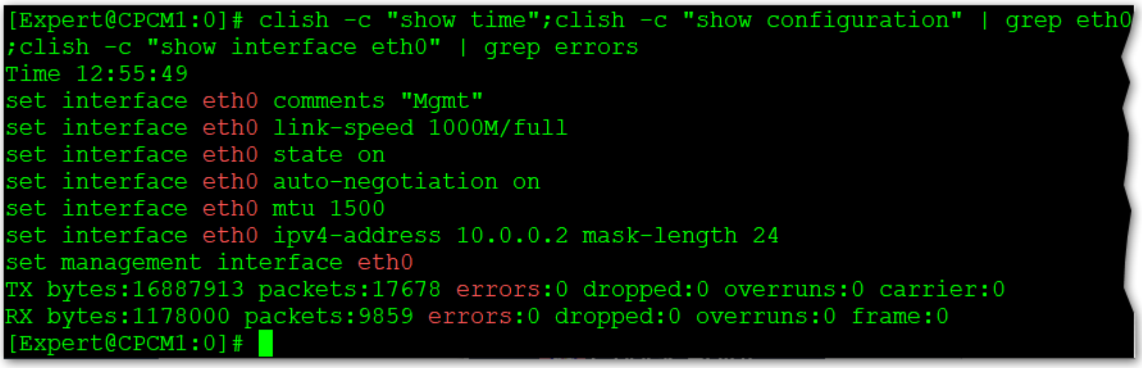
```
set snmp traps advanced coldStart reboot-only off
set static-route default nexthop gateway address 200.100.0.254 on
CPCM1>
```



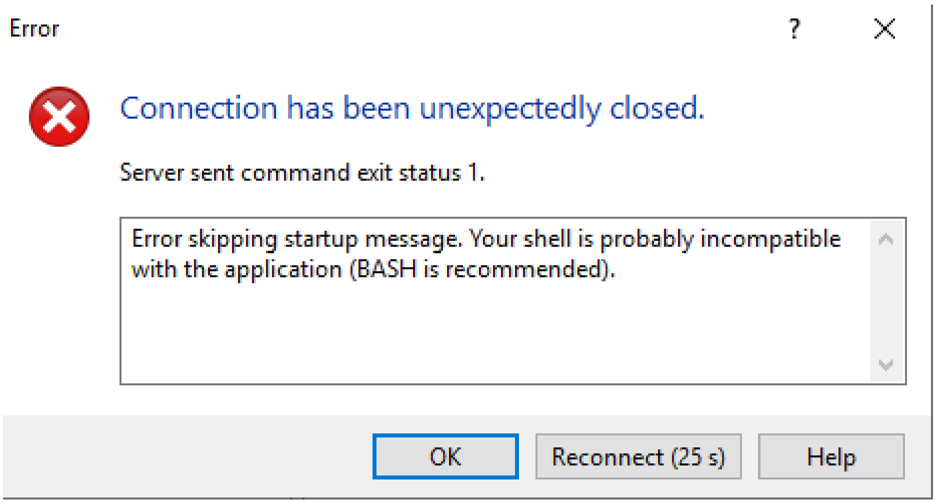
```
set static-route default nexthop gateway address 200.100.0.250 on
set static-route default nexthop gateway address 200.100.0.254 on
CPCM1>
```



```
CPCM1> expert
Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@CPCM1:0]#
```



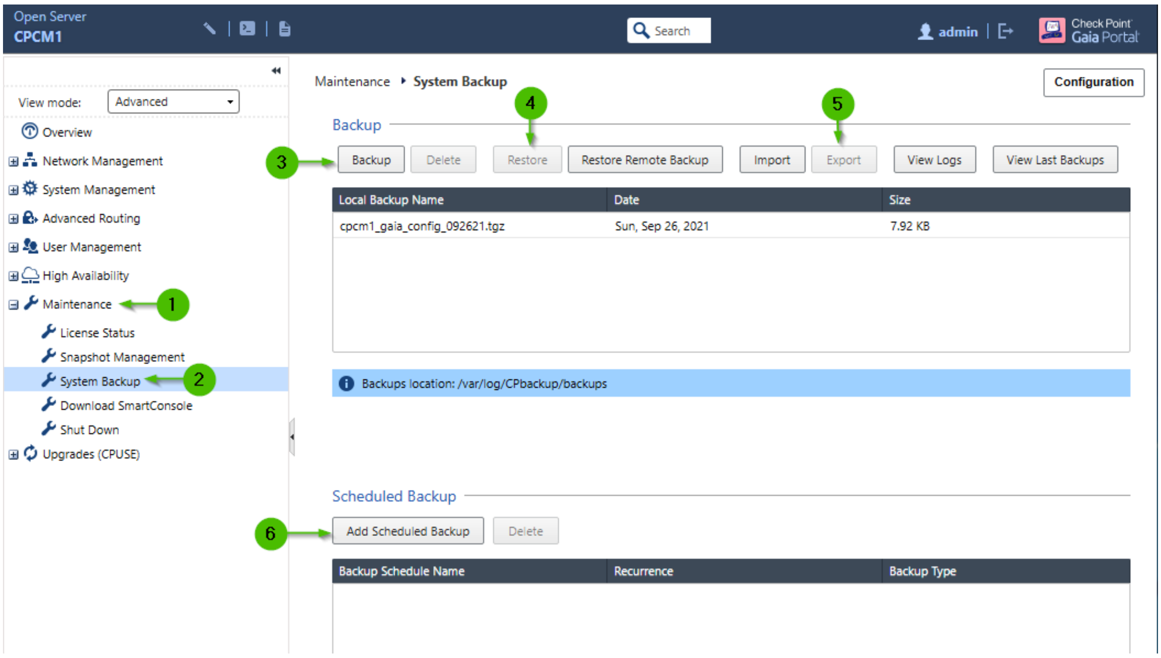
```
[Expert@CPCM1:0]# clish -c "show time";clish -c "show configuration" | grep eth0
;clish -c "show interface eth0" | grep errors
Time 12:55:49
set interface eth0 comments "Mgmt"
set interface eth0 link-speed 1000M/full
set interface eth0 state on
set interface eth0 auto-negotiation on
set interface eth0 mtu 1500
set interface eth0 ipv4-address 10.0.0.2 mask-length 24
set management interface eth0
TX bytes:16887913 packets:17678 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:1178000 packets:9859 errors:0 dropped:0 overruns:0 frame:0
[Expert@CPCM1:0]#
```



Connection has been unexpectedly closed.

Server sent command exit status 1.

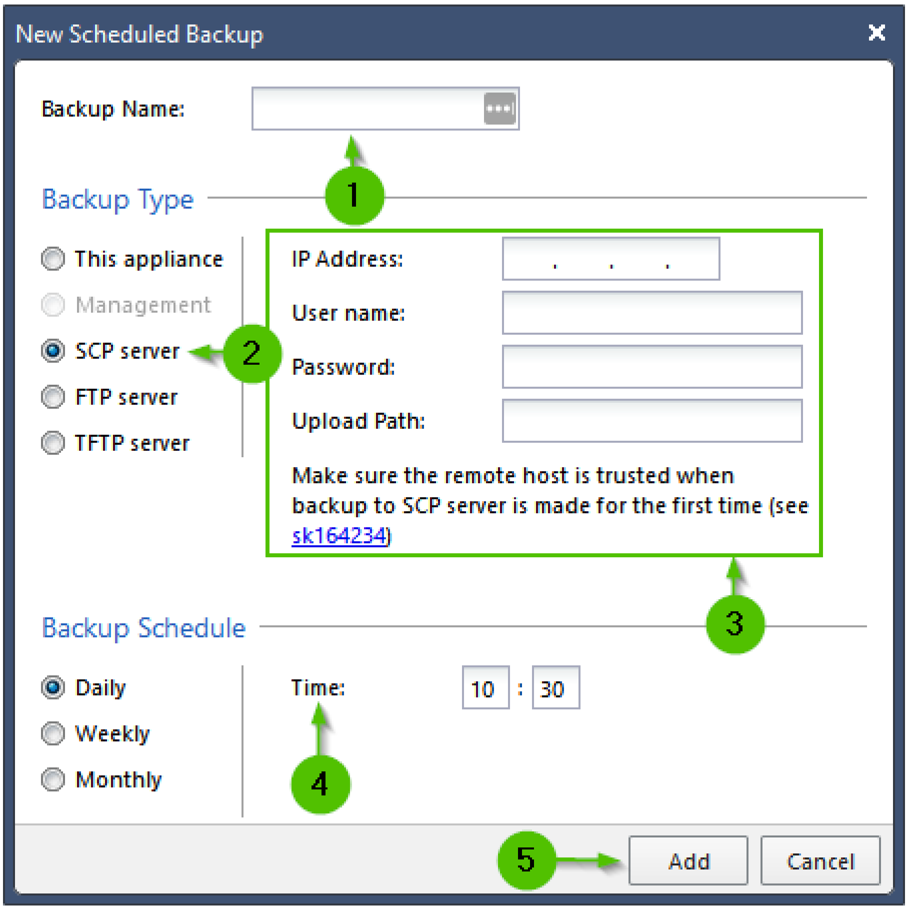
```
Error skipping startup message. Your shell is probably incompatible
with the application (BASH is recommended).
```



Local Backup Name	Date	Size
cpcm1_gaia_config_092621.tgz	Sun, Sep 26, 2021	7.92 KB

Backups location: /var/log/CPbackup/backups

Backup Schedule Name	Recurrence	Backup Type


New Scheduled Backup

Backup Name:

Backup Type

- ○ This appliance
- ○ Management
- ● SCP server
- ○ FTP server
- ○ TFTP server

IP Address: . . .

User name:

Password:

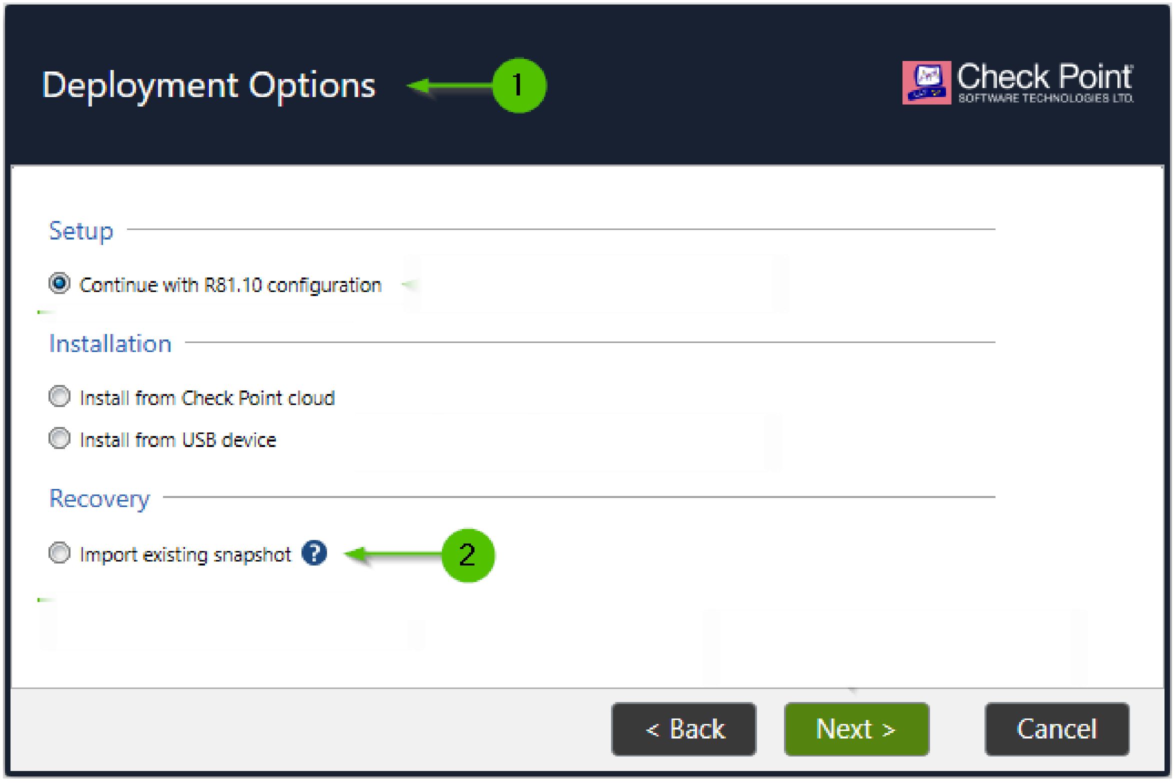
Upload Path:

Make sure the remote host is trusted when backup to SCP server is made for the first time (see sk164234)

Backup Schedule

- ● Daily
- ○ Weekly
- ○ Monthly

Time: 10 : 30


Deployment Options

Setup

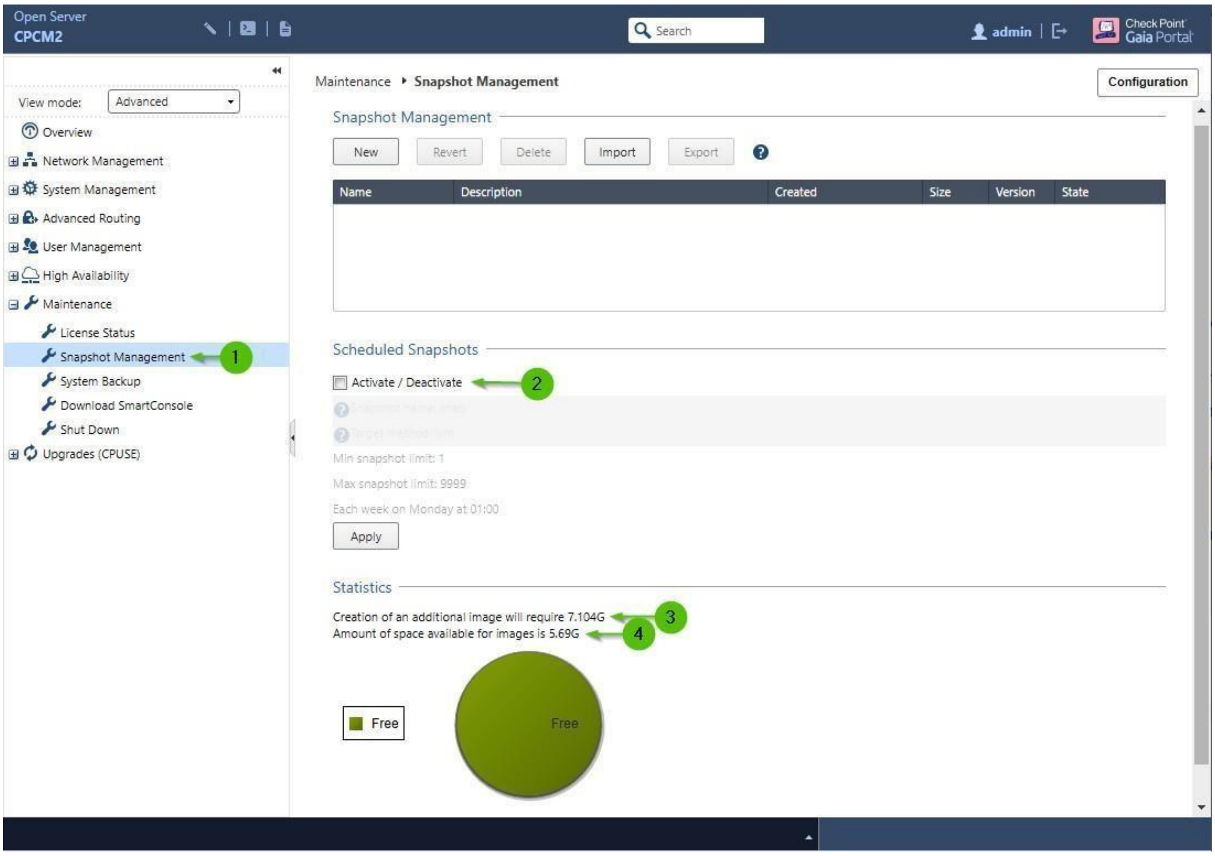
- ● Continue with R81.10 configuration

Installation

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

Recovery

- ○ Import existing snapshot ?



☐ Activate / Deactivate

Min snapshot limit: 1

Max snapshot limit: 9999

Each week on Monday at 01:00

Creation of an additional image will require 7.104G

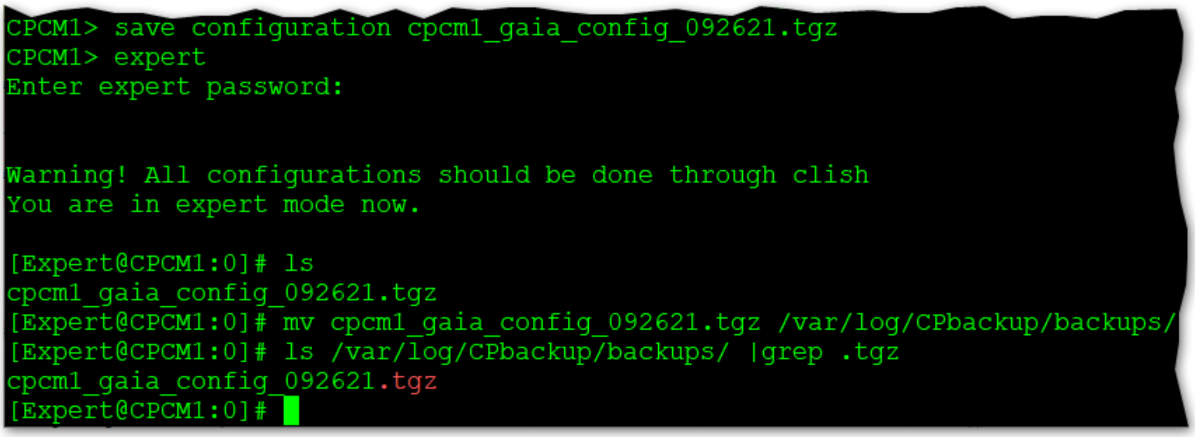
Amount of space available for images is 5.69G

To manually install the latest version of the Check Point Upgrade Tools Package:

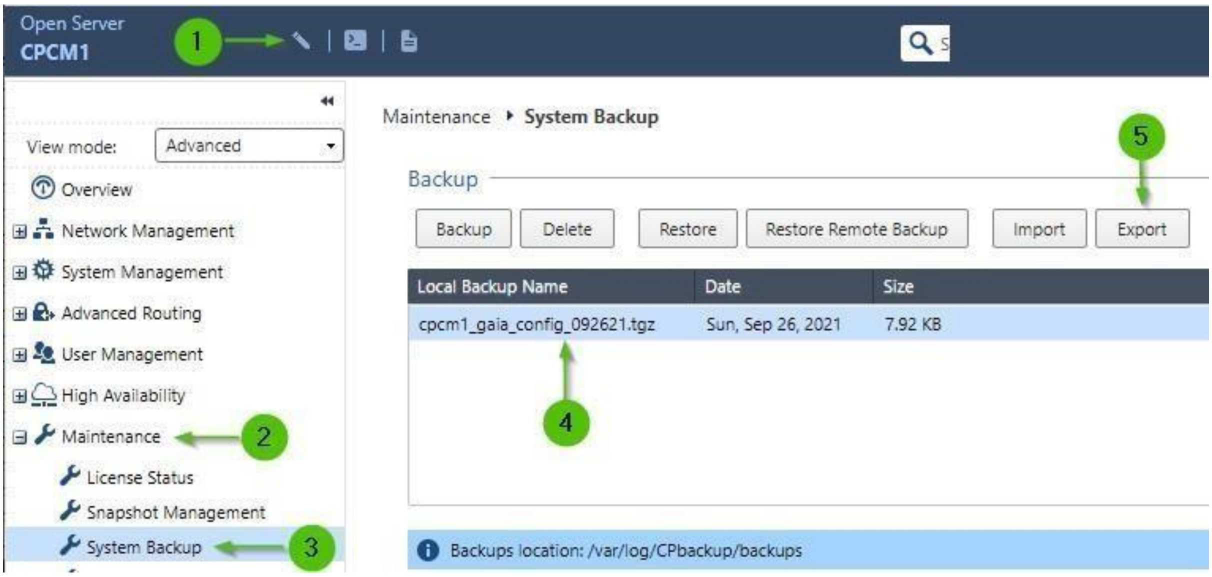
1. Make sure your Deployment Agent is up-to-date.
   To download latest Deployment Agent, refer to sk92449.

2. Download the applicable Check Point Upgrade Tools Package from the table below:

Target Version (to which you upgrade)	Download Link
R80.20	(TGZ)
R80.20.M2	(TGZ)
R80.30	(TGZ)
R80.40	(TGZ)
R81	(TGZ)
R81.10	(TGZ)

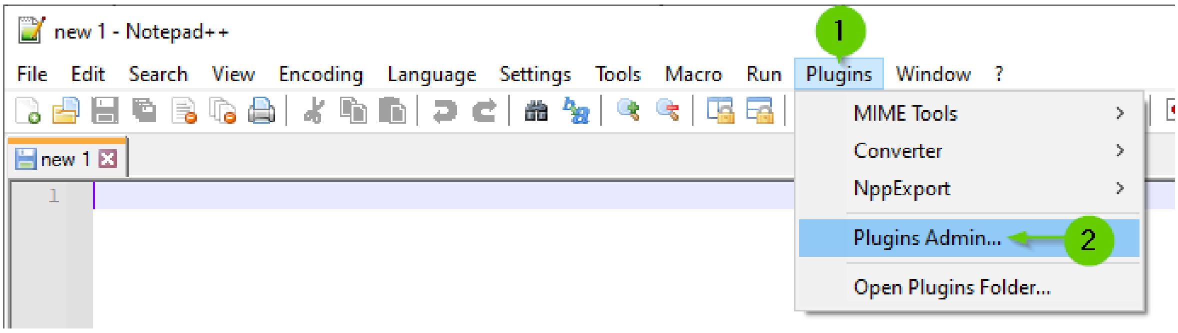


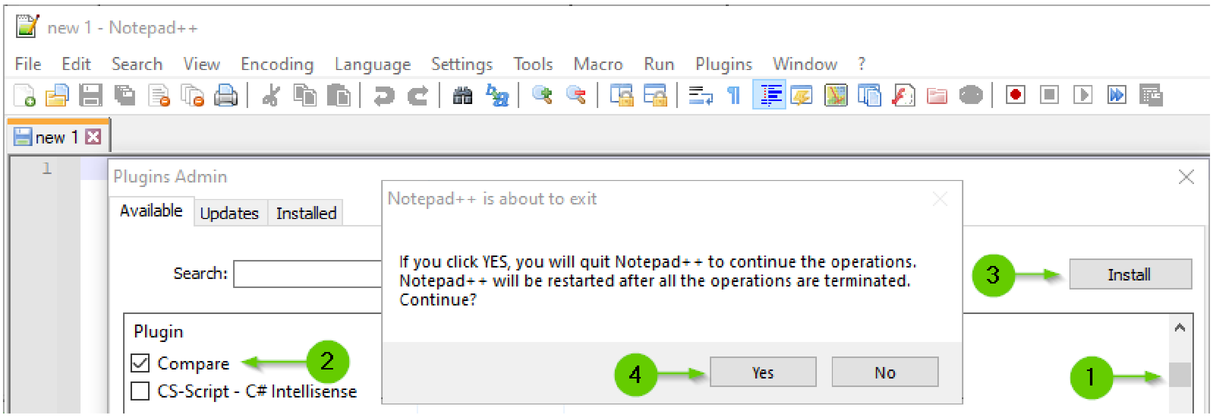
```
CPCM1> save configuration cpcm1_gaia_config_092621.tgz
CPCM1> expert
Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@CPCM1:0]# ls
cpcm1_gaia_config_092621.tgz
[Expert@CPCM1:0]# mv cpcm1_gaia_config_092621.tgz /var/log/CPbackup/backups/
[Expert@CPCM1:0]# ls /var/log/CPbackup/backups/ |grep .tgz
cpcm1_gaia_config_092621.tgz
[Expert@CPCM1:0]#
```



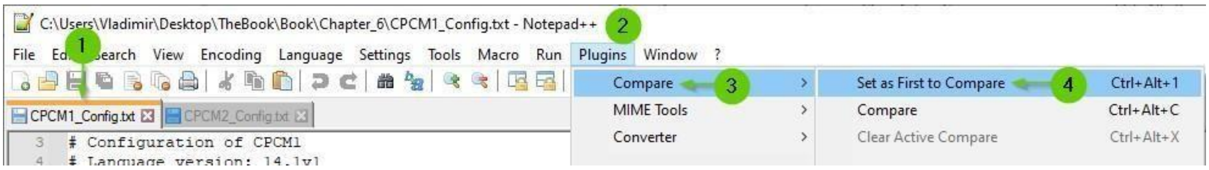
Local Backup Name	Date	Size
cpcm1_gaia_config_092621.tgz	Sun, Sep 26, 2021	7.92 KB

Backups location: /var/log/CPbackup/backups

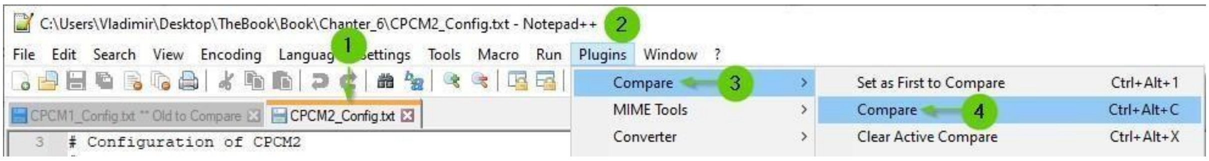



new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
Plugins Admin
Available Updates Installed
Search:
Plugin
☑ Compare
□ CS-Script - C# Intellisense
Install
Notepad++ is about to exit
Yes
No
1
2
3
4

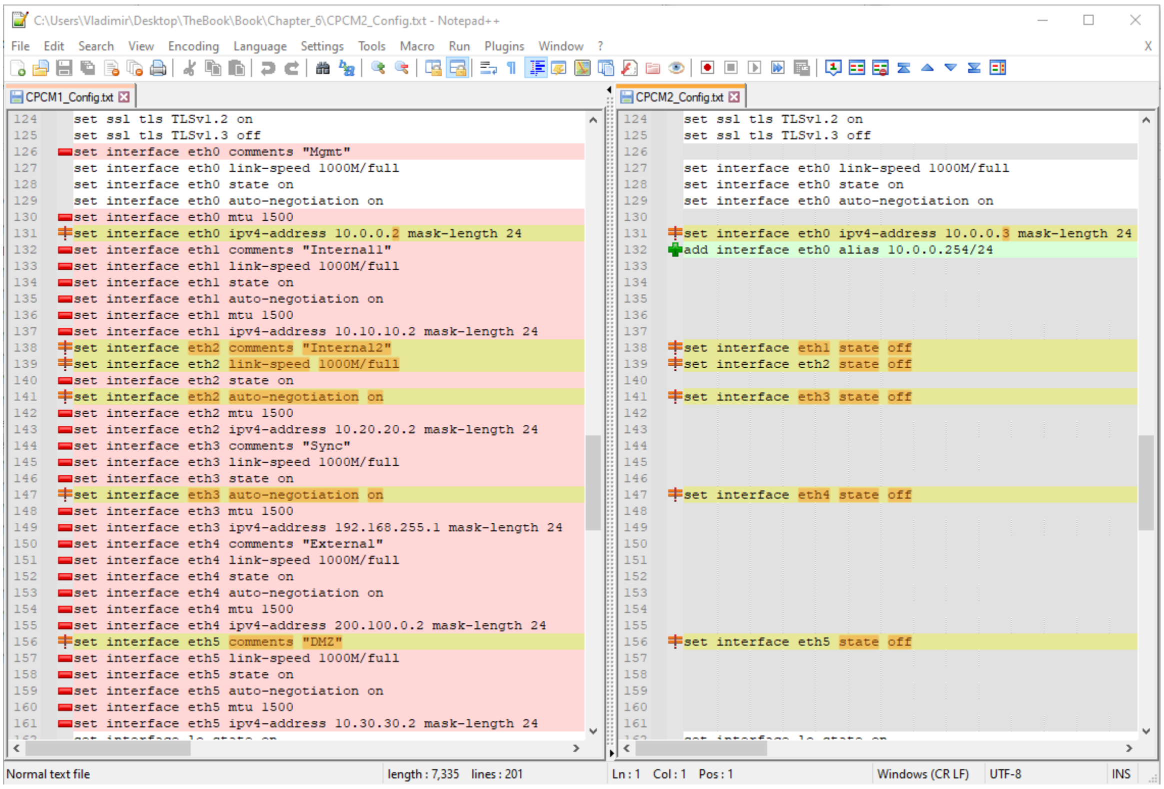
If you click YES, you will quit Notepad++ to continue the operations.
Notepad++ will be restarted after all the operations are terminated.
Continue?


C:\Users\Vladimir\Desktop\TheBook\Book\Chapter_6\CPCM1_Config.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
CPCM1_Config.txt
CPCM2_Config.txt
Compare
MIME Tools
Converter
Set as First to Compare Ctrl+Alt+1
Compare Ctrl+Alt+C
Clear Active Compare Ctrl+Alt+X
1
2
3
4

```
# Configuration of CPCM1
# Language version: 14.1v1
```

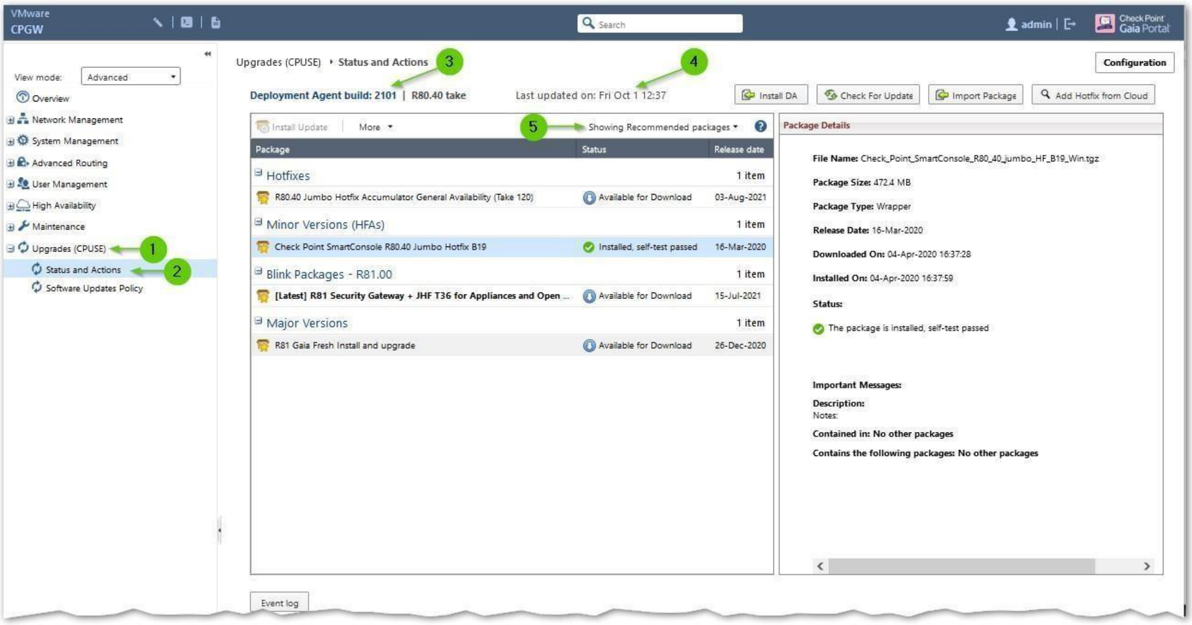

C:\Users\Vladimir\Desktop\TheBook\Book\Chapter_6\CPCM2_Config.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
CPCM1_Config.txt ** Old to Compare
CPCM2_Config.txt
Compare
MIME Tools
Converter
Set as First to Compare Ctrl+Alt+1
Compare Ctrl+Alt+C
Clear Active Compare Ctrl+Alt+X
1
2
3
4

```
# Configuration of CPCM2
```


C:\Users\Vladimir\Desktop\TheBook\Book\Chapter_6\CPCM2_Config.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
CPCM1_Config.txt
CPCM2_Config.txt
Normal text file
length : 7,335 lines : 201
Ln : 1 Col : 1 Pos : 1
Windows (CR LF)
UTF-8
INS

```
set ssl tls TLSv1.2 on
set ssl tls TLSv1.3 off
set interface eth0 comments "Mgmt"
set interface eth0 link-speed 1000M/full
set interface eth0 state on
set interface eth0 auto-negotiation on
set interface eth0 mtu 1500
set interface eth0 ipv4-address 10.0.0.2 mask-length 24
set interface eth1 comments "Internal1"
set interface eth1 link-speed 1000M/full
set interface eth1 state on
set interface eth1 auto-negotiation on
set interface eth1 mtu 1500
set interface eth1 ipv4-address 10.10.10.2 mask-length 24
set interface eth2 comments "Internal2"
set interface eth2 link-speed 1000M/full
set interface eth2 state on
set interface eth2 auto-negotiation on
set interface eth2 mtu 1500
set interface eth2 ipv4-address 10.20.20.2 mask-length 24
set interface eth3 comments "Sync"
set interface eth3 link-speed 1000M/full
set interface eth3 state on
set interface eth3 auto-negotiation on
set interface eth3 mtu 1500
set interface eth3 ipv4-address 192.168.255.1 mask-length 24
set interface eth4 comments "External"
set interface eth4 link-speed 1000M/full
set interface eth4 state on
set interface eth4 auto-negotiation on
set interface eth4 mtu 1500
set interface eth4 ipv4-address 200.100.0.2 mask-length 24
set interface eth5 comments "DMZ"
set interface eth5 link-speed 1000M/full
set interface eth5 state on
set interface eth5 auto-negotiation on
set interface eth5 mtu 1500
set interface eth5 ipv4-address 10.30.30.2 mask-length 24
```

```
set ssl tls TLSv1.2 on
set ssl tls TLSv1.3 off

set interface eth0 link-speed 1000M/full
set interface eth0 state on
set interface eth0 auto-negotiation on

set interface eth0 ipv4-address 10.0.0.3 mask-length 24
add interface eth0 alias 10.0.0.254/24





set interface eth1 state off
set interface eth2 state off

set interface eth3 state off





set interface eth4 state off








set interface eth5 state off
```



Deployment Agent build: 2101 | R80.40 take

Last updated on: Fri Oct 1 12:37

Package	Status	Release date
Hotfixes		1 item
R80.40 Jumbo Hotfix Accumulator General Availability (Take 120)	Available for Download	03-Aug-2021
Minor Versions (HFAs)		1 item
Check Point SmartConsole R80.40 Jumbo Hotfix B19	Installed, self-test passed	16-Mar-2020
Blink Packages - R81.00		1 item
[Latest] R81 Security Gateway + JHF T36 for Appliances and Open ...	Available for Download	15-Jul-2021
Major Versions		1 item
R81 Gaia Fresh Install and upgrade	Available for Download	26-Dec-2020

Package Details

File Name: Check_Point_SmartConsole_R80_40_jumbo_HF_B19_Win.tgz

Package Size: 472.4 MB

Package Type: Wrapper

Release Date: 16-Mar-2020

Downloaded On: 04-Apr-2020 16:37:28

Installed On: 04-Apr-2020 16:37:59

Status:

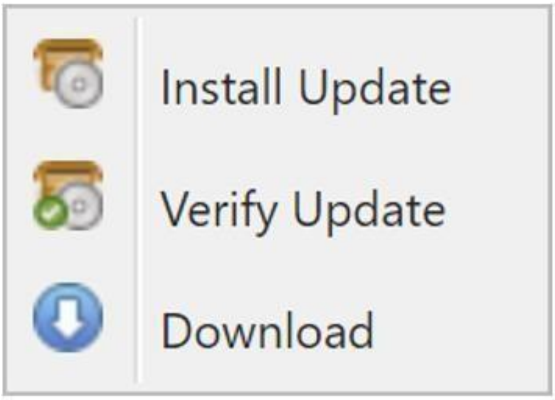
The package is installed, self-test passed

Important Messages:

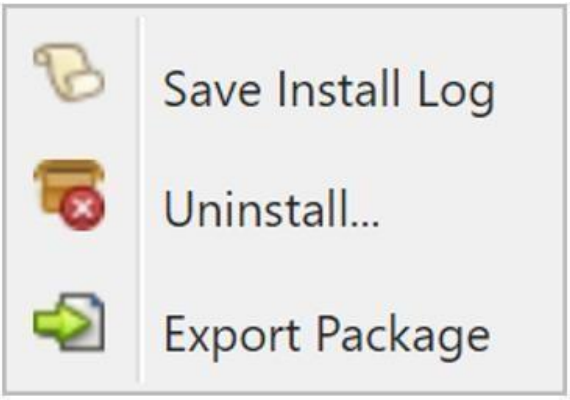
Description:
Notes:

Contained in: No other packages

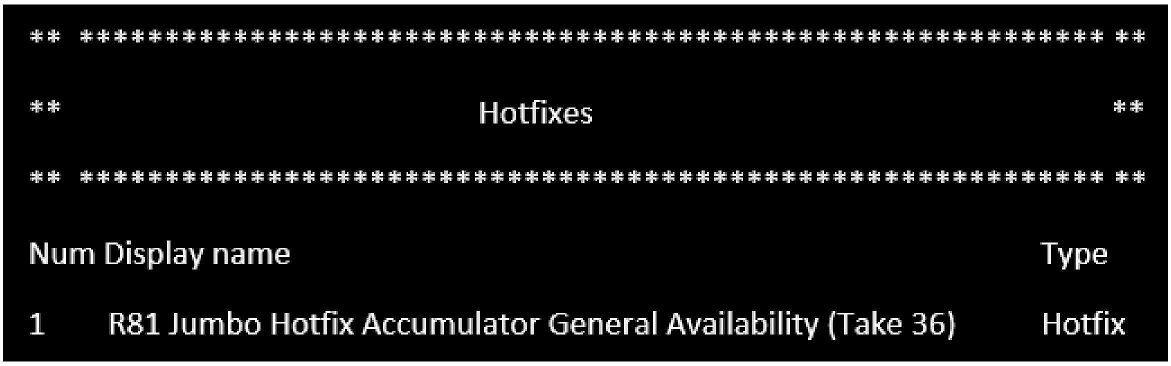
Contains the following packages: No other packages



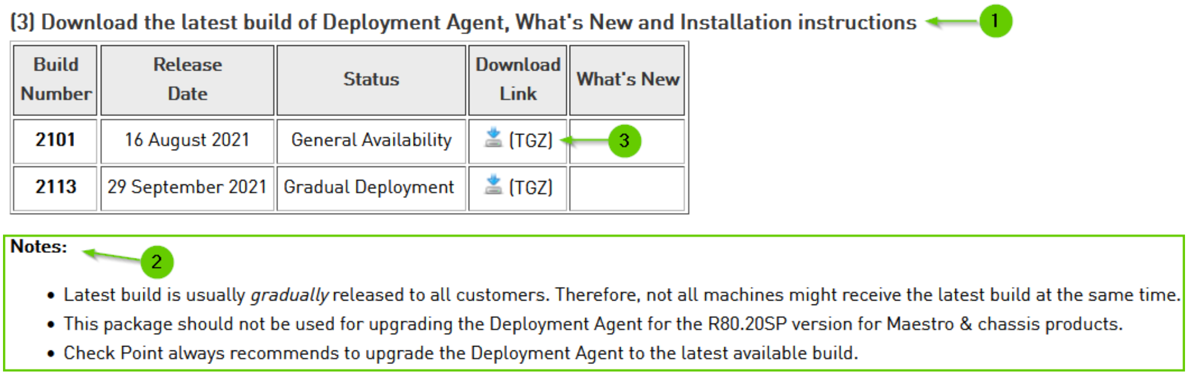
A



B



```
** ************************************************************** **
**                            Hotfixes                              **
** ************************************************************** **
Num Display name                                                Type
1    R81 Jumbo Hotfix Accumulator General Availability (Take 36)   Hotfix
```

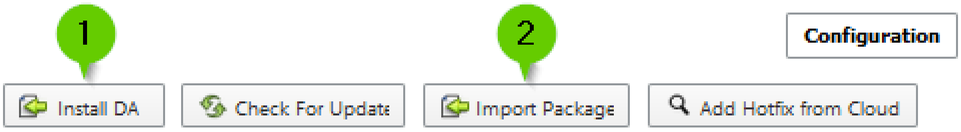


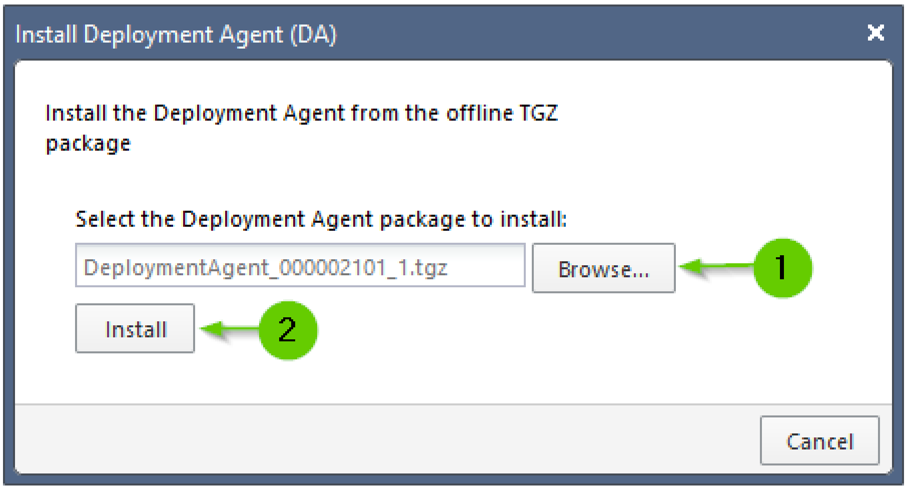
(3) Download the latest build of Deployment Agent, What's New and Installation instructions

Build Number	Release Date	Status	Download Link	What's New
2101	16 August 2021	General Availability	(TGZ)	
2113	29 September 2021	Gradual Deployment	(TGZ)	

Notes:

- Latest build is usually *gradually* released to all customers. Therefore, not all machines might receive the latest build at the same time.
- This package should not be used for upgrading the Deployment Agent for the R80.20SP version for Maestro & chassis products.
- Check Point always recommends to upgrade the Deployment Agent to the latest available build.



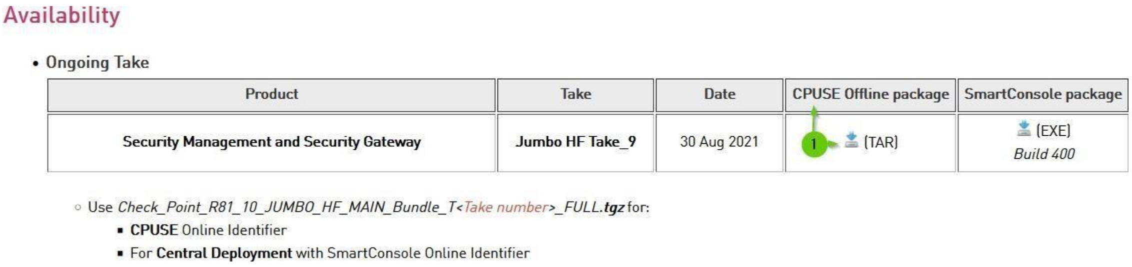


Install Deployment Agent (DA)

Install the Deployment Agent from the offline TGZ package

Select the Deployment Agent package to install:

DeploymentAgent_000002101_1.tgz

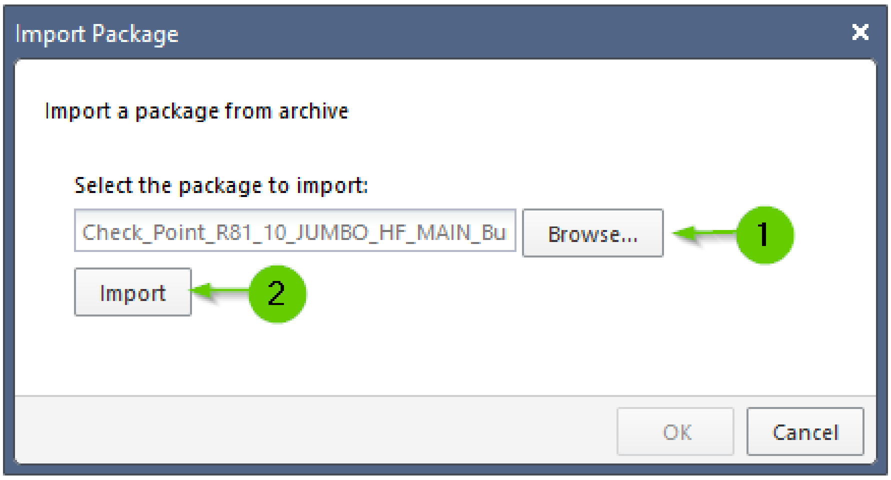


Availability

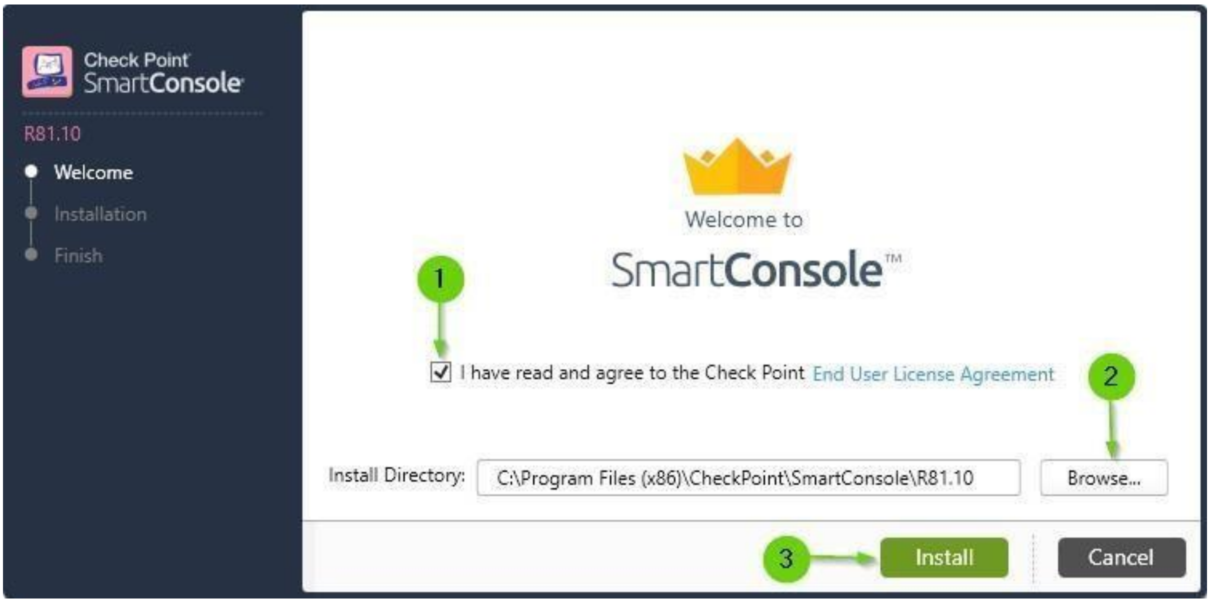
- Ongoing Take

Product	Take	Date	CPUSE Offline package	SmartConsole package
Security Management and Security Gateway	**Jumbo HF Take_9**	30 Aug 2021	(TAR)	(EXE) *Build 400*

- Use *Check_Point_R81_10_JUMBO_HF_MAIN_Bundle_T<Take number>_FULL.tgz* for:
  - **CPUSE** Online Identifier
  - For **Central Deployment** with SmartConsole Online Identifier

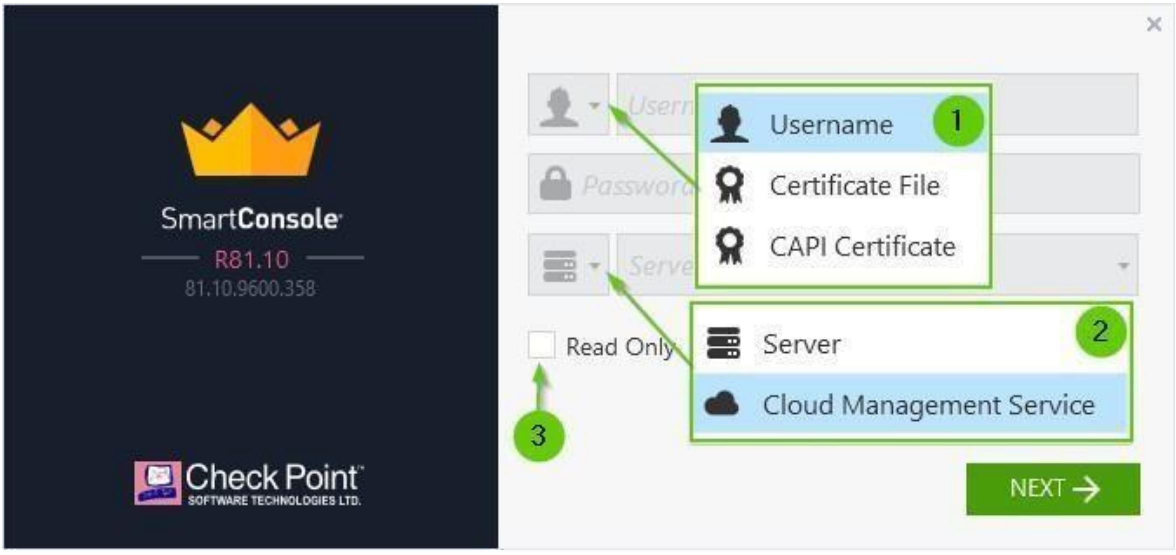
Import Package
×
Import a package from archive
Select the package to import:
Check_Point_R81_10_JUMBO_HF_MAIN_Bu
Browse...
1
Import
2
OK
Cancel

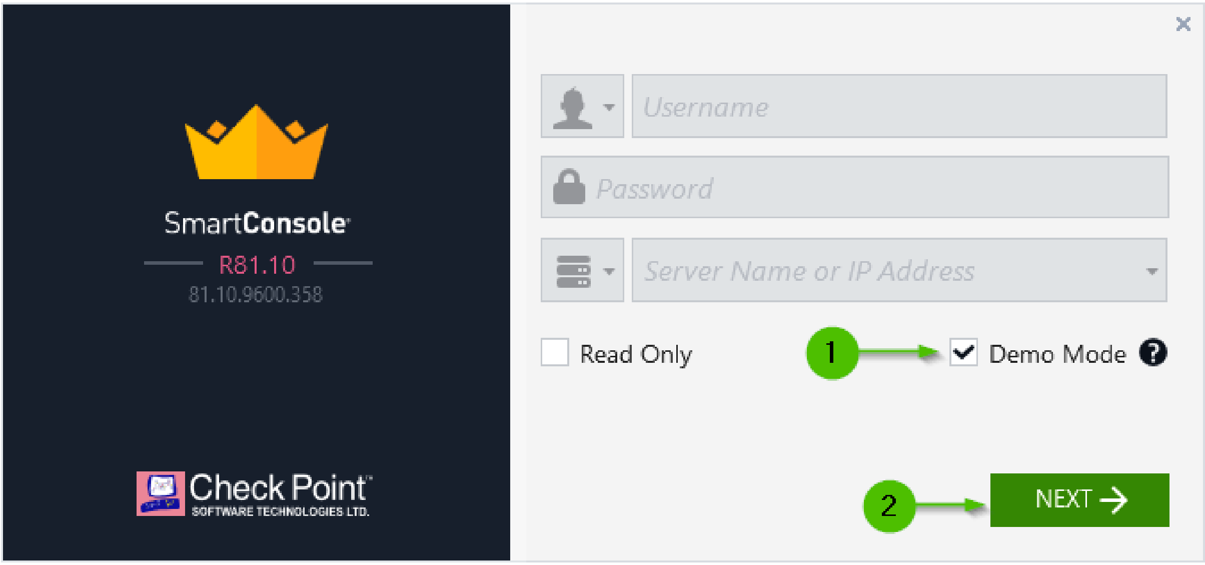
Chapter 7: SmartConsole – Familiarization and Navigation



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

Install Directory: C:\Program Files (x86)\CheckPoint\SmartConsole\R81.10





SmartConsole R81.10 81.10.9600.358

Check Point SOFTWARE TECHNOLOGIES LTD.

Username

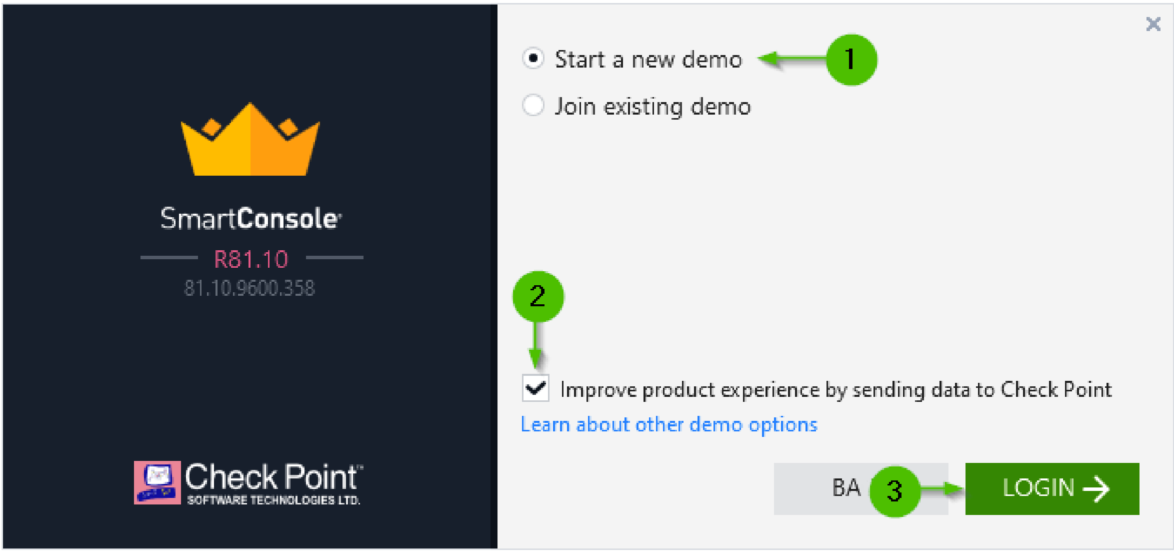
Password

Server Name or IP Address

□ Read Only

1 ☑ Demo Mode

2 NEXT →



SmartConsole R81.10 81.10.9600.358

Check Point SOFTWARE TECHNOLOGIES LTD.

● Start a new demo 1

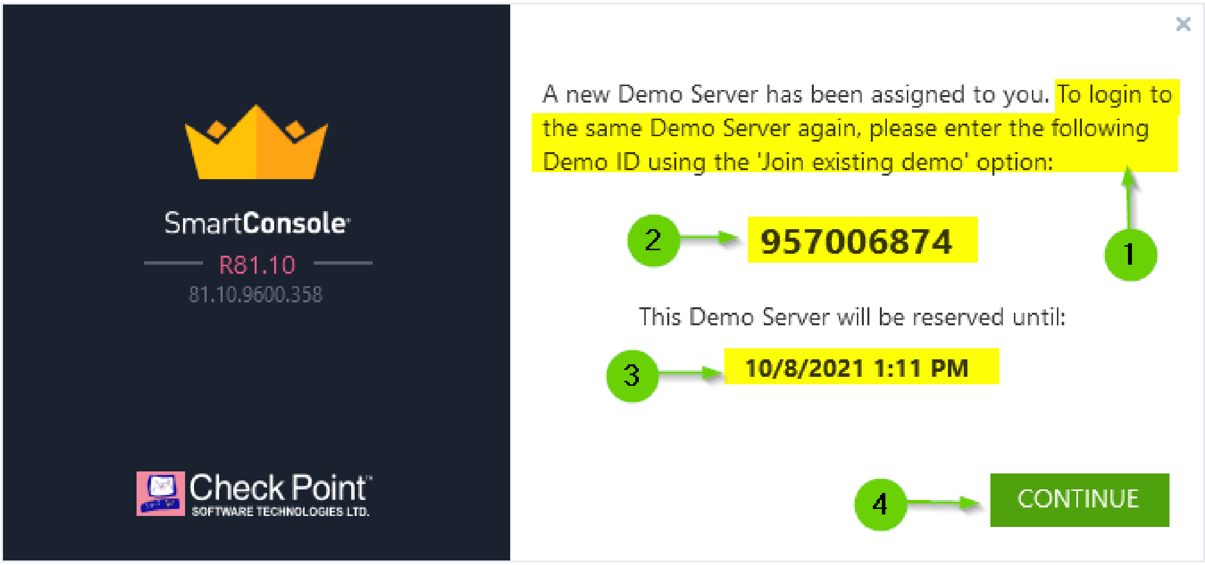
○ Join existing demo

2

☑ Improve product experience by sending data to Check Point

Learn about other demo options

BA 3 LOGIN →

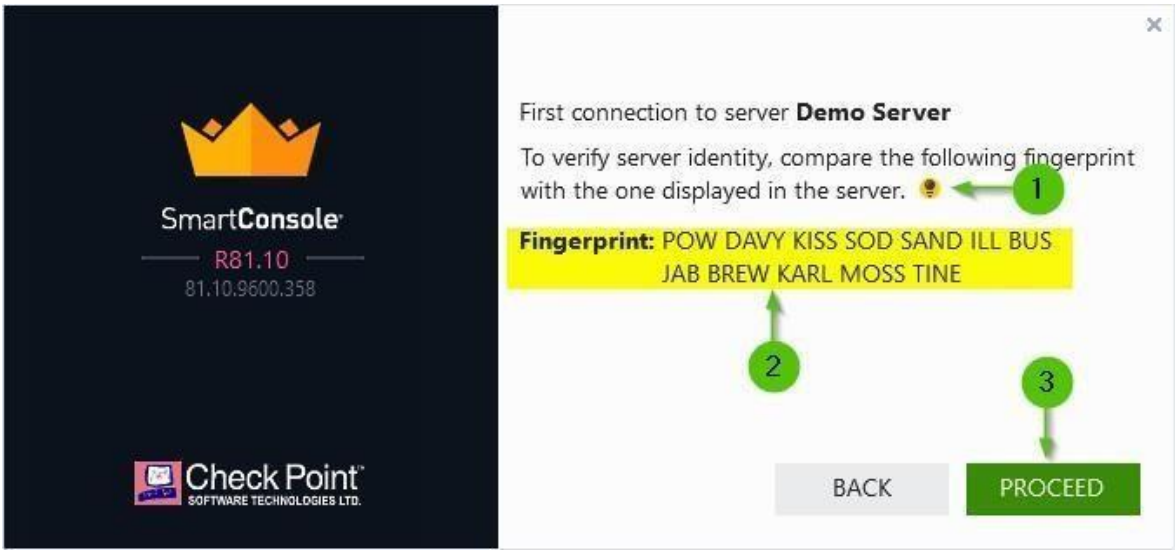


A new Demo Server has been assigned to you. To login to the same Demo Server again, please enter the following Demo ID using the 'Join existing demo' option:

957006874

This Demo Server will be reserved until:

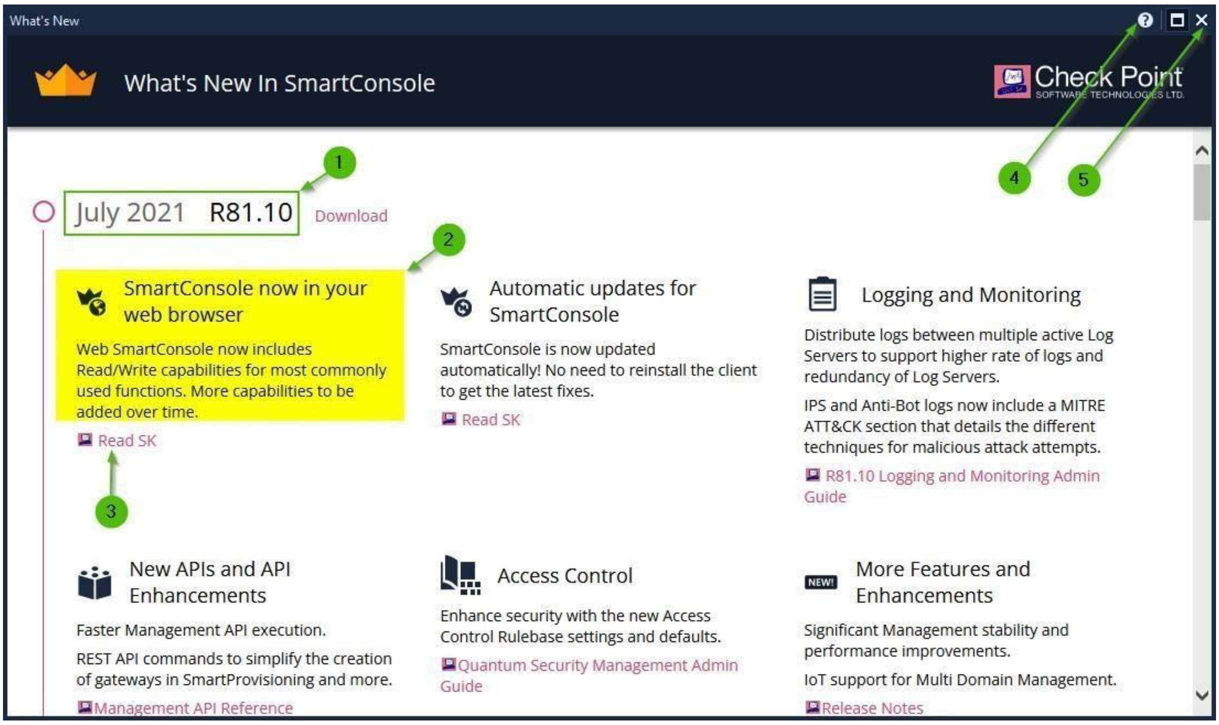
10/8/2021 1:11 PM



First connection to server **Demo Server**

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

Fingerprint: POW DAVY KISS SOD SAND ILL BUS JAB BREW KARL MOSS TINE



July 2021 R81.10 Download

SmartConsole now in your web browser

Web SmartConsole now includes Read/Write capabilities for most commonly used functions. More capabilities to be added over time.

Read SK

Automatic updates for SmartConsole

SmartConsole is now updated automatically! No need to reinstall the client to get the latest fixes.

Read SK

Logging and Monitoring

Distribute logs between multiple active Log Servers to support higher rate of logs and redundancy of Log Servers.

IPS and Anti-Bot logs now include a MITRE ATT&CK section that details the different techniques for malicious attack attempts.

R81.10 Logging and Monitoring Admin Guide

New APIs and API Enhancements

Faster Management API execution.

REST API commands to simplify the creation of gateways in SmartProvisioning and more.

Management API Reference

Access Control

Enhance security with the new Access Control Rulebase settings and defaults.

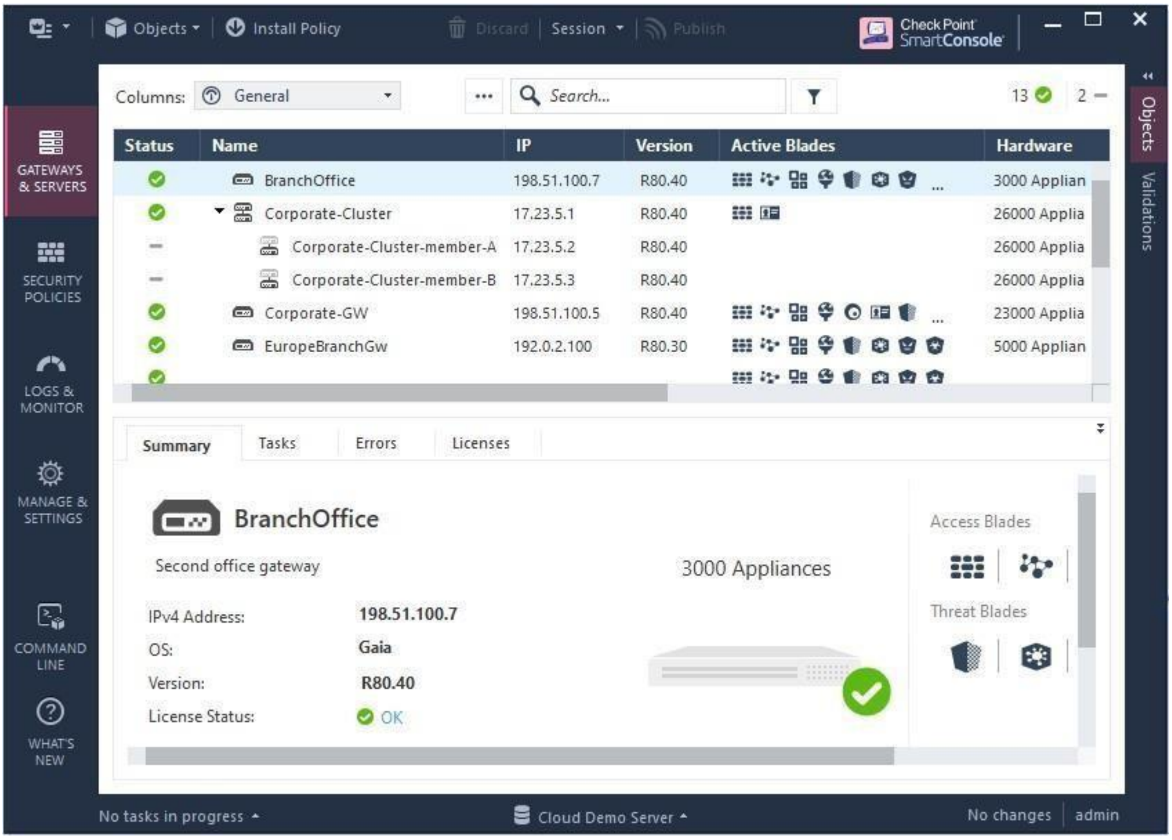
Quantum Security Management Admin Guide

More Features and Enhancements

Significant Management stability and performance improvements.

IoT support for Multi Domain Management.

Release Notes



Columns: General

Status	Name	IP	Version	Active Blades	Hardware
✓	BranchOffice	198.51.100.7	R80.40		3000 Applian
✓	Corporate-Cluster	17.23.5.1	R80.40		26000 Applia
–	Corporate-Cluster-member-A	17.23.5.2	R80.40		26000 Applia
–	Corporate-Cluster-member-B	17.23.5.3	R80.40		26000 Applia
✓	Corporate-GW	198.51.100.5	R80.40		23000 Applia
✓	EuropeBranchGw	192.0.2.100	R80.30		5000 Applian

Summary | Tasks | Errors | Licenses

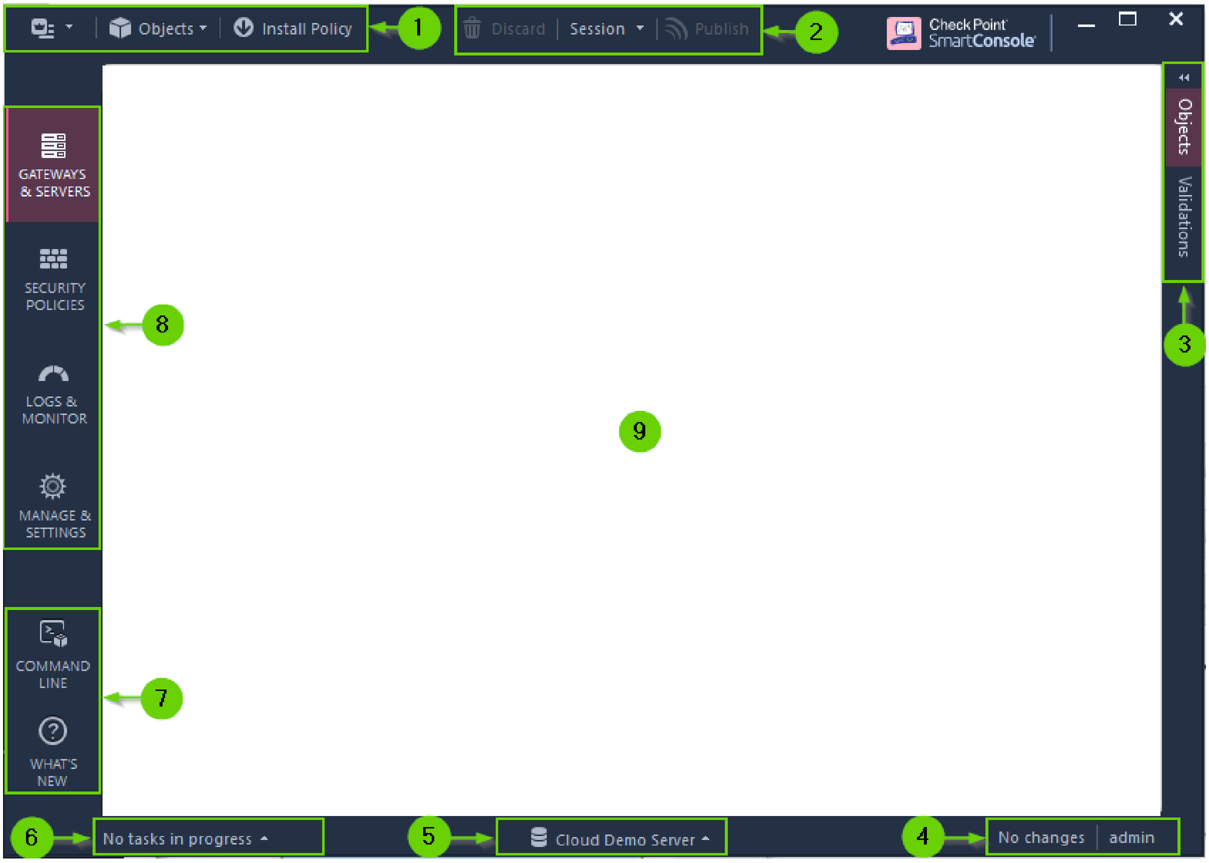
BranchOffice

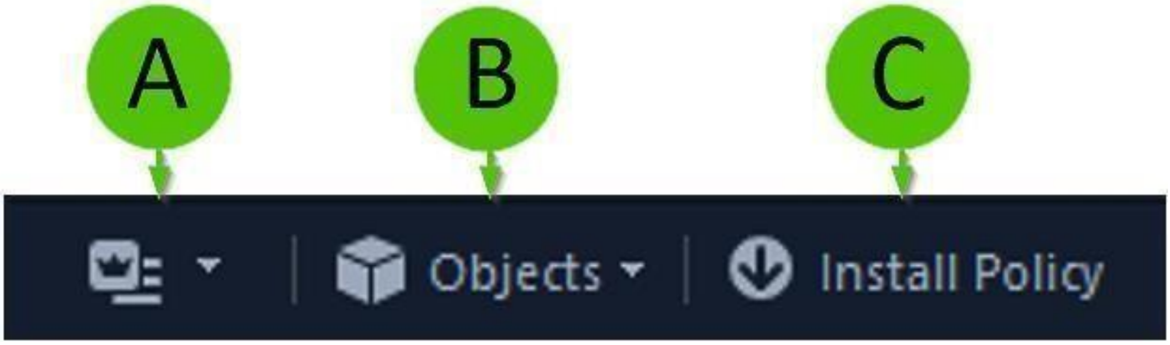
Second office gateway

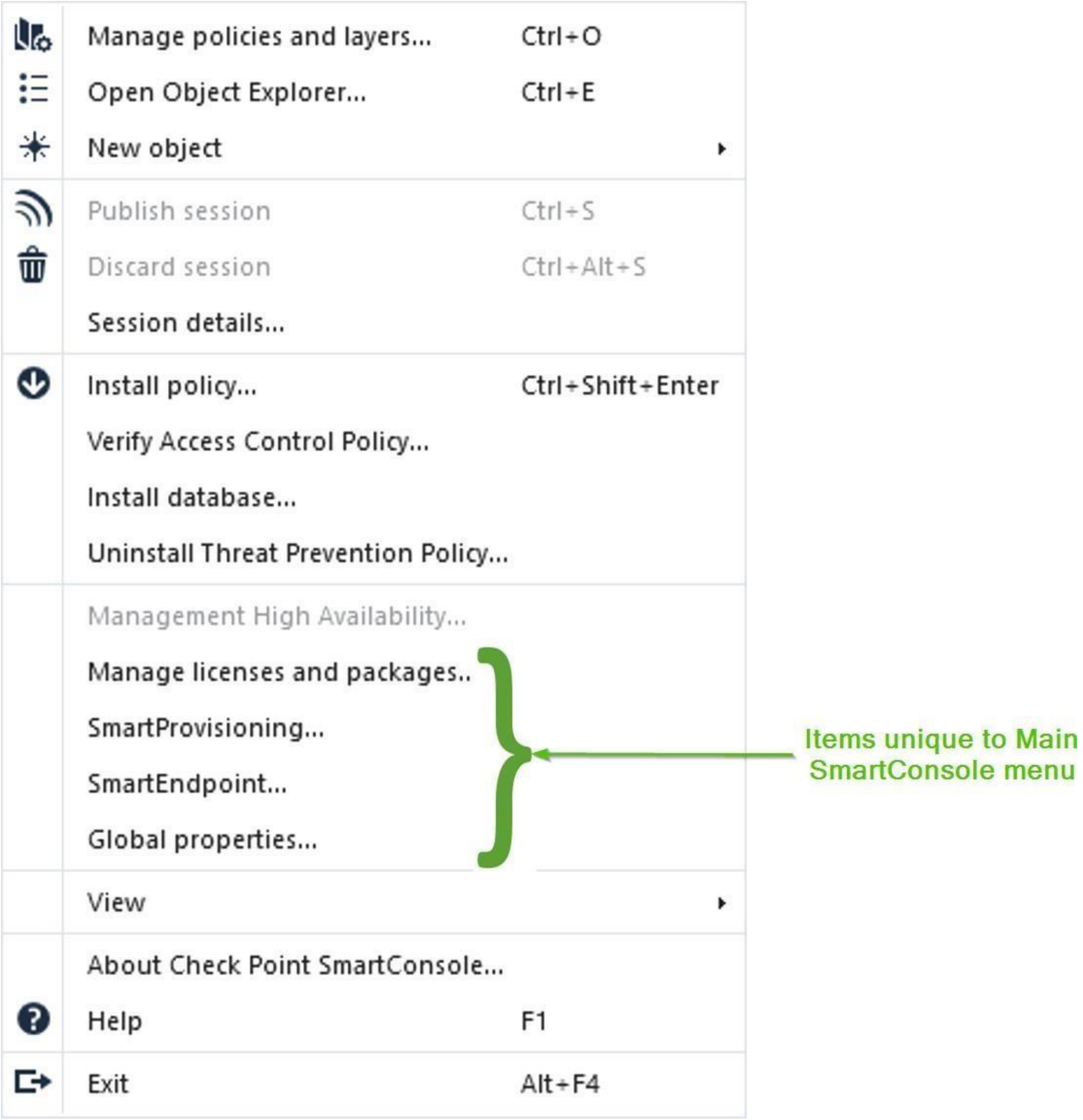
3000 Appliances

IPv4 Address:	198.51.100.7
OS:	Gaia
Version:	R80.40
License Status:	✓ OK

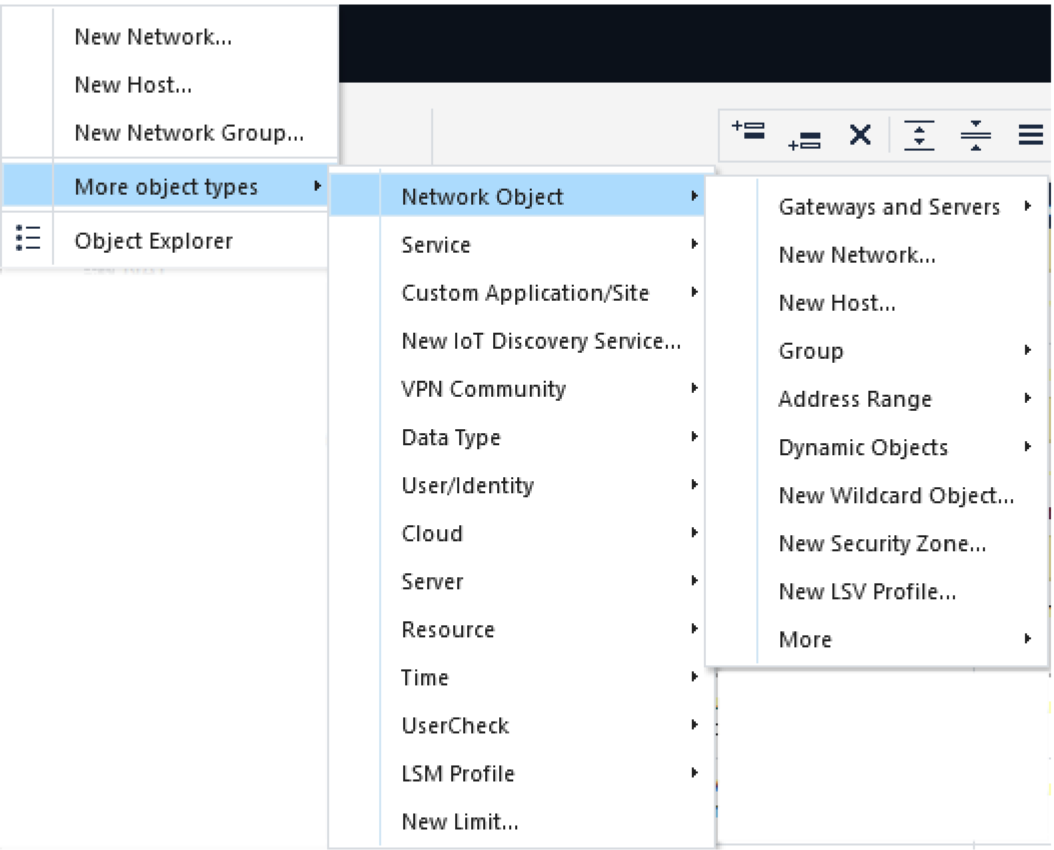
No tasks in progress | Cloud Demo Server | No changes | admin

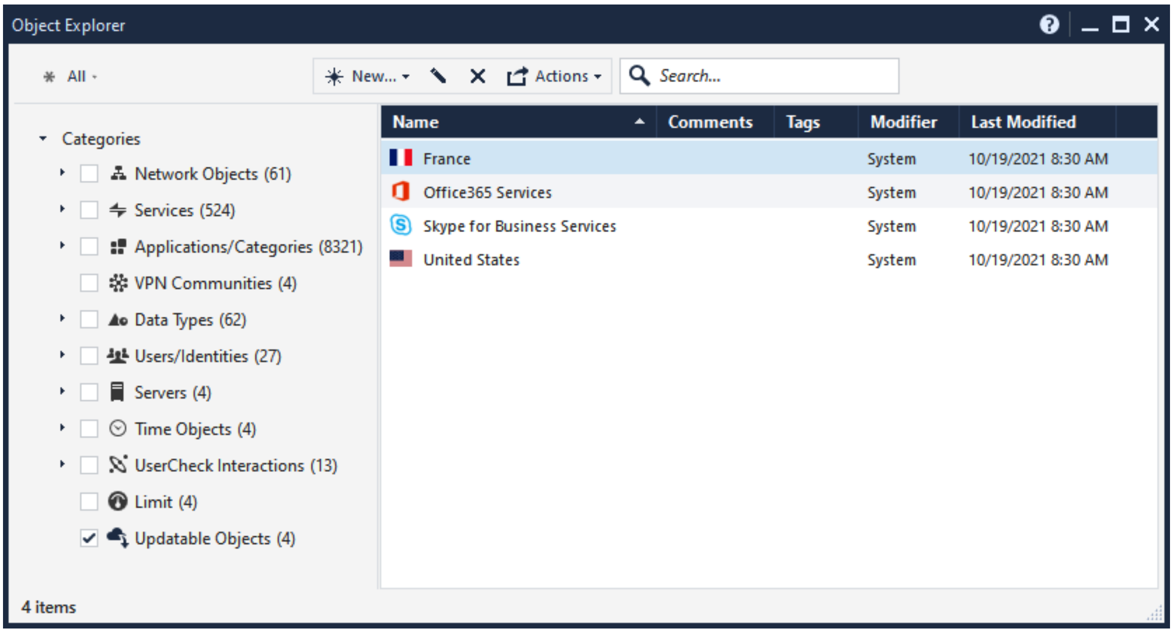

Objects
Install Policy
1
Discard
Session
Publish
2
Check Point SmartConsole
Objects
Validations
3
GATEWAYS & SERVERS
SECURITY POLICIES
8
LOGS & MONITOR
MANAGE & SETTINGS
9
COMMAND LINE
7
WHAT'S NEW
6
No tasks in progress
5
Cloud Demo Server
4
No changes
admin


A
B
C
Objects
Install Policy

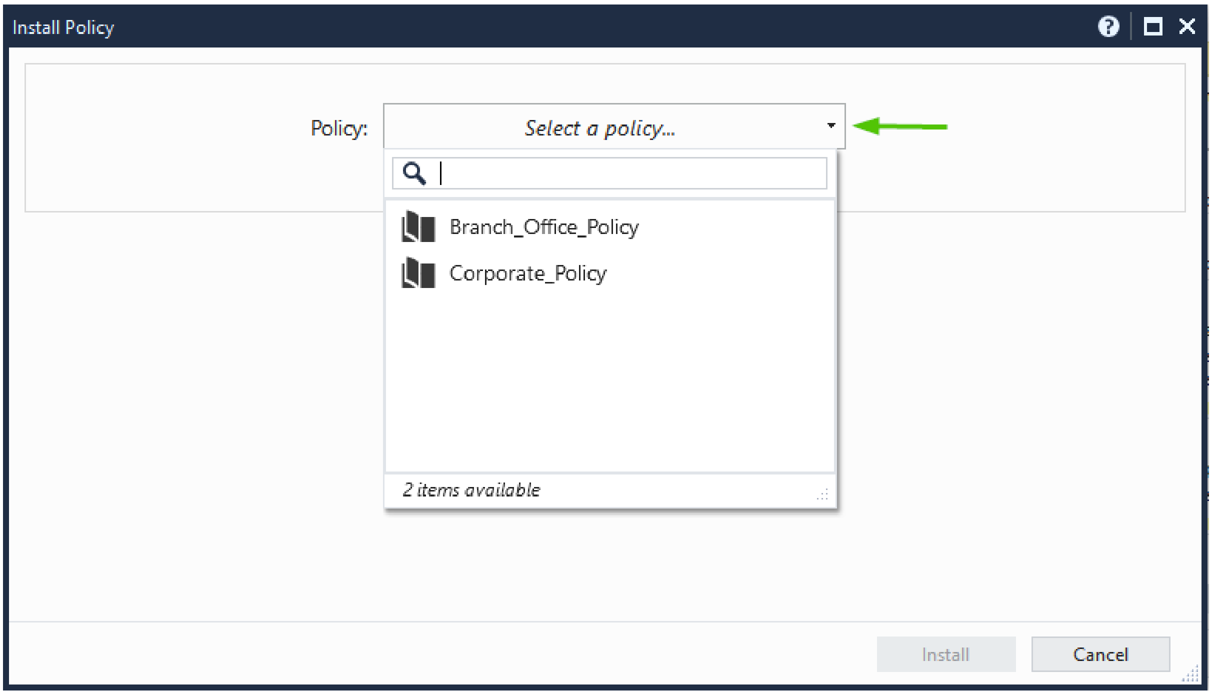

Manage policies and layers... Ctrl+O
Open Object Explorer... Ctrl+E
New object
Publish session Ctrl+S
Discard session Ctrl+Alt+S
Session details...
Install policy... Ctrl+Shift+Enter
Verify Access Control Policy...
Install database...
Uninstall Threat Prevention Policy...
Management High Availability...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

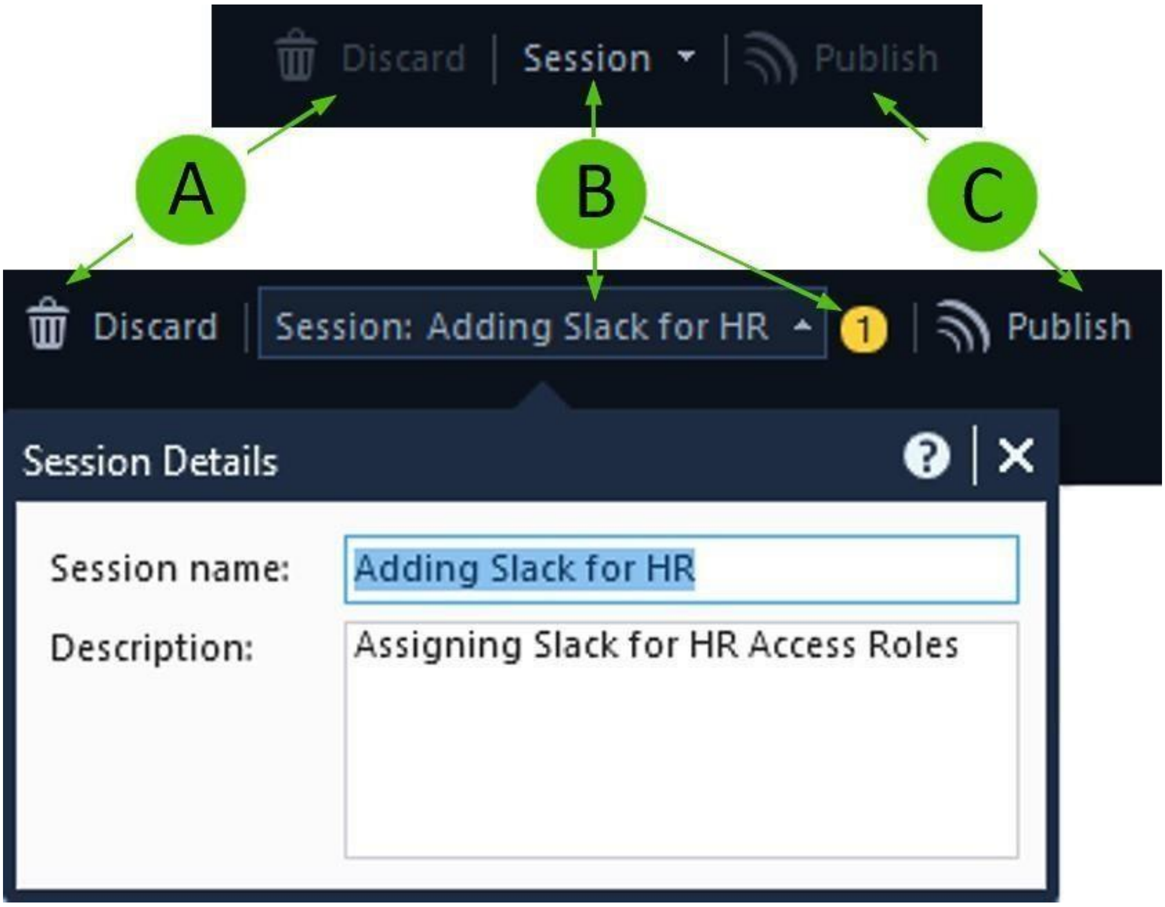
Items unique to Main SmartConsole menu





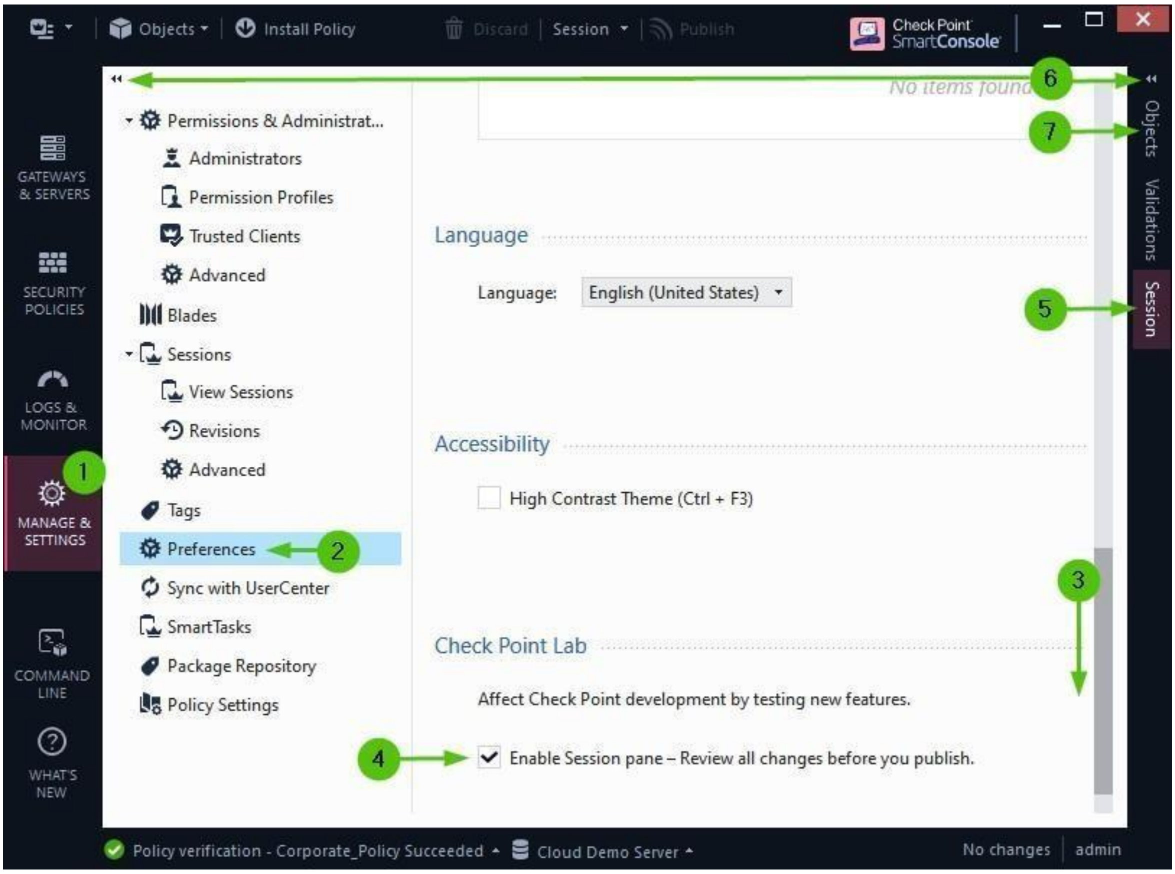
Name	Comments	Tags	Modifier	Last Modified
France			System	10/19/2021 8:30 AM
Office365 Services			System	10/19/2021 8:30 AM
Skype for Business Services			System	10/19/2021 8:30 AM
United States			System	10/19/2021 8:30 AM





Session name: Adding Slack for HR

Description: Assigning Slack for HR Access Roles



Language

Language: English (United States)

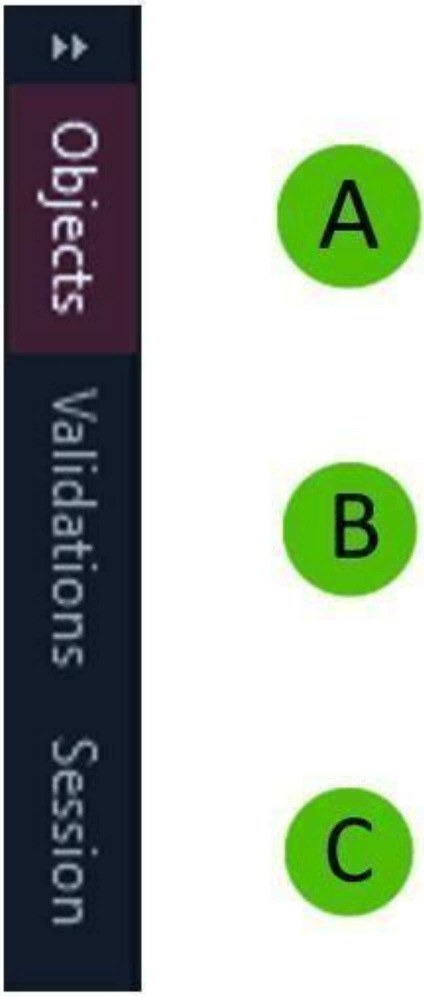
Accessibility

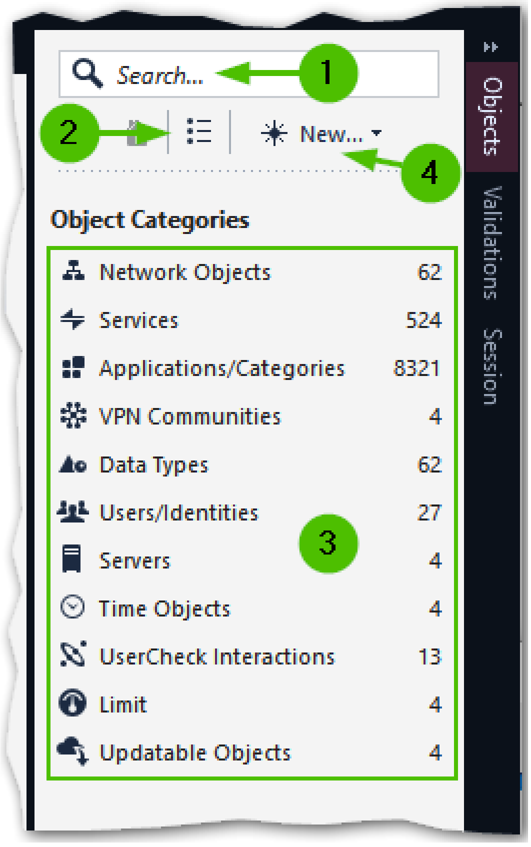
□ High Contrast Theme (Ctrl + F3)

Check Point Lab

Affect Check Point development by testing new features.

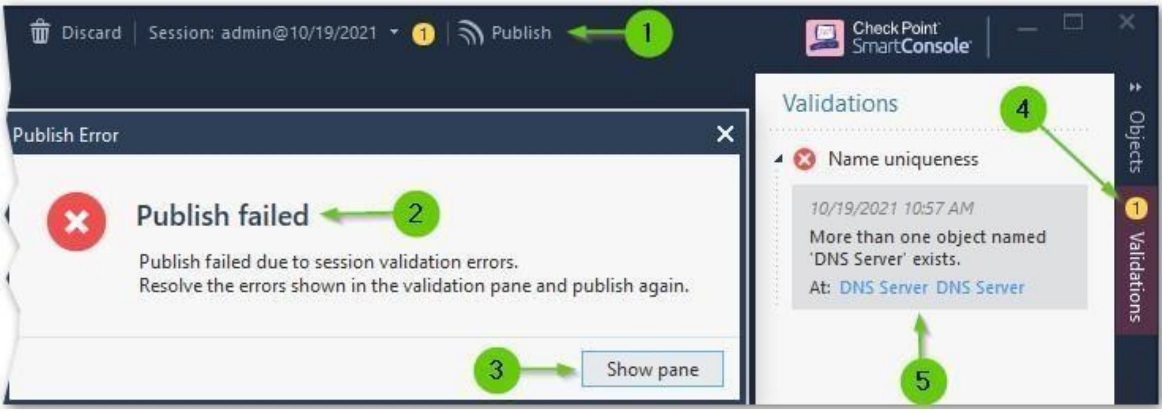
☑ Enable Session pane – Review all changes before you publish.


Objects
Validations
Session
A
B
C



Object Categories

Network Objects	62
Services	524
Applications/Categories	8321
VPN Communities	4
Data Types	62
Users/Identities	27
Servers	4
Time Objects	4
UserCheck Interactions	13
Limit	4
Updatable Objects	4



Publish Error

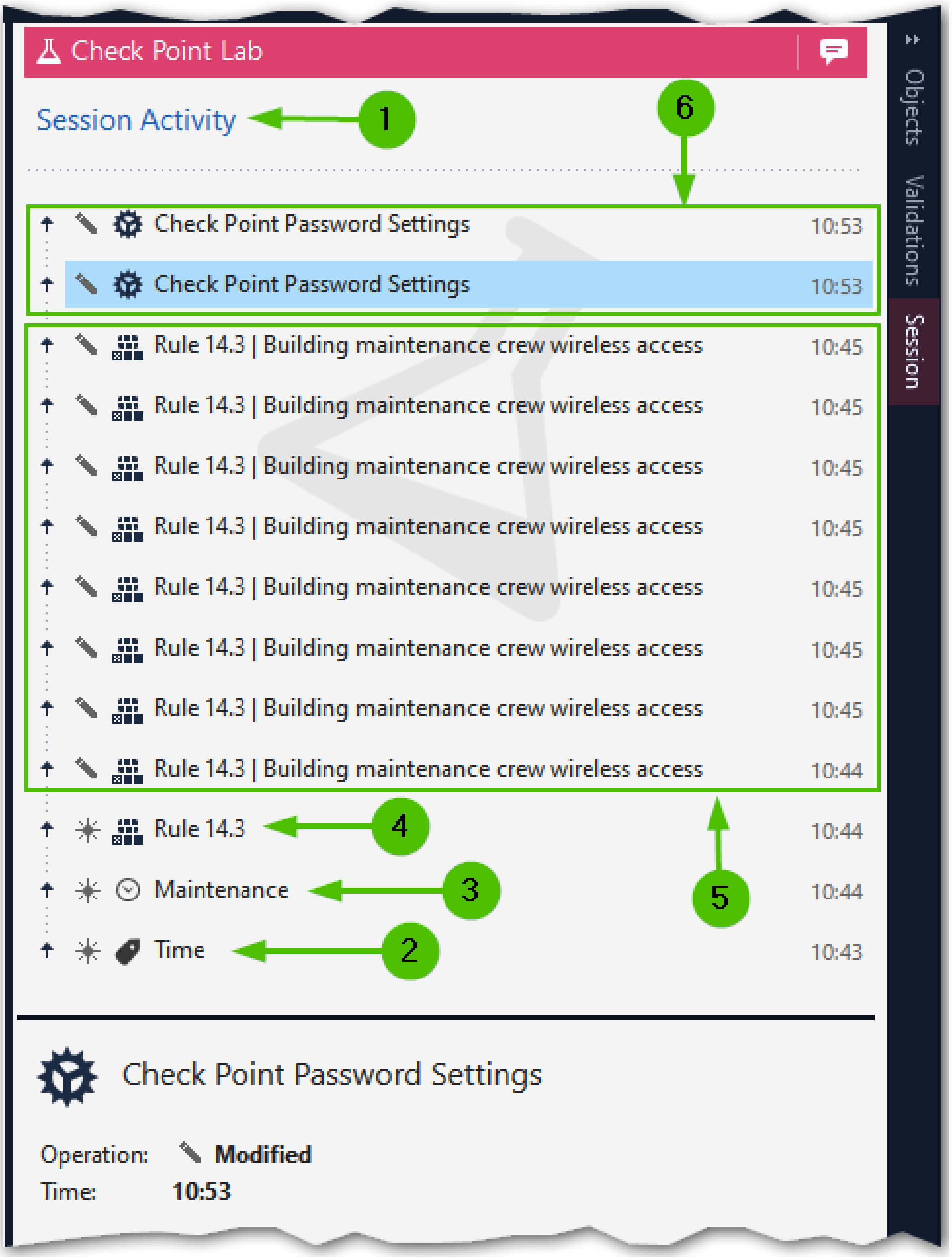
Publish failed

Publish failed due to session validation errors.
Resolve the errors shown in the validation pane and publish again.

Validations

Name uniqueness

10/19/2021 10:57 AM
More than one object named 'DNS Server' exists.
At: DNS Server DNS Server



Check Point Lab

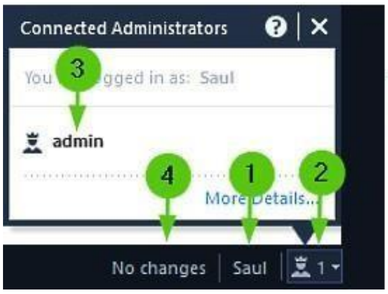
Session Activity

✎	Check Point Password Settings	10:53
✎	Check Point Password Settings	10:53
✎	Rule 14.3 | Building maintenance crew wireless access	10:45
✎	Rule 14.3 | Building maintenance crew wireless access	10:45
✎	Rule 14.3 | Building maintenance crew wireless access	10:45
✎	Rule 14.3 | Building maintenance crew wireless access	10:45
✎	Rule 14.3 | Building maintenance crew wireless access	10:45
✎	Rule 14.3 | Building maintenance crew wireless access	10:45
✎	Rule 14.3 | Building maintenance crew wireless access	10:45
✎	Rule 14.3 | Building maintenance crew wireless access	10:44
✳	Rule 14.3	10:44
✳	Maintenance	10:44
✳	Time	10:43

Check Point Password Settings

Operation: ✎ **Modified**

Time: **10:53**



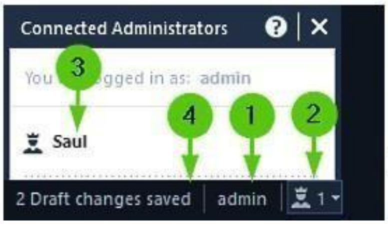
Connected Administrators

You are logged in as: Saul

admin

More Details...

No changes | Saul | 1

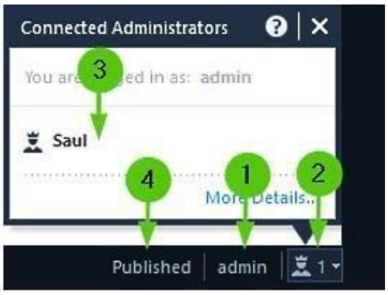


Connected Administrators

You are logged in as: admin

Saul

2 Draft changes saved | admin | 1



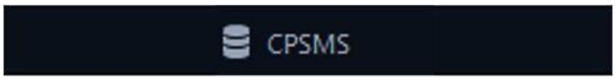
Connected Administrators

You are logged in as: admin

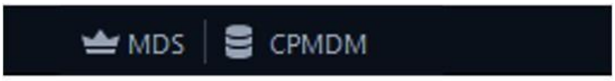
Saul

More Details...

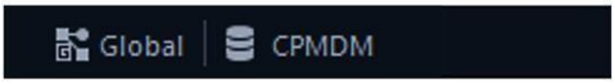
Published | admin | 1



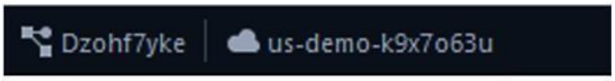
Single or High-Availability Management Server



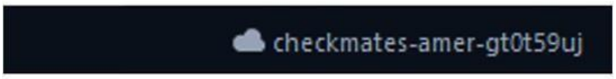
Multi-Domain Management Server (root)



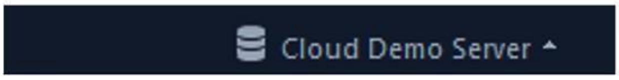
Multi-Domain Management Server Global Settings



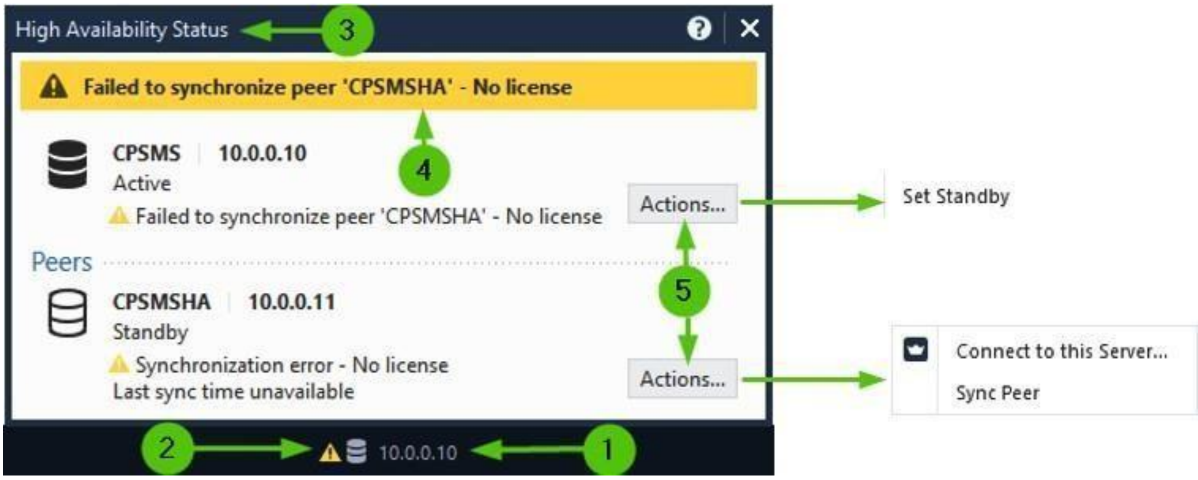
Cloud Management Service Demo Tenant



Cloud Management Service Tenant



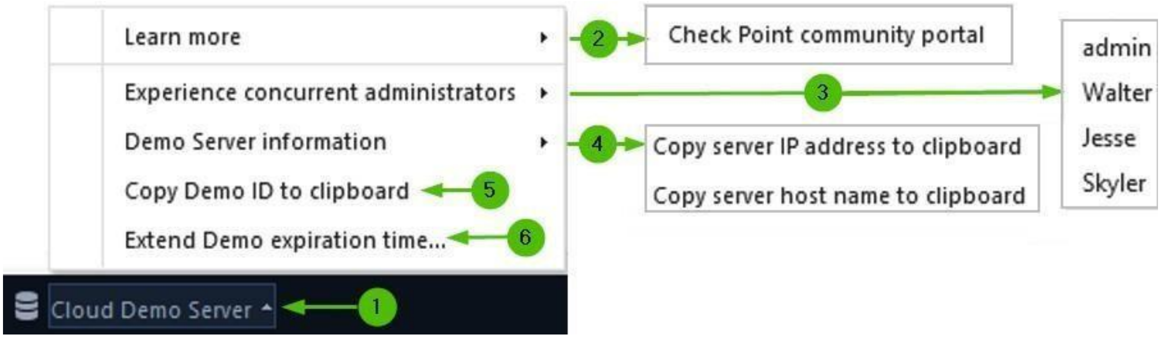
Cloud Demo Server

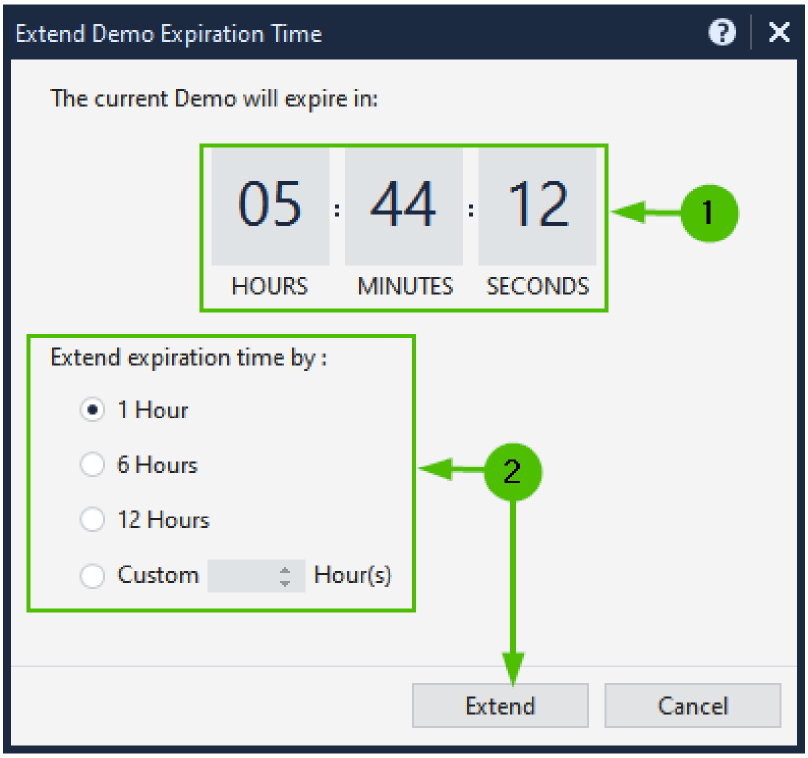


Failed to synchronize peer 'CPSMSHA' - No license

CPSMS | 10.0.0.10
Active
Failed to synchronize peer 'CPSMSHA' - No license

CPSMSHA | 10.0.0.11
Standby
Synchronization error - No license
Last sync time unavailable


Learn more
Experience concurrent administrators
Demo Server information
Copy Demo ID to clipboard
Extend Demo expiration time...
Cloud Demo Server
1
2
3
4
5
6
Check Point community portal
admin
Walter
Jesse
Skyler
Copy server IP address to clipboard
Copy server host name to clipboard



Extend Demo Expiration Time

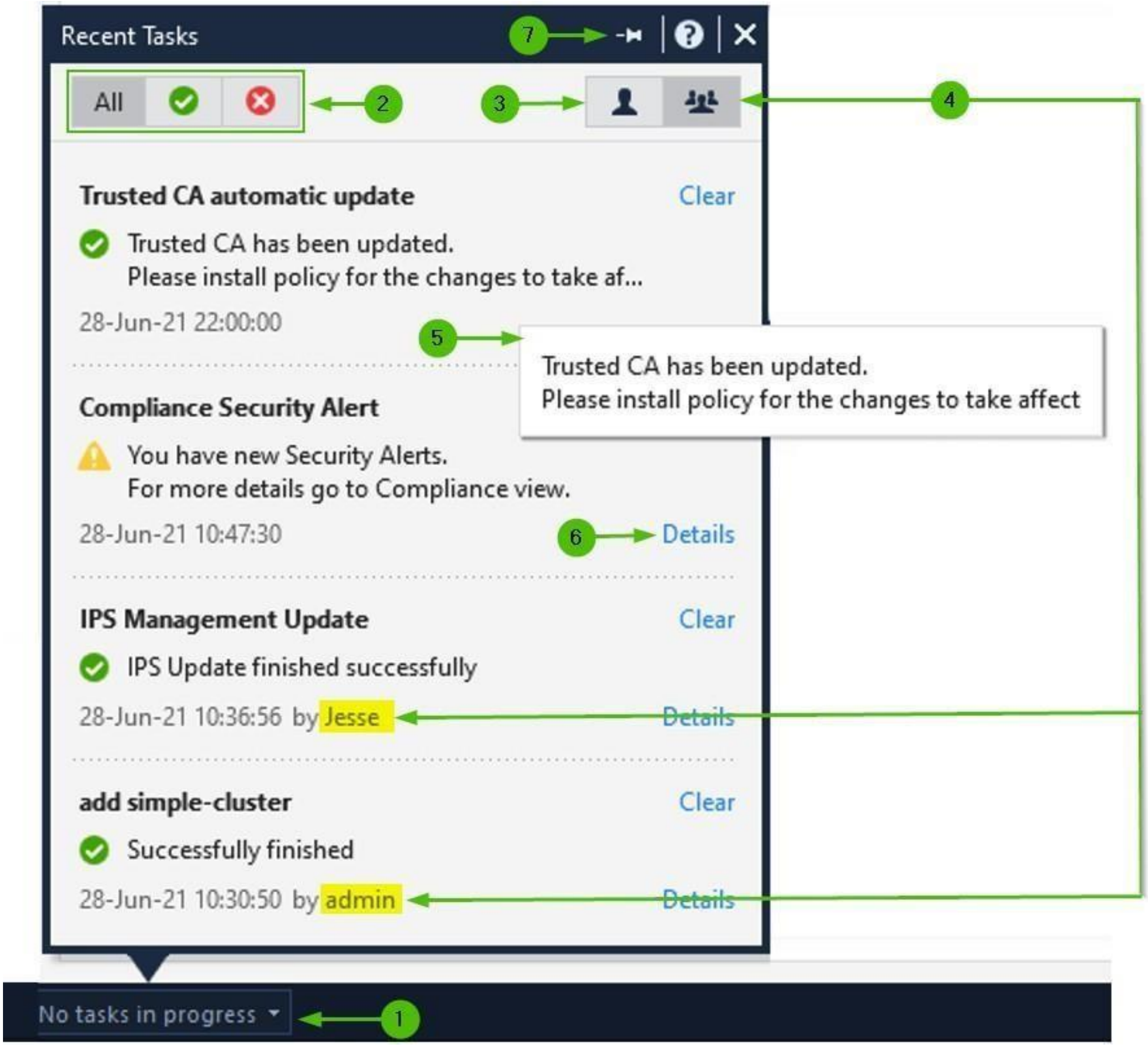
The current Demo will expire in:

05 : 44 : 12

HOURS MINUTES SECONDS

Extend expiration time by :

- ● 1 Hour
- ○ 6 Hours
- ○ 12 Hours
- ○ Custom Hour(s)



Trusted CA automatic update

✓ Trusted CA has been updated.
Please install policy for the changes to take af...

28-Jun-21 22:00:00

Trusted CA has been updated.
Please install policy for the changes to take affect

Compliance Security Alert

You have new Security Alerts.
For more details go to Compliance view.

28-Jun-21 10:47:30

IPS Management Update

✓ IPS Update finished successfully

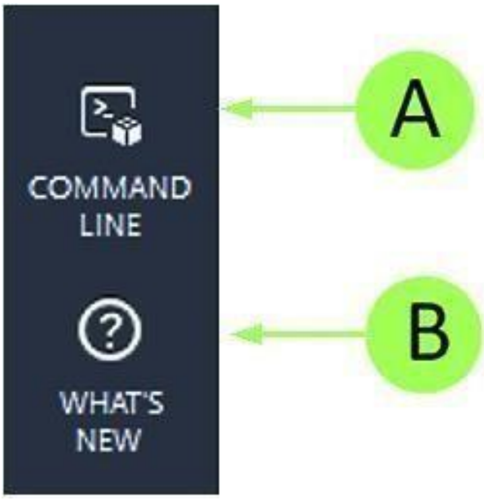
28-Jun-21 10:36:56 by Jesse

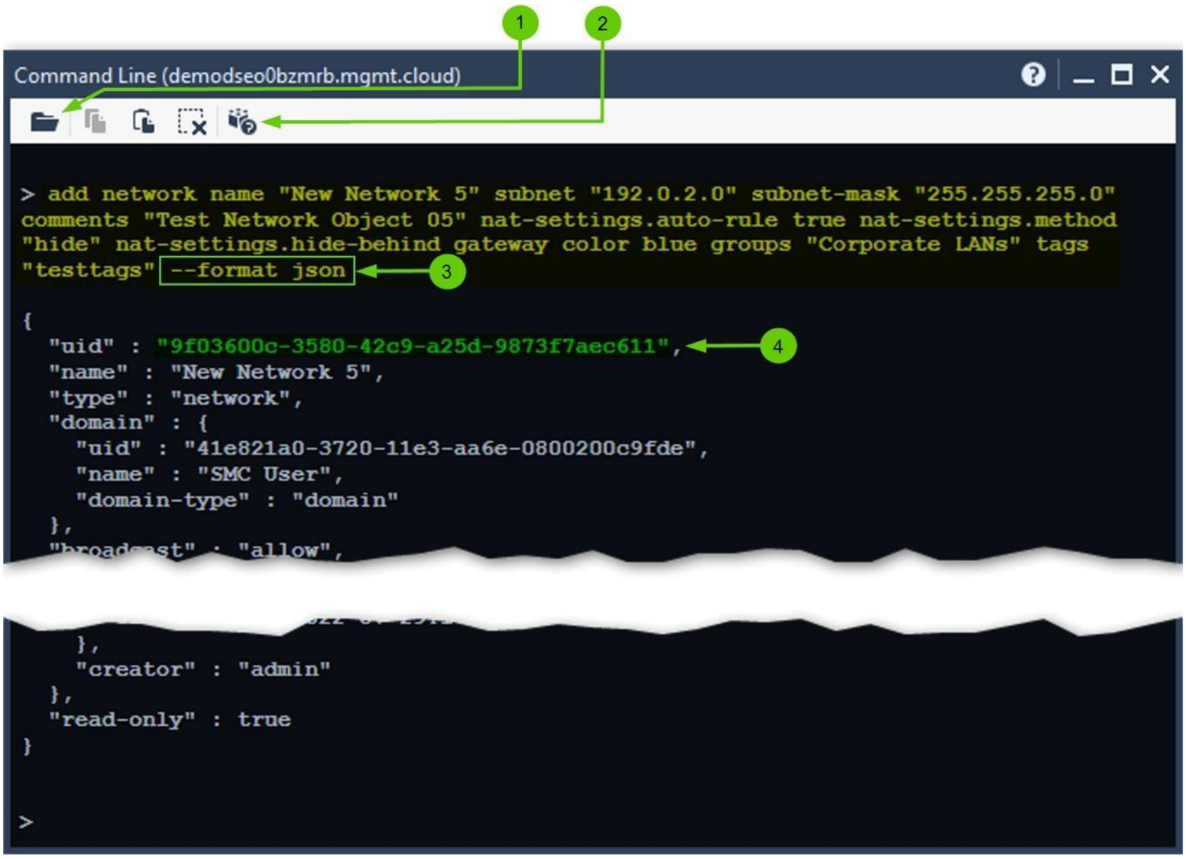
add simple-cluster

✓ Successfully finished

28-Jun-21 10:30:50 by admin

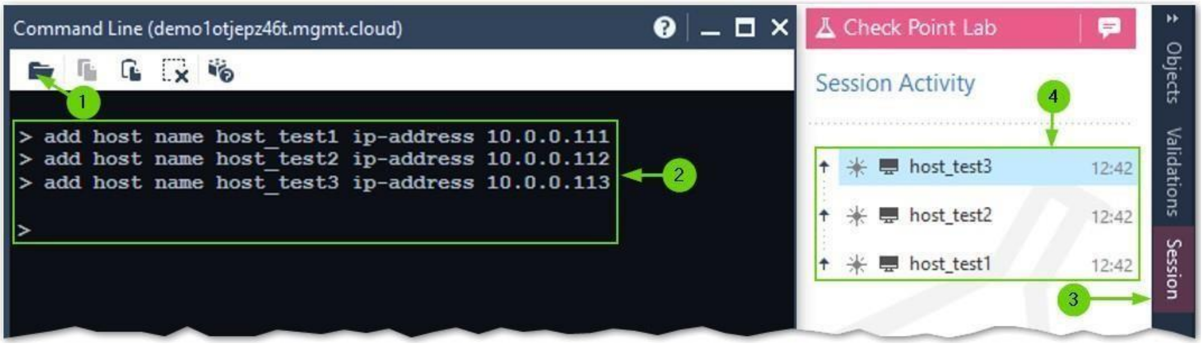
No tasks in progress



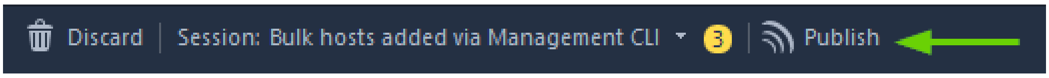


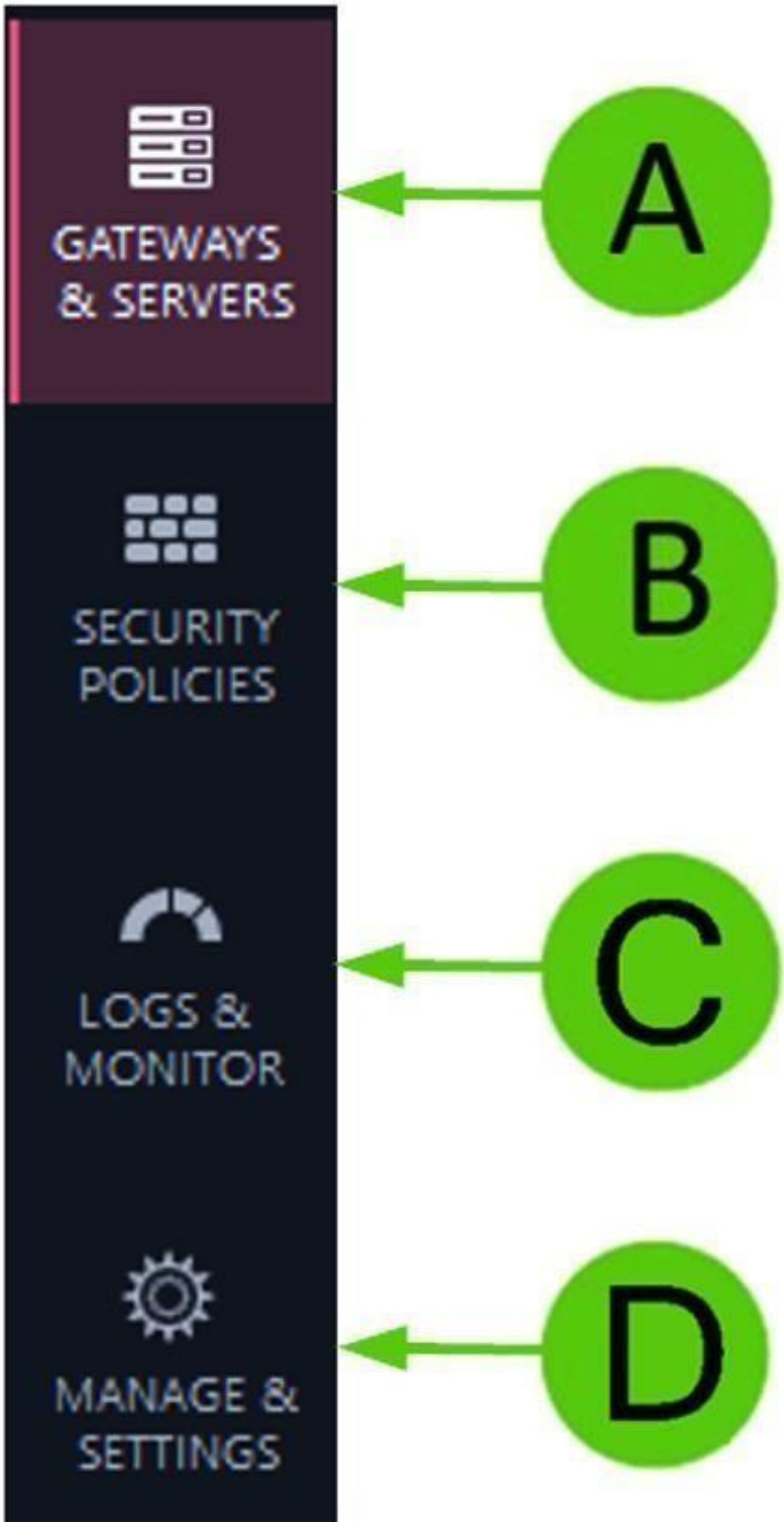
```
> add network name "New Network 5" subnet "192.0.2.0" subnet-mask "255.255.255.0"
comments "Test Network Object 05" nat-settings.auto-rule true nat-settings.method
"hide" nat-settings.hide-behind gateway color blue groups "Corporate LANs" tags
"testtags" --format json

{
  "uid" : "9f03600c-3580-42c9-a25d-9873f7aec611",
  "name" : "New Network 5",
  "type" : "network",
  "domain" : {
    "uid" : "41e821a0-3720-11e3-aa6e-0800200c9fde",
    "name" : "SMC User",
    "domain-type" : "domain"
  },
  "broadcast" : "allow",
```

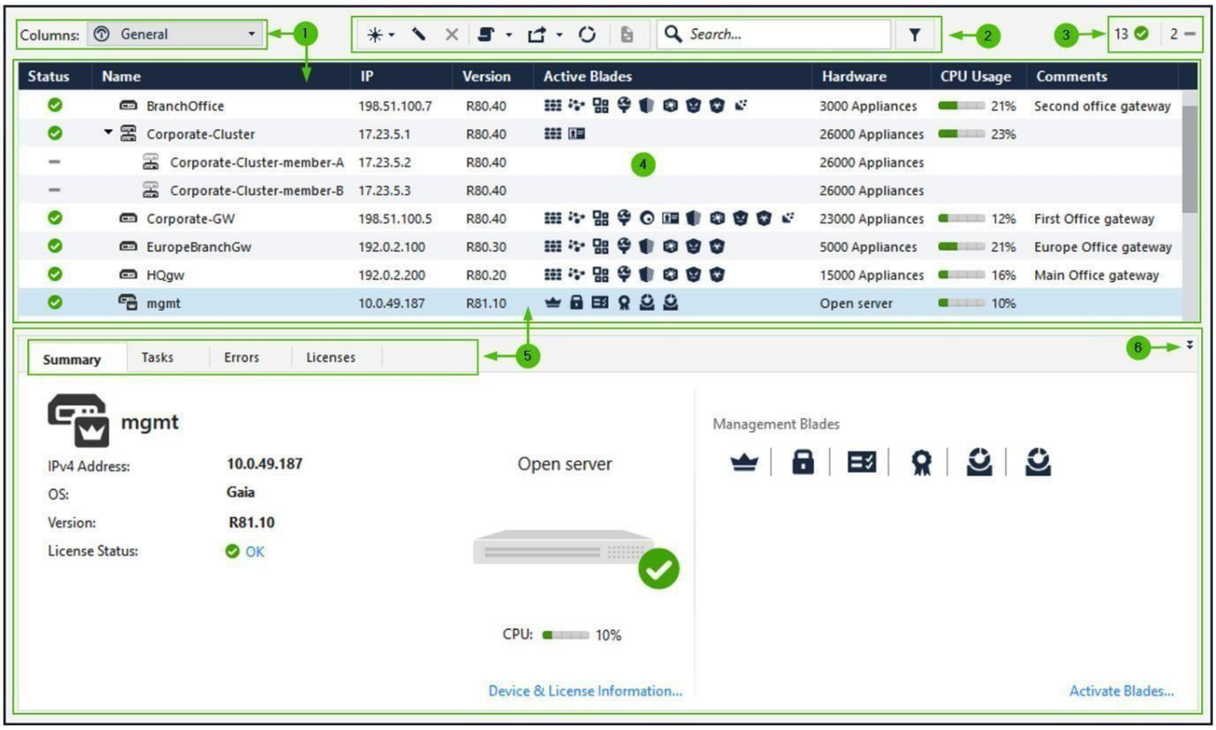
```
    },
    "creator" : "admin"
  },
  "read-only" : true
}


>
```



```
> add host name host_test1 ip-address 10.0.0.111
> add host name host_test2 ip-address 10.0.0.112
> add host name host_test3 ip-address 10.0.0.113

>
```




GATEWAYS & SERVERS
A
SECURITY POLICIES
B
LOGS & MONITOR
C
MANAGE & SETTINGS
D



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Comments
✓	BranchOffice	198.51.100.7	R80.40		3000 Appliances	21%	Second office gateway
✓	Corporate-Cluster	17.23.5.1	R80.40		26000 Appliances	23%	
—	Corporate-Cluster-member-A	17.23.5.2	R80.40		26000 Appliances		
—	Corporate-Cluster-member-B	17.23.5.3	R80.40		26000 Appliances		
✓	Corporate-GW	198.51.100.5	R80.40		23000 Appliances	12%	First Office gateway
✓	EuropeBranchGw	192.0.2.100	R80.30		5000 Appliances	21%	Europe Office gateway
✓	HQgw	192.0.2.200	R80.20		15000 Appliances	16%	Main Office gateway
✓	mgmt	10.0.49.187	R81.10		Open server	10%	

mgmt

IPv4 Address:	10.0.49.187
OS:	Gaia
Version:	R81.10
License Status:	✓ OK

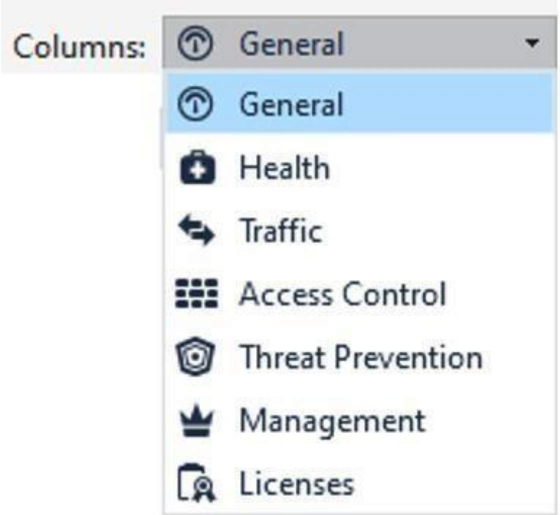
Open server

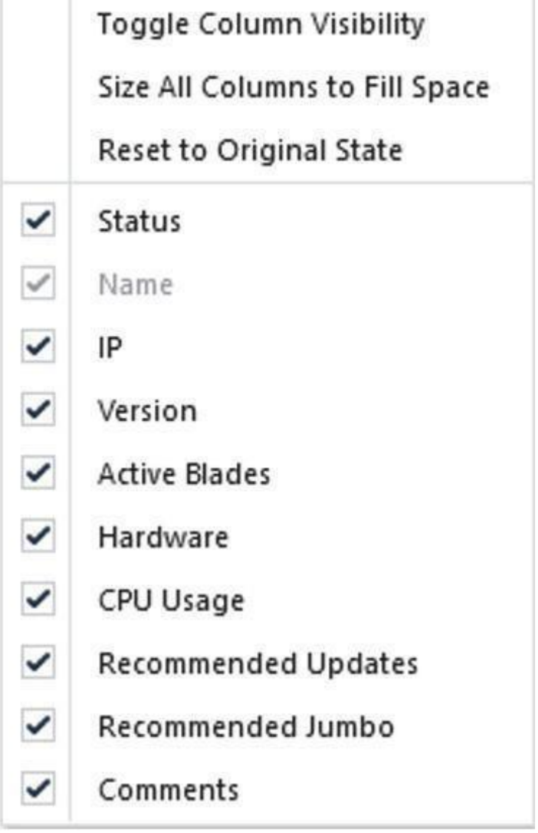
CPU: 10%

Device & License Information...

Management Blades

Activate Blades...

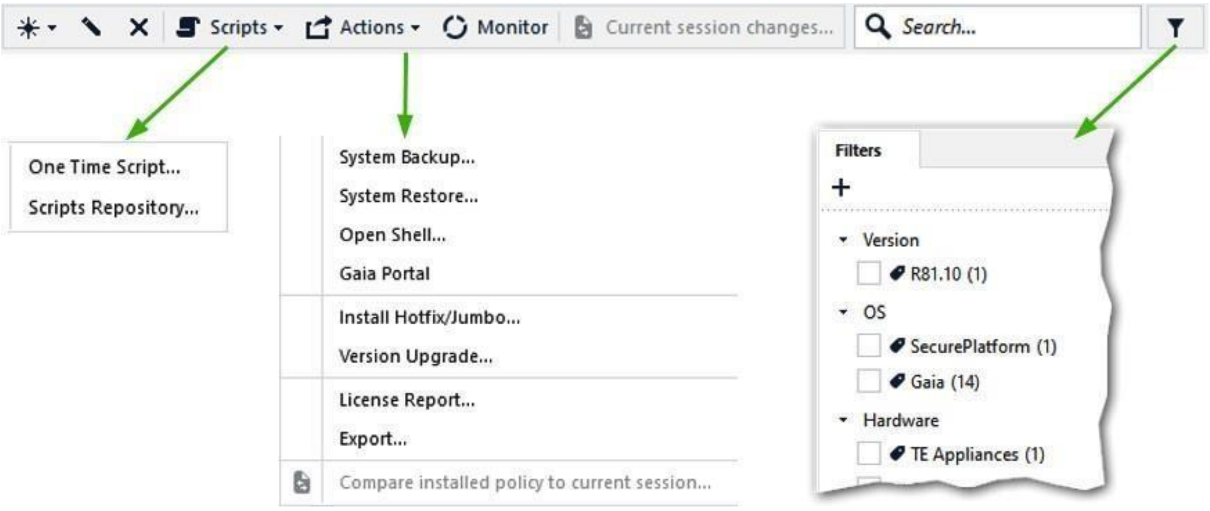


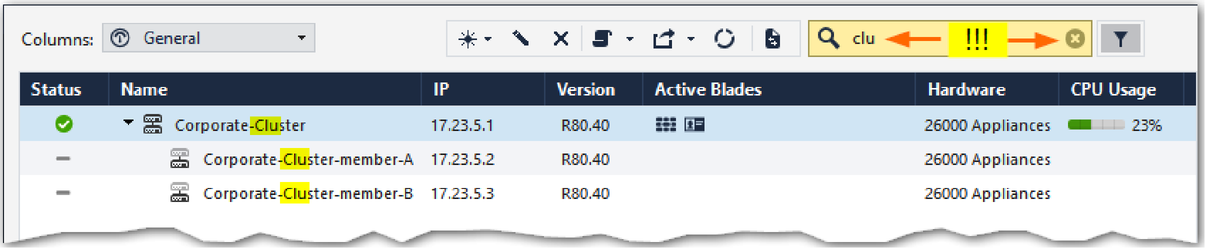

Toggle Column Visibility

Size All Columns to Fill Space

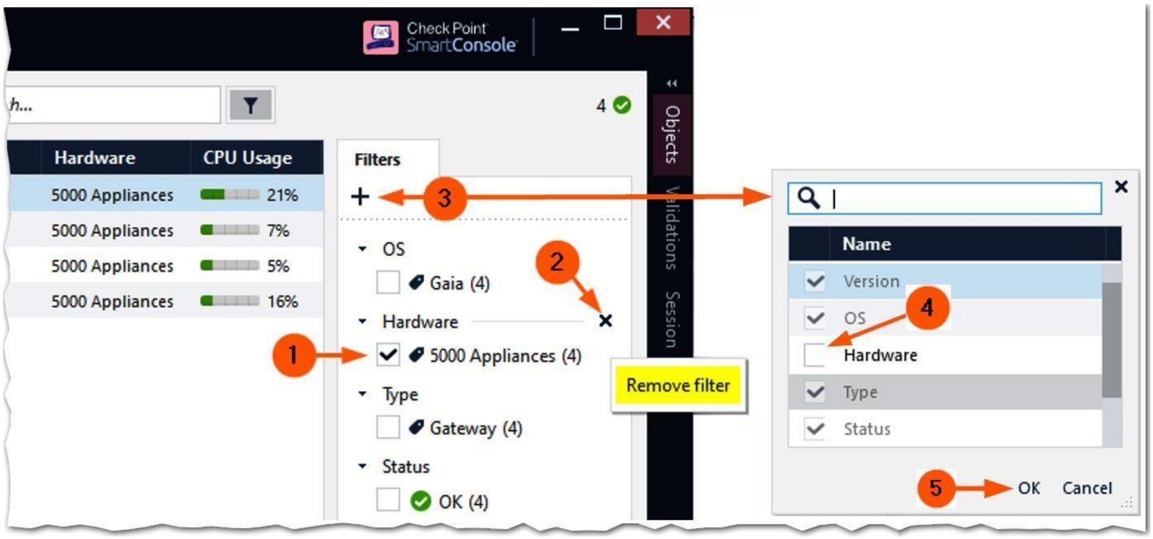
Reset to Original State

- ☑ Status
- ☑ Name
- ☑ IP
- ☑ Version
- ☑ Active Blades
- ☑ Hardware
- ☑ CPU Usage
- ☑ Recommended Updates
- ☑ Recommended Jumbo
- ☑ Comments

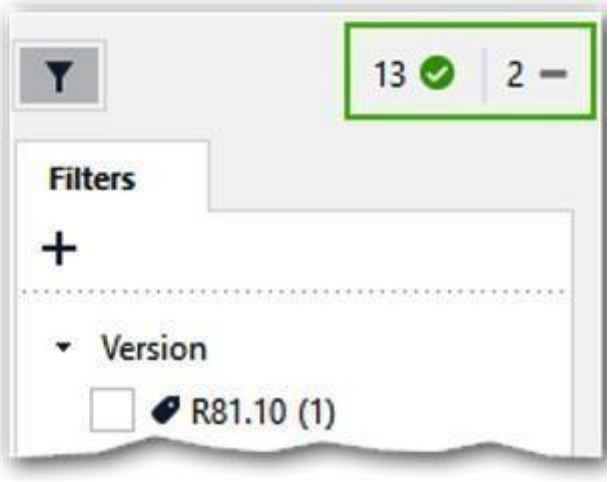


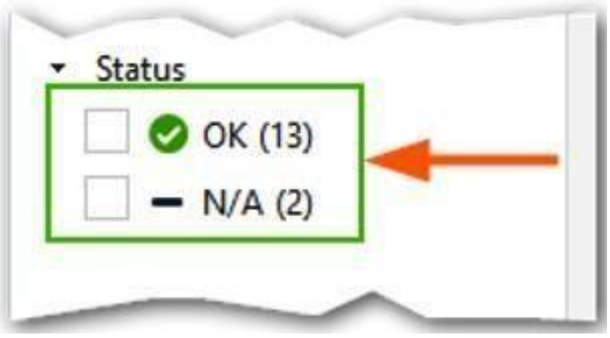


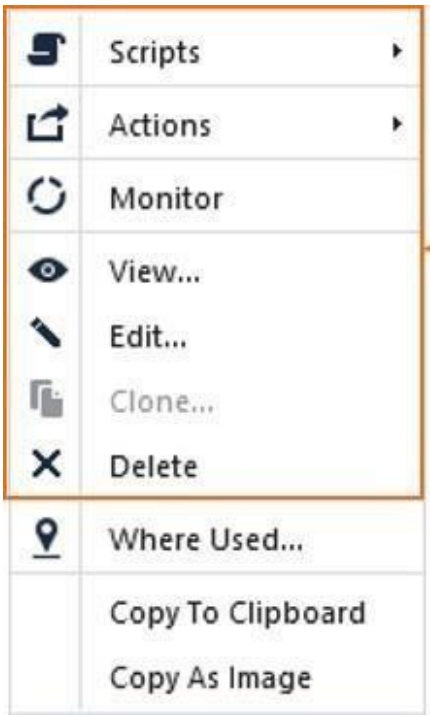
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage
✓	Corporate-Cluster	17.23.5.1	R80.40		26000 Appliances	23%
—	Corporate-Cluster-member-A	17.23.5.2	R80.40		26000 Appliances	
—	Corporate-Cluster-member-B	17.23.5.3	R80.40		26000 Appliances	



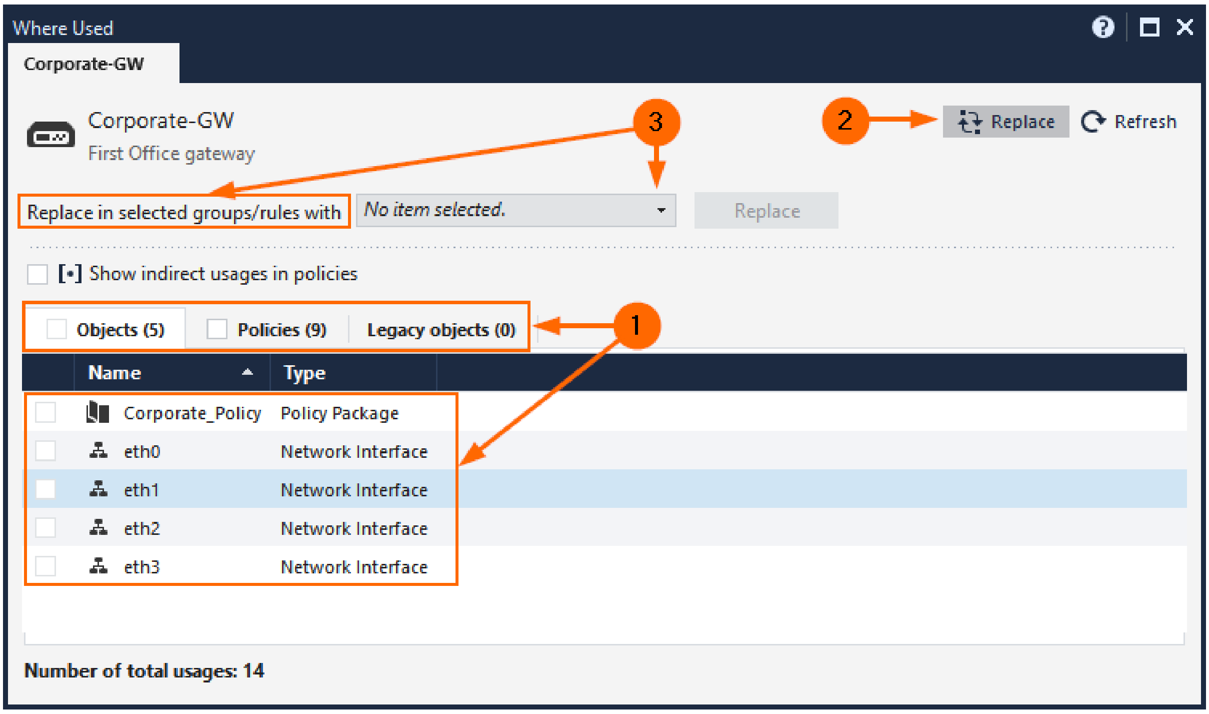
Hardware	CPU Usage
5000 Appliances	21%
5000 Appliances	7%
5000 Appliances	5%
5000 Appliances	16%







Same as in Action Toolbar



Corporate-GW
First Office gateway

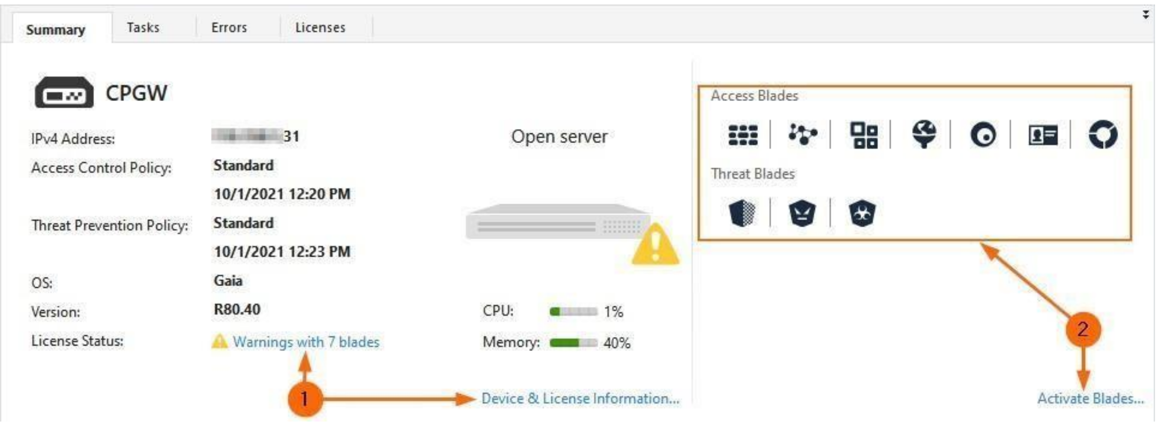
Replace in selected groups/rules with: *No item selected.*

□ Show indirect usages in policies

□ Objects (5) | □ Policies (9) | Legacy objects (0)

	Name	Type
□	Corporate_Policy	Policy Package
□	eth0	Network Interface
□	eth1	Network Interface
□	eth2	Network Interface
□	eth3	Network Interface

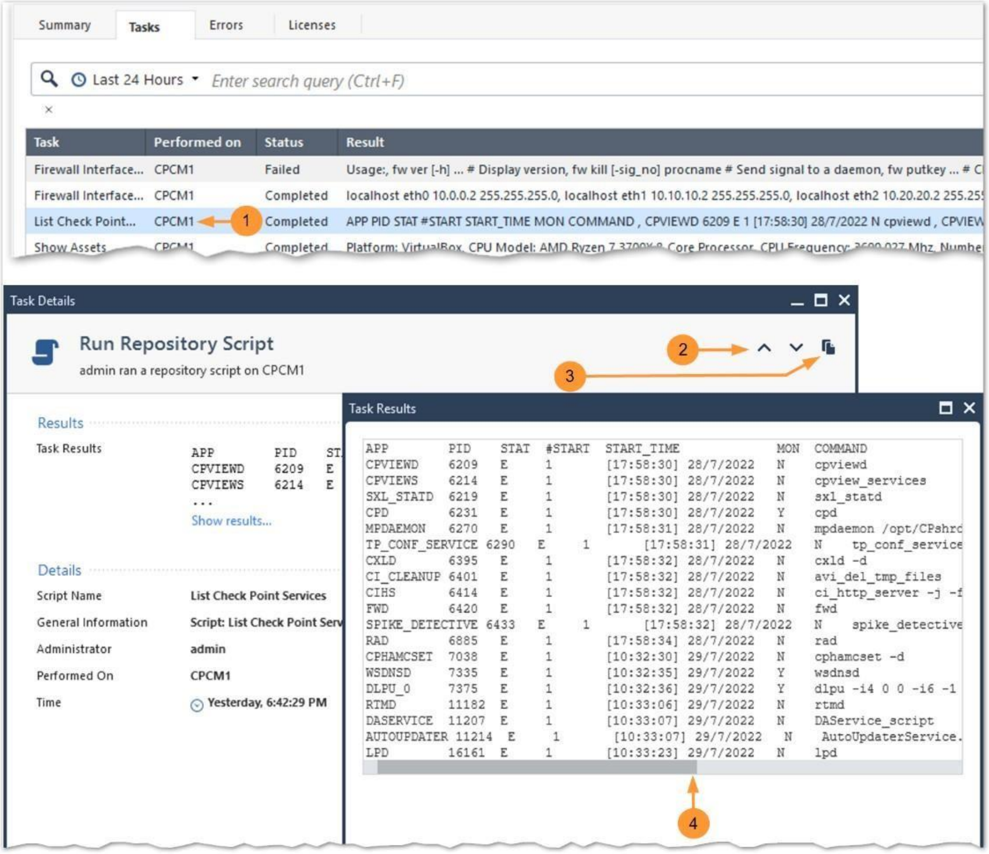
Number of total usages: 14



CPGW

IPv4 Address:	[redacted]31
Access Control Policy:	Standard 10/1/2021 12:20 PM
Threat Prevention Policy:	Standard 10/1/2021 12:23 PM
OS:	Gaia
Version:	R80.40
License Status:	Warnings with 7 blades

CPU: 1%
Memory: 40%



Task	Performed on	Status	Result
Firewall Interface...	CPCM1	Failed	Usage:, fw ver [-h] ... # Display version, fw kill [-sig_no] procname # Send signal to a daemon, fw putkey ... # C
Firewall Interface...	CPCM1	Completed	localhost eth0 10.0.0.2 255.255.255.0, localhost eth1 10.10.10.2 255.255.255.0, localhost eth2 10.20.20.2 255.25
List Check Point...	CPCM1	Completed	APP PID STAT #START START_TIME MON COMMAND , CPVIEWD 6209 E 1 [17:58:30] 28/7/2022 N cpviewd , CPVIEW
Show Assets	CPCM1	Completed	Platform: VirtualBox, CPU Model: AMD Ryzen 7 3700X 8 Core Processor, CPU Frequency: 3600.027 Mhz, Numbe

Run Repository Script

admin ran a repository script on CPCM1

Results

Task Results

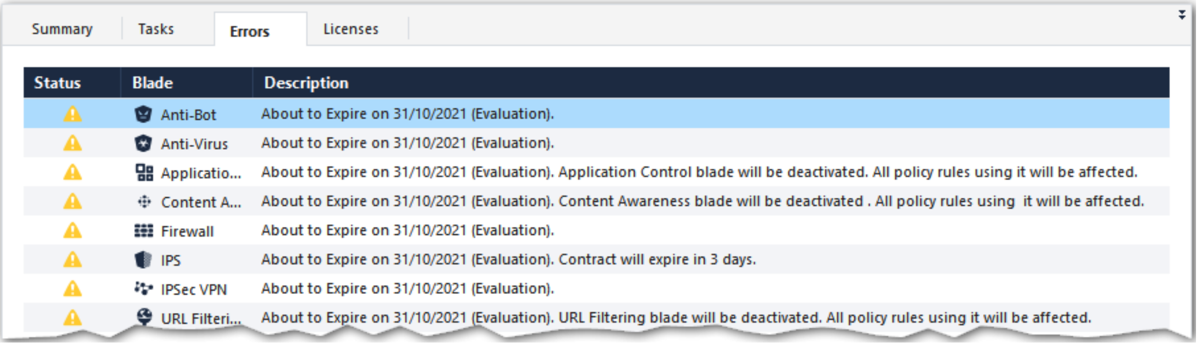
```
APP       PID   ST
CPVIEWD   6209  E
CPVIEWS   6214  E
...
```

Show results...

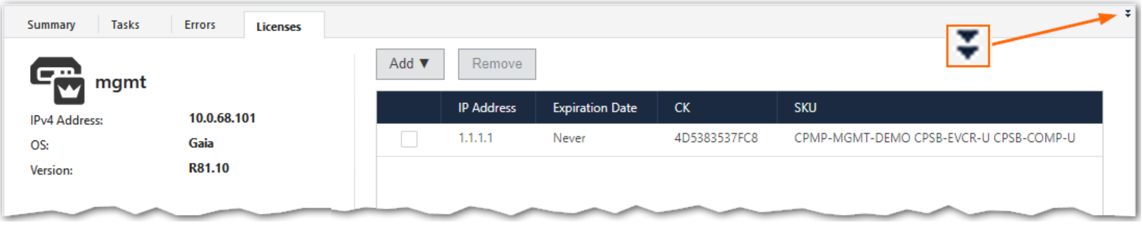
Details

Script Name	List Check Point Services
General Information	Script: List Check Point Serv
Administrator	admin
Performed On	CPCM1
Time	Yesterday, 6:42:29 PM

```
APP         PID   STAT  #START  START_TIME             MON  COMMAND
CPVIEWD     6209  E     1       [17:58:30] 28/7/2022   N    cpviewd
CPVIEWS     6214  E     1       [17:58:30] 28/7/2022   N    cpview_services
SXL_STATD   6219  E     1       [17:58:30] 28/7/2022   N    sxl_statd
CPD         6231  E     1       [17:58:30] 28/7/2022   Y    cpd
MPDAEMON    6270  E     1       [17:58:31] 28/7/2022   N    mpdaemon /opt/CPshrd
TP_CONF_SERVICE 6290   E     1       [17:58:31] 28/7/2022   N    tp_conf_service
CXLD        6395  E     1       [17:58:32] 28/7/2022   N    cxld -d
CI_CLEANUP  6401  E     1       [17:58:32] 28/7/2022   N    avi_del_tmp_files
CIHS        6414  E     1       [17:58:32] 28/7/2022   N    ci_http_server -j -f
FWD         6420  E     1       [17:58:32] 28/7/2022   N    fwd
SPIKE_DETECTIVE 6433   E     1       [17:58:32] 28/7/2022   N    spike_detective
RAD         6885  E     1       [17:58:34] 28/7/2022   N    rad
CPHAMCSET   7038  E     1       [10:32:30] 29/7/2022   N    cphamcset -d
WSDNSD      7335  E     1       [10:32:35] 29/7/2022   Y    wsdnsd
DLPU_0      7375  E     1       [10:32:36] 29/7/2022   Y    dlpu -i4 0 0 -i6 -1
RTMD        11182 E     1       [10:33:06] 29/7/2022   N    rtmd
DASERVICE   11207 E     1       [10:33:07] 29/7/2022   N    DAService_script
AUTOUPDATER 11214  E     1       [10:33:07] 29/7/2022   N    AutoUpdaterService.
LPD         16161 E     1       [10:33:23] 29/7/2022   N    lpd
```



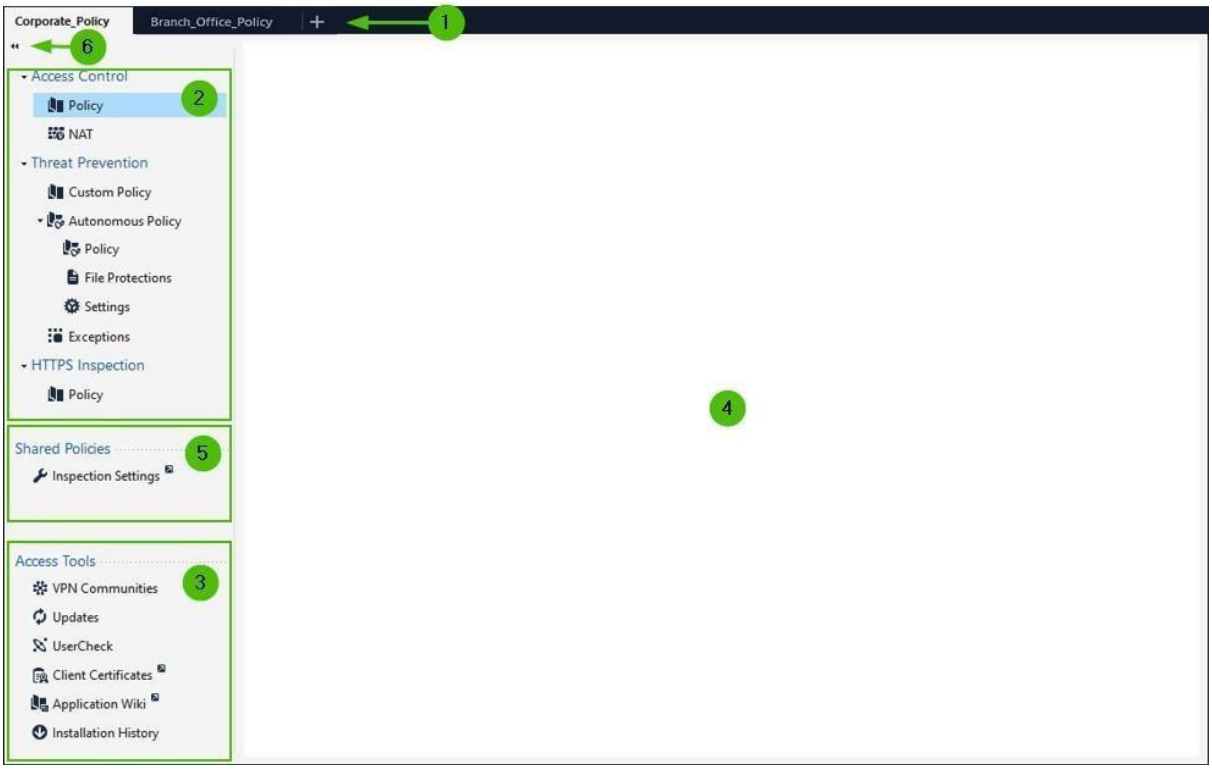
Status	Blade	Description
⚠	Anti-Bot	About to Expire on 31/10/2021 (Evaluation).
⚠	Anti-Virus	About to Expire on 31/10/2021 (Evaluation).
⚠	Applicatio...	About to Expire on 31/10/2021 (Evaluation). Application Control blade will be deactivated. All policy rules using it will be affected.
⚠	Content A...	About to Expire on 31/10/2021 (Evaluation). Content Awareness blade will be deactivated . All policy rules using it will be affected.
⚠	Firewall	About to Expire on 31/10/2021 (Evaluation).
⚠	IPS	About to Expire on 31/10/2021 (Evaluation). Contract will expire in 3 days.
⚠	IPSec VPN	About to Expire on 31/10/2021 (Evaluation).
⚠	URL Filteri...	About to Expire on 31/10/2021 (Evaluation). URL Filtering blade will be deactivated. All policy rules using it will be affected.

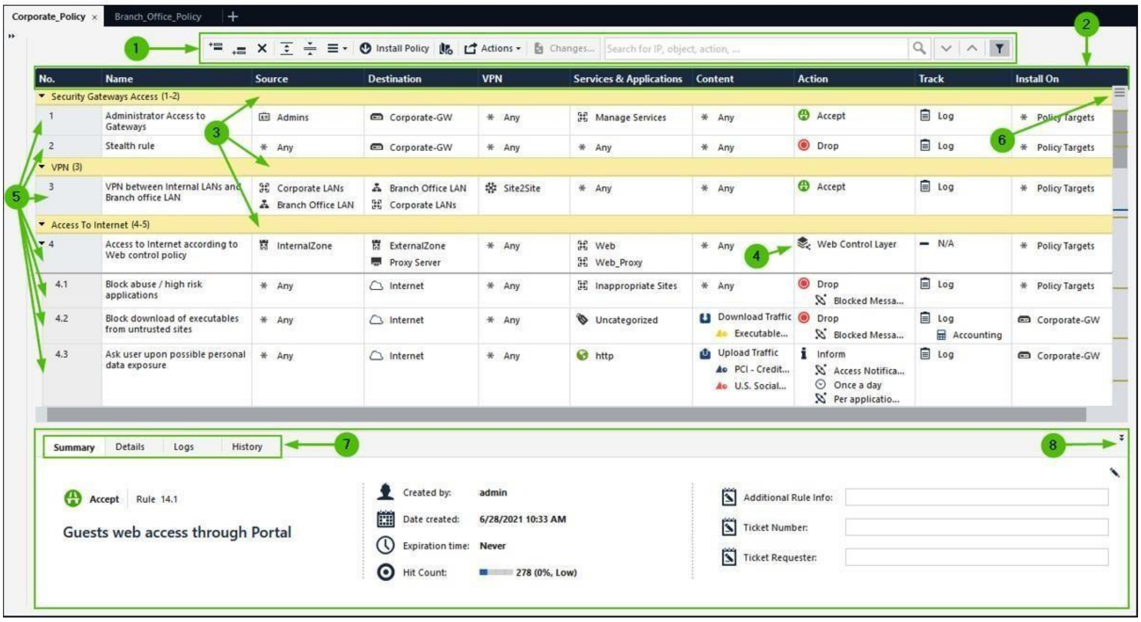


mgmt

IPv4 Address:	10.0.68.101
OS:	Gaia
Version:	R81.10

	IP Address	Expiration Date	CK	SKU
□	1.1.1.1	Never	4D5383537FC8	CPMP-MGMT-DEMO CPSB-EVCR-U CPSB-COMP-U





No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track	Install On
Security Gateways Access (1-2)									
1	Administrator Access to Gateways	Admins	Corporate-GW	Any	Manage Services	Any	Accept	Log	Policy Targets
2	Stealth rule	Any	Corporate-GW	Any	Any	Any	Drop	Log	Policy Targets
VPN (3)									
3	VPN between Internal LANs and Branch office LAN	Corporate LANs Branch Office LAN	Branch Office LAN Corporate LANs	Site2Site	Any	Any	Accept	Log	Policy Targets
Access To Internet (4-5)									
4	Access to Internet according to Web control policy	InternalZone	ExternalZone Proxy Server	Any	Web Web_Proxy	Any	Web Control Layer	N/A	Policy Targets
4.1	Block abuse / high risk applications	Any	Internet	Any	Inappropriate Sites	Any	Drop Blocked Messa...	Log	Policy Targets
4.2	Block download of executables from untrusted sites	Any	Internet	Any	Uncategorized	Download Traffic Executable...	Drop Blocked Messa...	Log Accounting	Corporate-GW
4.3	Ask user upon possible personal data exposure	Any	Internet	Any	http	Upload Traffic PCI - Credit... U.S. Social...	Inform Access Notifica... Once a day Per applicatio...	Log	Corporate-GW

Summary | Details | Logs | History

Accept | Rule 14.1

Guests web access through Portal

Created by: admin

Date created: 6/28/2021 10:33 AM

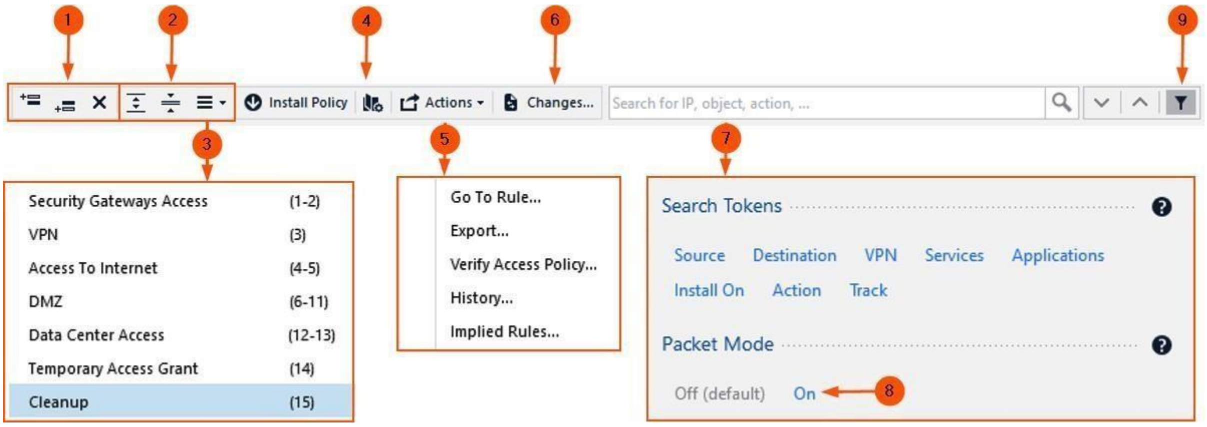
Expiration time: Never

Hit Count: 278 (0%, Low)

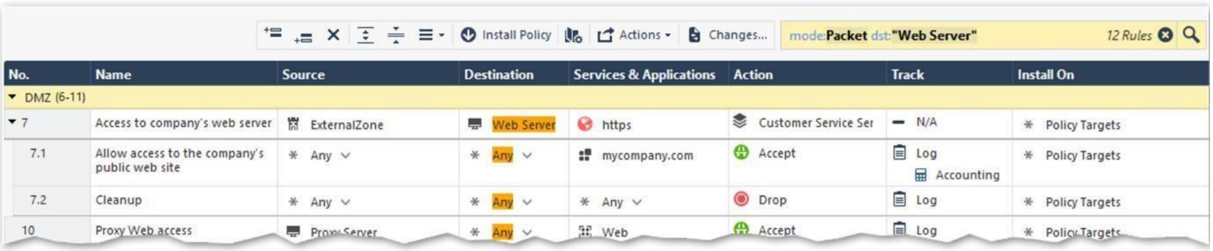
Additional Rule Info:

Ticket Number:

Ticket Requester:



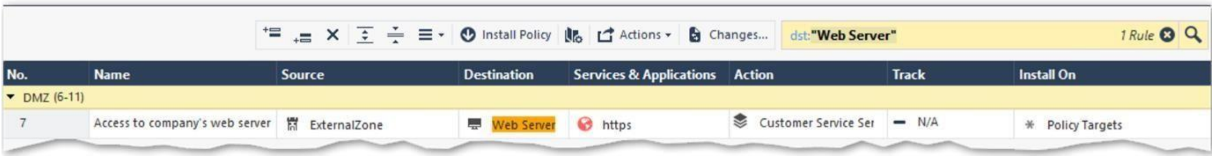
Packet mode On



mode:Packet dst:"Web Server" 12 Rules

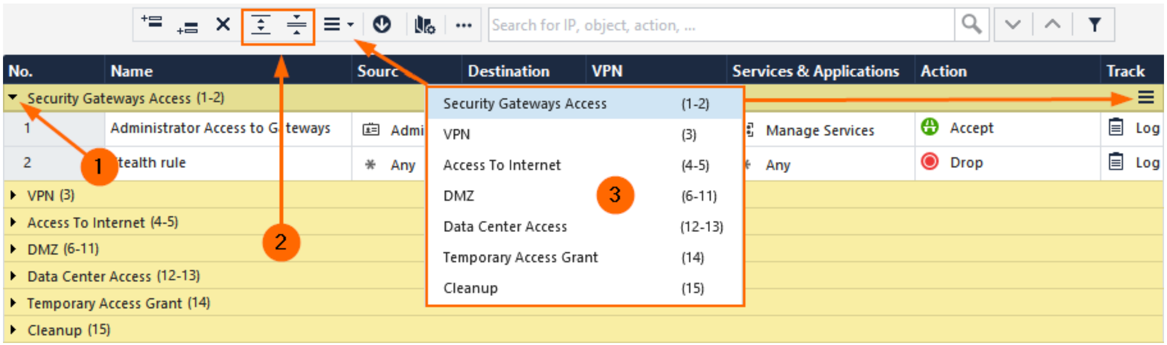
No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
DMZ (6-11)							
7	Access to company's web server	ExternalZone	Web Server	https	Customer Service Ser	N/A	Policy Targets
7.1	Allow access to the company's public web site	Any	Any	mycompany.com	Accept	Log Accounting	Policy Targets
7.2	Cleanup	Any	Any	Any	Drop	Log	Policy Targets
10	Proxy Web access	Proxy Server	Any	Web	Accept	Log	Policy Targets

Packet mode Off

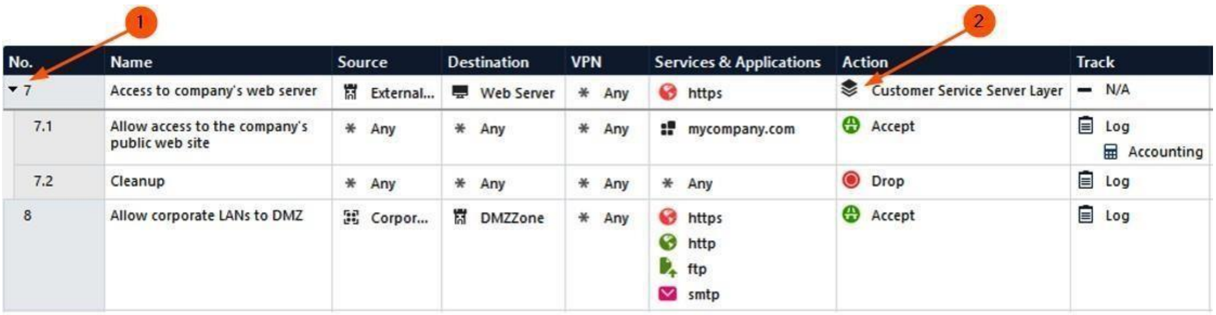


dst:"Web Server" 1 Rule

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
DMZ (6-11)							
7	Access to company's web server	ExternalZone	Web Server	https	Customer Service Ser	N/A	Policy Targets

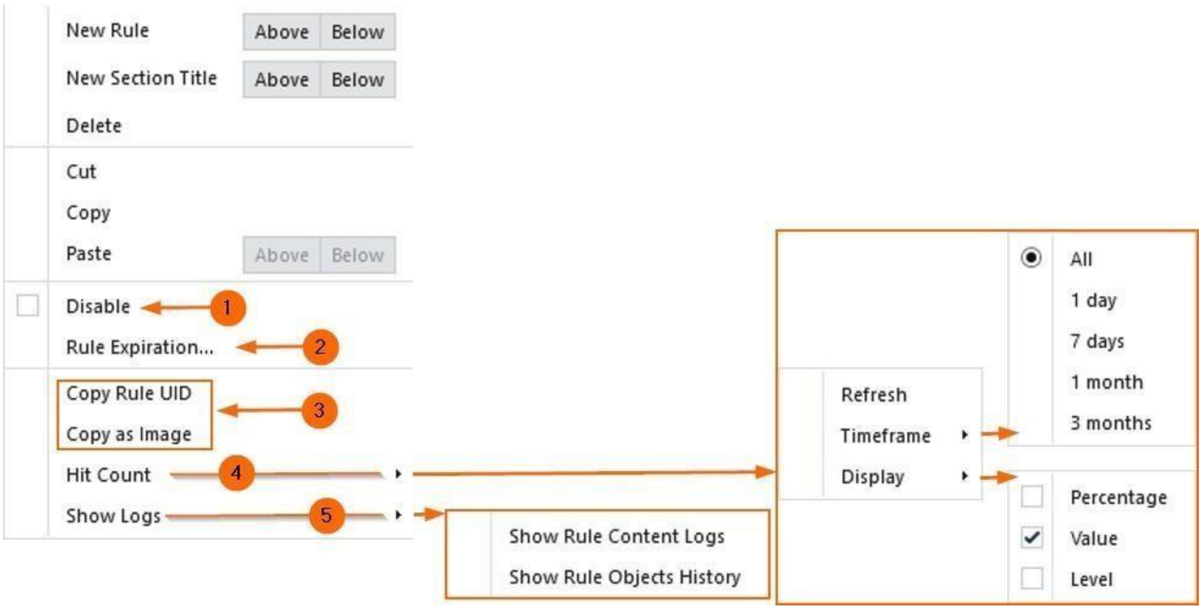

Search for IP, object, action, ...
1
2
3
Security Gateways Access (1-2)
VPN (3)
Access To Internet (4-5)
DMZ (6-11)
Data Center Access (12-13)
Temporary Access Grant (14)
Cleanup (15)

No.	Name	Sourc	Destination	VPN	Services & Applications	Action	Track
Security Gateways Access (1-2)							
1	Administrator Access to G teways	Admi			Manage Services	Accept	Log
2	tealth rule	Any			Any	Drop	Log
VPN (3)							
Access To Internet (4-5)							
DMZ (6-11)							
Data Center Access (12-13)							
Temporary Access Grant (14)							
Cleanup (15)							

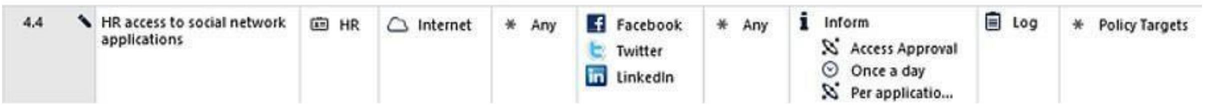


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
7	Access to company's web server	External...	Web Server	Any	https	Customer Service Server Layer	N/A
7.1	Allow access to the company's public web site	Any	Any	Any	mycompany.com	Accept	Log Accounting
7.2	Cleanup	Any	Any	Any	Any	Drop	Log
8	Allow corporate LANs to DMZ	Corpor...	DMZZone	Any	https http ftp smtp	Accept	Log

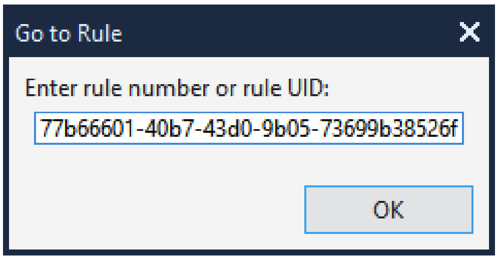
Not Shared Shared



872405ec-e9f7-4b6b-9af9-e495338536f3

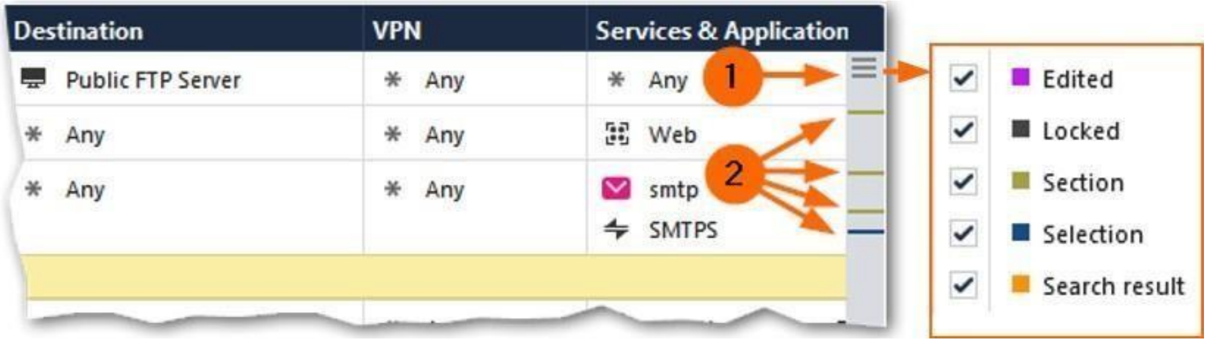


4.4	HR access to social network applications	HR	Internet	Any	Facebook Twitter LinkedIn	Any	Inform Access Approval Once a day Per applicatio...	Log	Policy Targets


Go to Rule

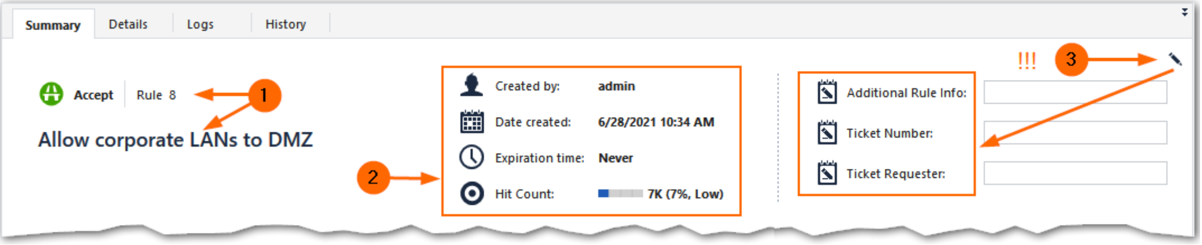
Enter rule number or rule UID:

77b66601-40b7-43d0-9b05-73699b38526f



Destination	VPN	Services & Application
Public FTP Server	Any	Any
Any	Any	Web
Any	Any	smtp SMTPS

- ☑ 🟪 Edited
- ☑ ■ Locked
- ☑ 🟩 Section
- ☑ 🟦 Selection
- ☑ 🟧 Search result



Accept Rule 8

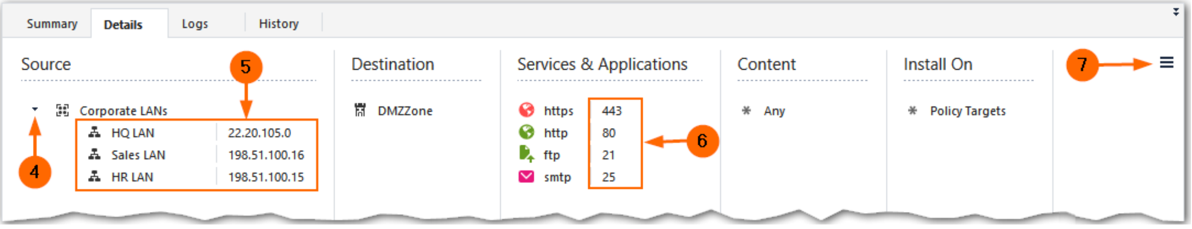
Allow corporate LANs to DMZ

Created by:	admin
Date created:	6/28/2021 10:34 AM
Expiration time:	Never
Hit Count:	7K (7%, Low)

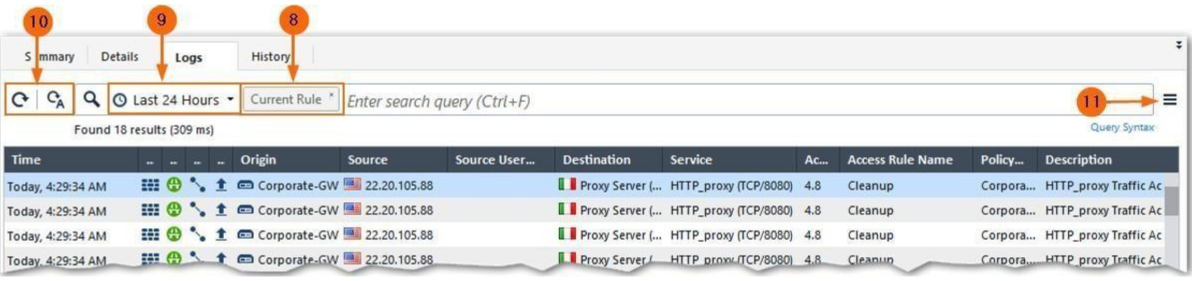
Additional Rule Info:

Ticket Number:

Ticket Requester:

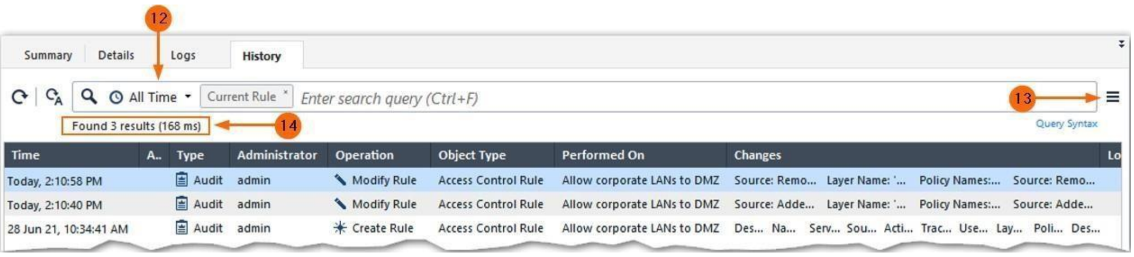


Source	Destination	Services & Applications	Content	Install On
Corporate LANs	DMZZone	https 443	Any	Policy Targets
HQ LAN 22.20.105.0		http 80		
Sales LAN 198.51.100.16		ftp 21		
HR LAN 198.51.100.15		smtp 25		



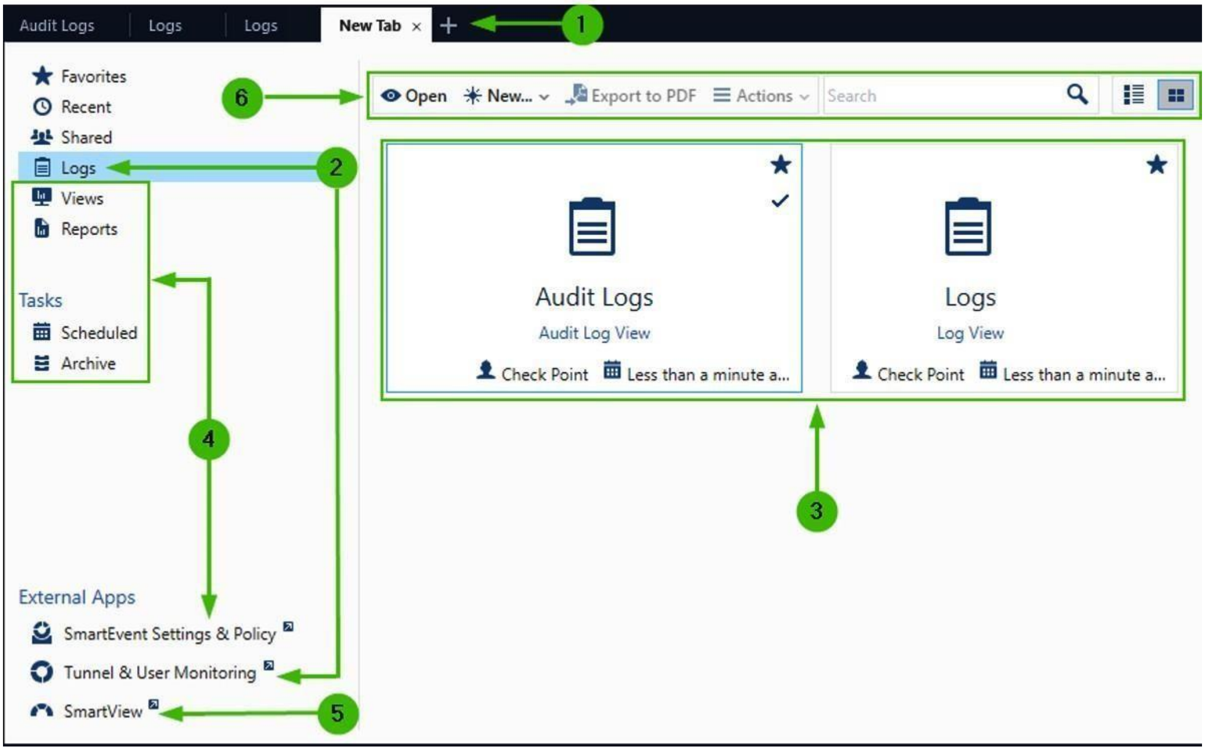
Found 18 results (309 ms)

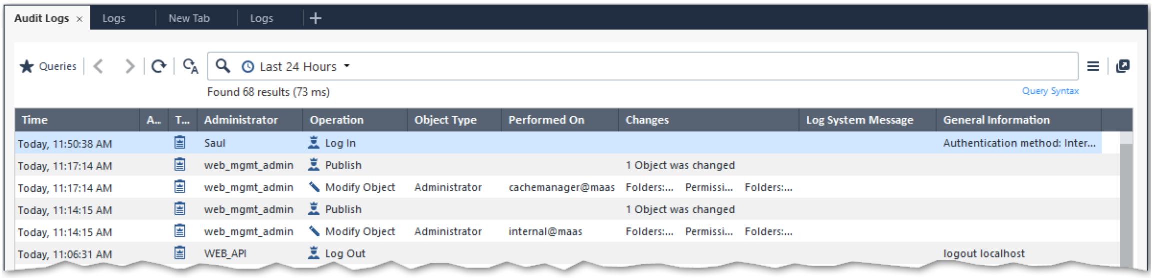
Time	..	..	..	..	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule Name	Policy...	Description
Today, 4:29:34 AM					Corporate-GW	22.20.105.88		Proxy Server (...	HTTP_proxy (TCP/8080)	4.8	Cleanup	Corpora...	HTTP_proxy Traffic Ac
Today, 4:29:34 AM					Corporate-GW	22.20.105.88		Proxy Server (...	HTTP_proxy (TCP/8080)	4.8	Cleanup	Corpora...	HTTP_proxy Traffic Ac
Today, 4:29:34 AM					Corporate-GW	22.20.105.88		Proxy Server (...	HTTP_proxy (TCP/8080)	4.8	Cleanup	Corpora...	HTTP_proxy Traffic Ac
Today, 4:29:34 AM					Corporate-GW	22.20.105.88		Proxy Server (...	HTTP_proxy (TCP/8080)	4.8	Cleanup	Corpora...	HTTP_proxy Traffic Ac



Found 3 results (168 ms)

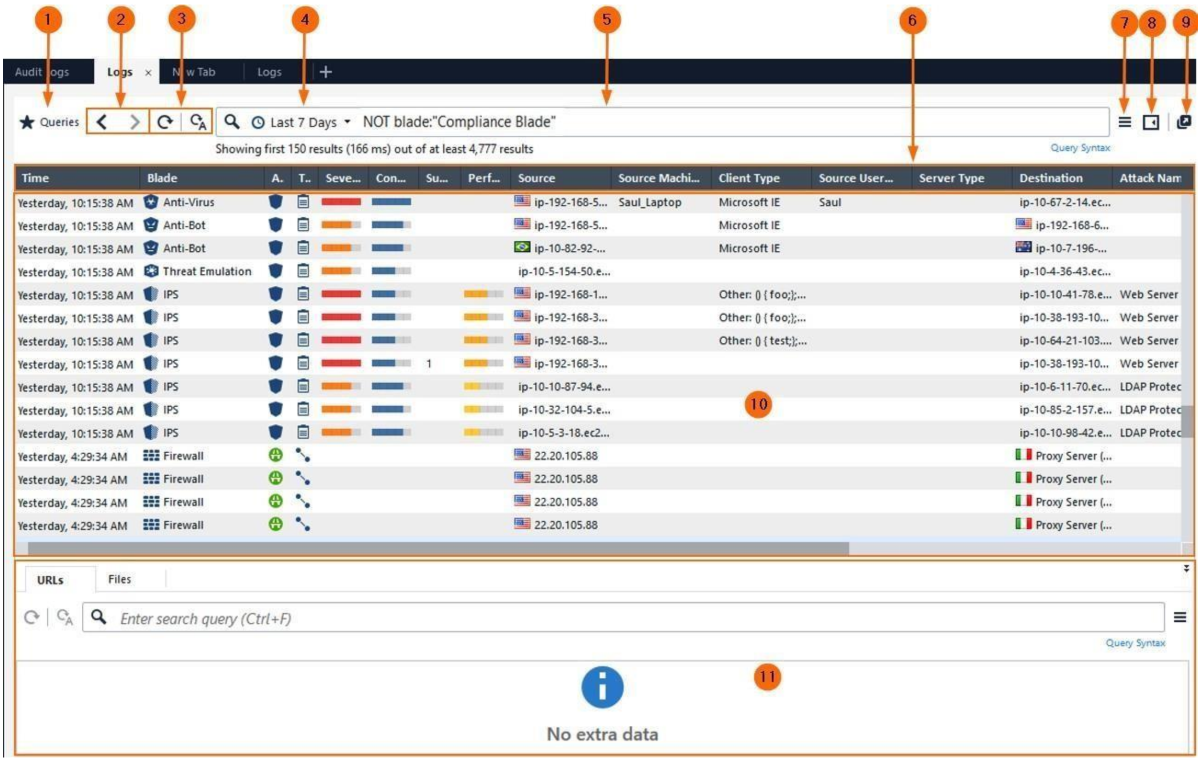
Time	A..	Type	Administrator	Operation	Object Type	Performed On	Changes	Lo
Today, 2:10:58 PM		Audit	admin	Modify Rule	Access Control Rule	Allow corporate LANs to DMZ	Source: Remo... Layer Name: '... Policy Names:... Source: Remo...	
Today, 2:10:40 PM		Audit	admin	Modify Rule	Access Control Rule	Allow corporate LANs to DMZ	Source: Adde... Layer Name: '... Policy Names:... Source: Adde...	
28 Jun 21, 10:34:41 AM		Audit	admin	Create Rule	Access Control Rule	Allow corporate LANs to DMZ	Des... Na... Serv... Sou... Acti... Trac... Use... Lay... Poli... Des...	





Found 68 results (73 ms)

Time	A...	T...	Administrator	Operation	Object Type	Performed On	Changes	Log System Message	General Information
Today, 11:50:38 AM			Saul	Log In					Authentication method: Inter...
Today, 11:17:14 AM			web_mgmt_admin	Publish			1 Object was changed		
Today, 11:17:14 AM			web_mgmt_admin	Modify Object	Administrator	cachemanager@maas	Folders:... Permissi... Folders:...		
Today, 11:14:15 AM			web_mgmt_admin	Publish			1 Object was changed		
Today, 11:14:15 AM			web_mgmt_admin	Modify Object	Administrator	internal@maas	Folders:... Permissi... Folders:...		
Today, 11:06:31 AM			WEB_API	Log Out					logout localhost

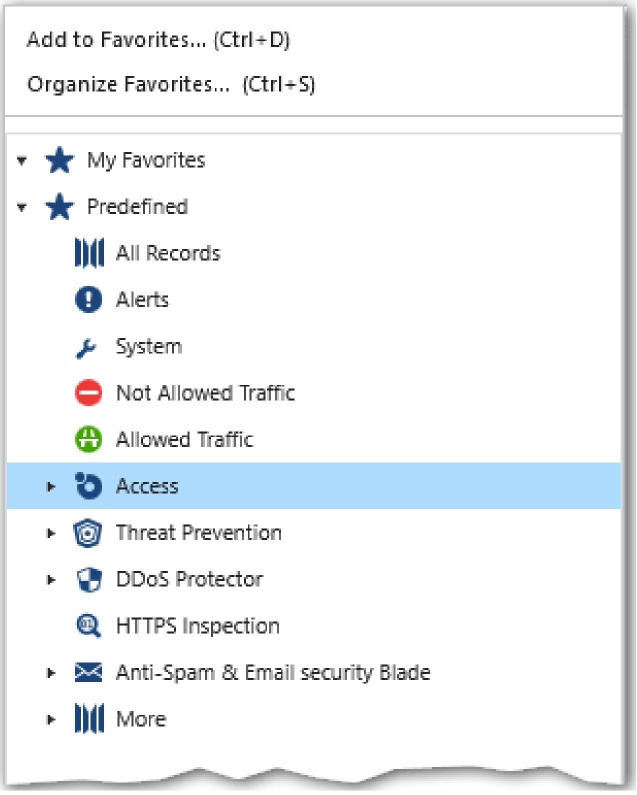


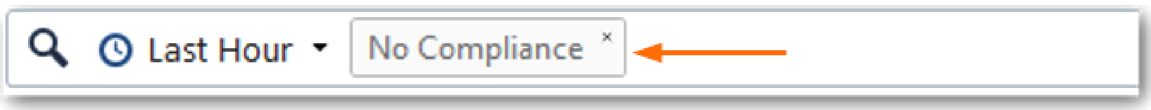
NOT blade:"Compliance Blade"

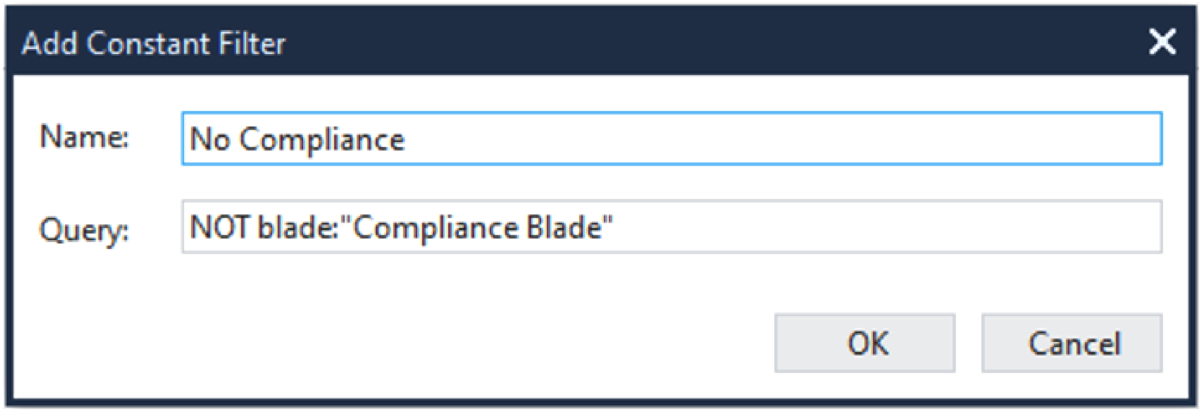
Showing first 150 results (166 ms) out of at least 4,777 results

Time	Blade	A.	T..	Seve...	Con...	Su...	Perf...	Source	Source Machi...	Client Type	Source User...	Server Type	Destination	Attack Nam
Yesterday, 10:15:38 AM	Anti-Virus							ip-192-168-5...	Saul_Laptop	Microsoft IE	Saul		ip-10-67-2-14.ec...	
Yesterday, 10:15:38 AM	Anti-Bot							ip-192-168-5...		Microsoft IE			ip-192-168-6...	
Yesterday, 10:15:38 AM	Anti-Bot							ip-10-82-92-...		Microsoft IE			ip-10-7-196-...	
Yesterday, 10:15:38 AM	Threat Emulation							ip-10-5-154-50.e...					ip-10-4-36-43.ec...	
Yesterday, 10:15:38 AM	IPS							ip-192-168-1...		Other: () { foo;};...			ip-10-10-41-78.e...	Web Server
Yesterday, 10:15:38 AM	IPS							ip-192-168-3...		Other: () { foo;};...			ip-10-38-193-10...	Web Server
Yesterday, 10:15:38 AM	IPS							ip-192-168-3...		Other: () { test;};...			ip-10-64-21-103....	Web Server
Yesterday, 10:15:38 AM	IPS					1		ip-192-168-3...					ip-10-38-193-10...	Web Server
Yesterday, 10:15:38 AM	IPS							ip-10-10-87-94.e...					ip-10-6-11-70.ec...	LDAP Protec
Yesterday, 10:15:38 AM	IPS							ip-10-32-104-5.e...					ip-10-85-2-157.e...	LDAP Protec
Yesterday, 10:15:38 AM	IPS							ip-10-5-3-18.ec2...					ip-10-10-98-42.e...	LDAP Protec
Yesterday, 4:29:34 AM	Firewall							22.20.105.88					Proxy Server (...	
Yesterday, 4:29:34 AM	Firewall							22.20.105.88					Proxy Server (...	
Yesterday, 4:29:34 AM	Firewall							22.20.105.88					Proxy Server (...	
Yesterday, 4:29:34 AM	Firewall							22.20.105.88					Proxy Server (...	

Enter search query (Ctrl+F)

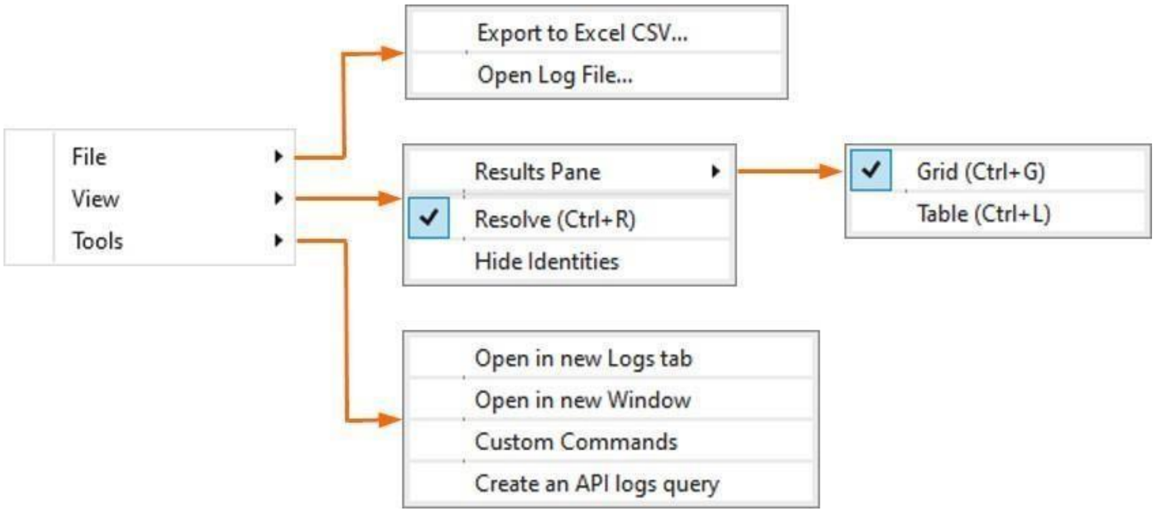


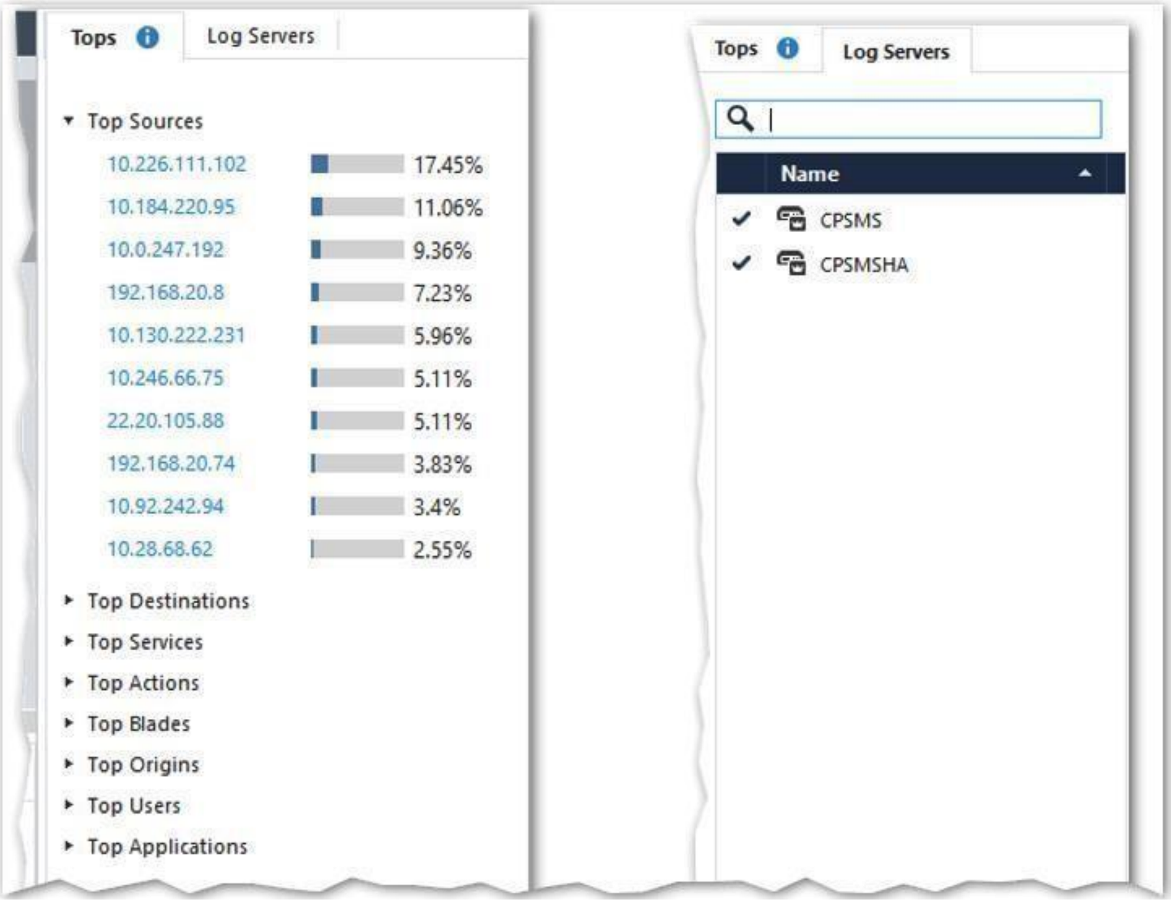




Name: No Compliance

Query: NOT blade:"Compliance Blade"





Tops | Log Servers

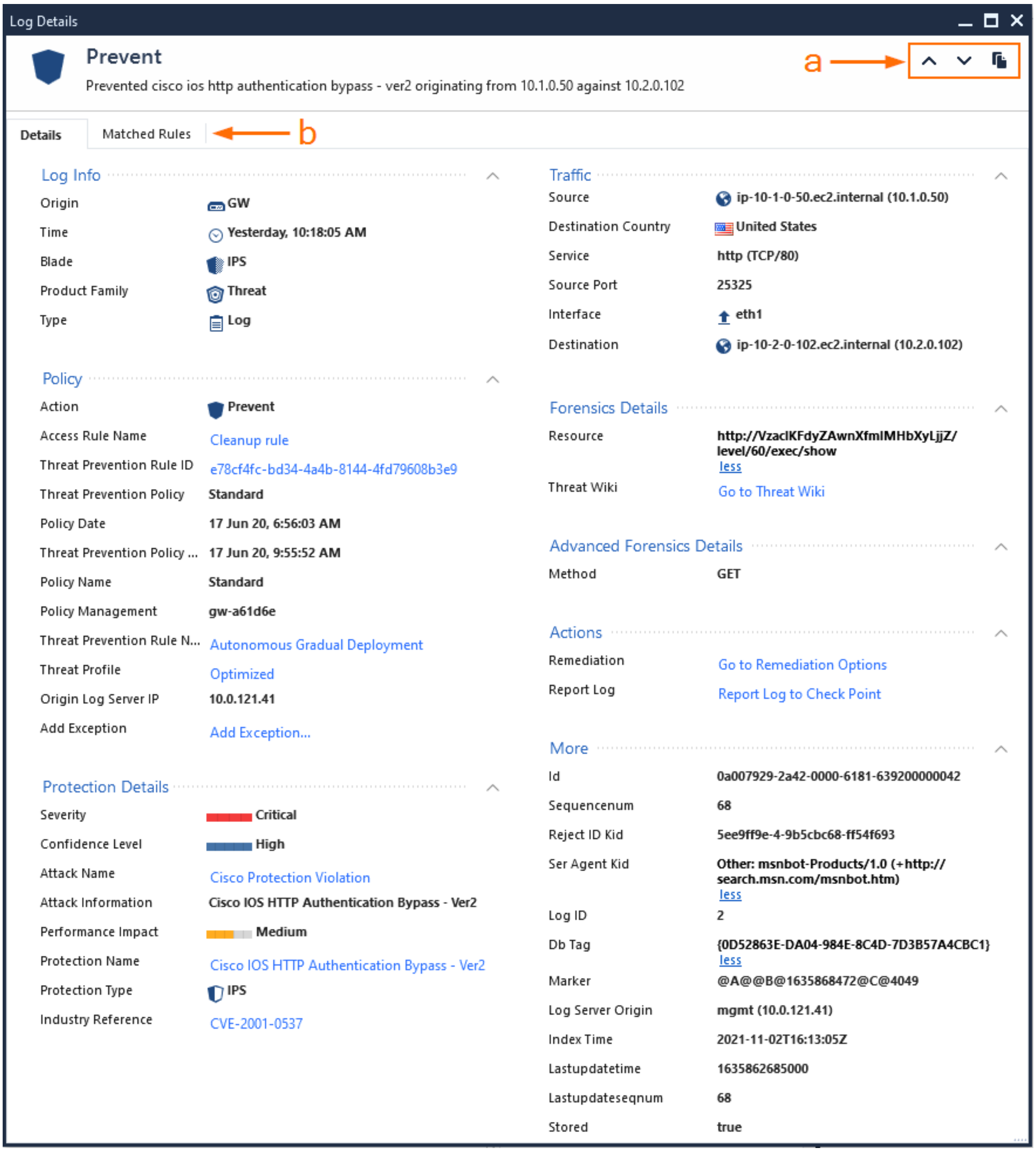
▾ Top Sources

10.226.111.102	17.45%
10.184.220.95	11.06%
10.0.247.192	9.36%
192.168.20.8	7.23%
10.130.222.231	5.96%
10.246.66.75	5.11%
22.20.105.88	5.11%
192.168.20.74	3.83%
10.92.242.94	3.4%
10.28.68.62	2.55%

▸ Top Destinations
▸ Top Services
▸ Top Actions
▸ Top Blades
▸ Top Origins
▸ Top Users
▸ Top Applications

Tops | Log Servers

	Name
✓	CPSMS
✓	CPSMSHA



Log Details

Prevent

Prevented cisco ios http authentication bypass - ver2 originating from 10.1.0.50 against 10.2.0.102

Details | Matched Rules

Log Info

Origin	GW
Time	Yesterday, 10:18:05 AM
Blade	IPS
Product Family	Threat
Type	Log

Policy

Action	Prevent
Access Rule Name	Cleanup rule
Threat Prevention Rule ID	e78cf4fc-bd34-4a4b-8144-4fd79608b3e9
Threat Prevention Policy	Standard
Policy Date	17 Jun 20, 6:56:03 AM
Threat Prevention Policy ...	17 Jun 20, 9:55:52 AM
Policy Name	Standard
Policy Management	gw-a61d6e
Threat Prevention Rule N...	Autonomous Gradual Deployment
Threat Profile	Optimized
Origin Log Server IP	10.0.121.41
Add Exception	Add Exception...

Protection Details

Severity	🟥 Critical
Confidence Level	🟦 High
Attack Name	Cisco Protection Violation
Attack Information	Cisco IOS HTTP Authentication Bypass - Ver2
Performance Impact	🟧 Medium
Protection Name	Cisco IOS HTTP Authentication Bypass - Ver2
Protection Type	IPS
Industry Reference	CVE-2001-0537

Traffic

Source	ip-10-1-0-50.ec2.internal (10.1.0.50)
Destination Country	United States
Service	http (TCP/80)
Source Port	25325
Interface	eth1
Destination	ip-10-2-0-102.ec2.internal (10.2.0.102)

Forensics Details

Resource	http://VzaclKFdyZAwnXfmlMHbXyLjjZ/level/60/exec/show less
Threat Wiki	Go to Threat Wiki

Advanced Forensics Details

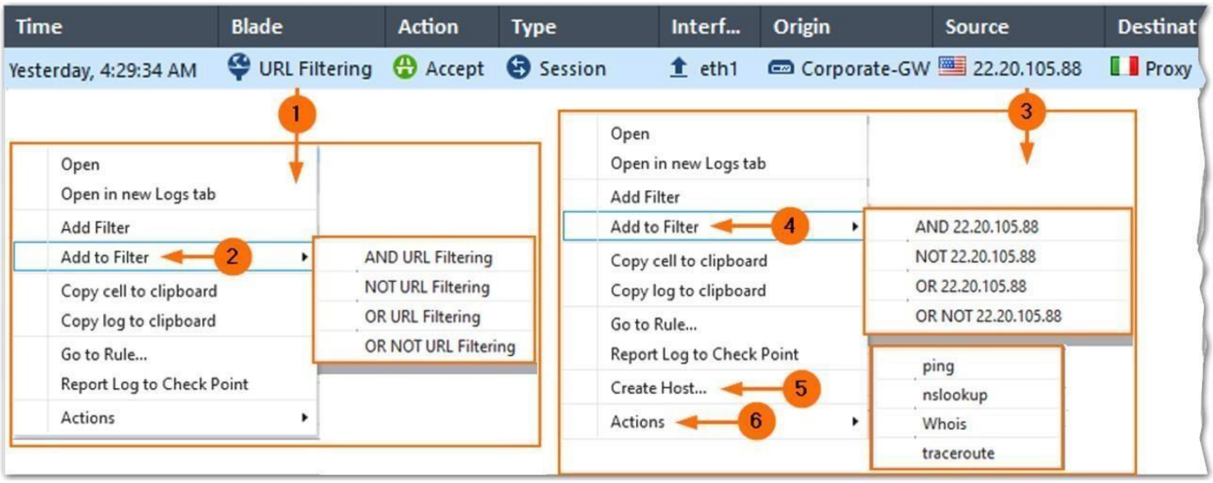
Method	GET

Actions

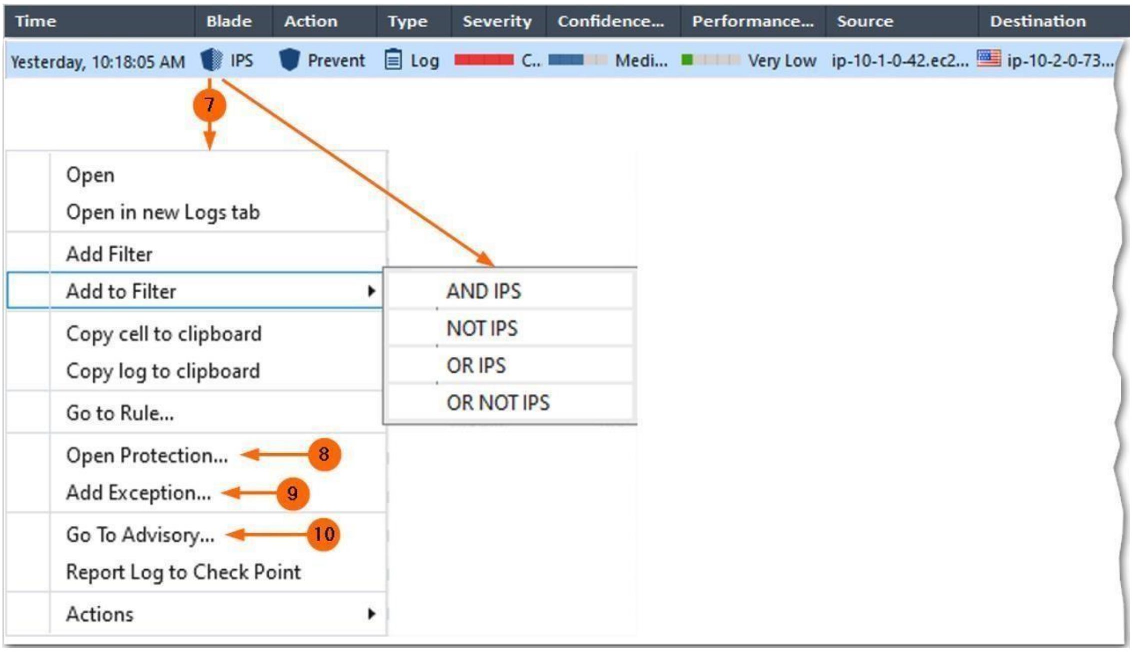
Remediation	Go to Remediation Options
Report Log	Report Log to Check Point

More

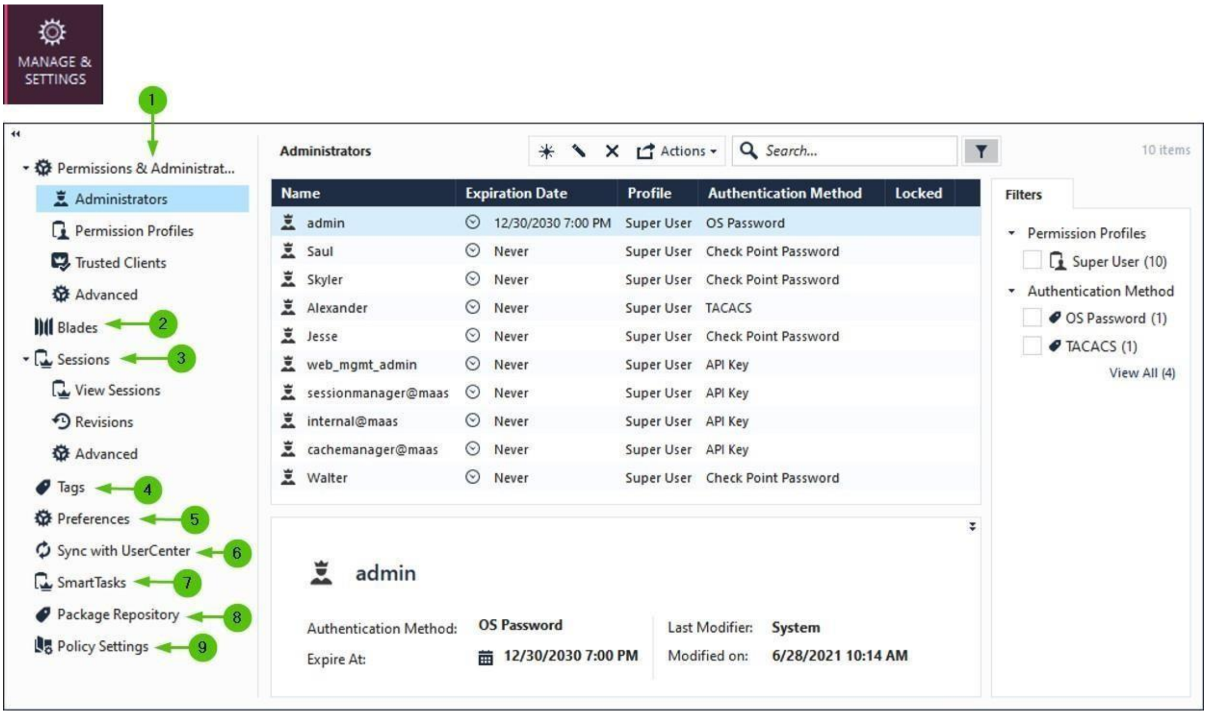
Id	0a007929-2a42-0000-6181-639200000042
Sequencenum	68
Reject ID Kid	5ee9ff9e-4-9b5cbc68-ff54f693
Ser Agent Kid	Other: msnbot-Products/1.0 (+http://search.msn.com/msnbot.htm) less
Log ID	2
Db Tag	{0D52863E-DA04-984E-8C4D-7D3B57A4CBC1} less
Marker	@A@@B@1635868472@C@4049
Log Server Origin	mgmt (10.0.121.41)
Index Time	2021-11-02T16:13:05Z
Lastupdatetime	1635862685000
Lastupdateseqnum	68
Stored	true



Time	Blade	Action	Type	Interf...	Origin	Source	Destinat
Yesterday, 4:29:34 AM	URL Filtering	Accept	Session	eth1	Corporate-GW	22.20.105.88	Proxy



Time	Blade	Action	Type	Severity	Confidence...	Performance...	Source	Destination
Yesterday, 10:18:05 AM	IPS	Prevent	Log	C...	Medi...	Very Low	ip-10-1-0-42.ec2...	ip-10-2-0-73...



Name	Expiration Date	Profile	Authentication Method	Locked
admin	12/30/2030 7:00 PM	Super User	OS Password	
Saul	Never	Super User	Check Point Password	
Skyler	Never	Super User	Check Point Password	
Alexander	Never	Super User	TACACS	
Jesse	Never	Super User	Check Point Password	
web_mgmt_admin	Never	Super User	API Key	
sessionmanager@maas	Never	Super User	API Key	
internal@maas	Never	Super User	API Key	
cachemanager@maas	Never	Super User	API Key	
Walter	Never	Super User	Check Point Password	

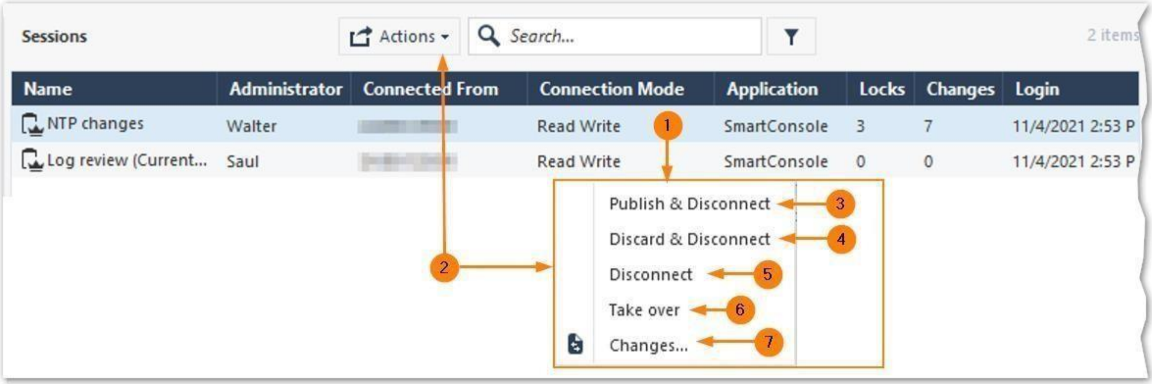
admin

Authentication Method: OS Password

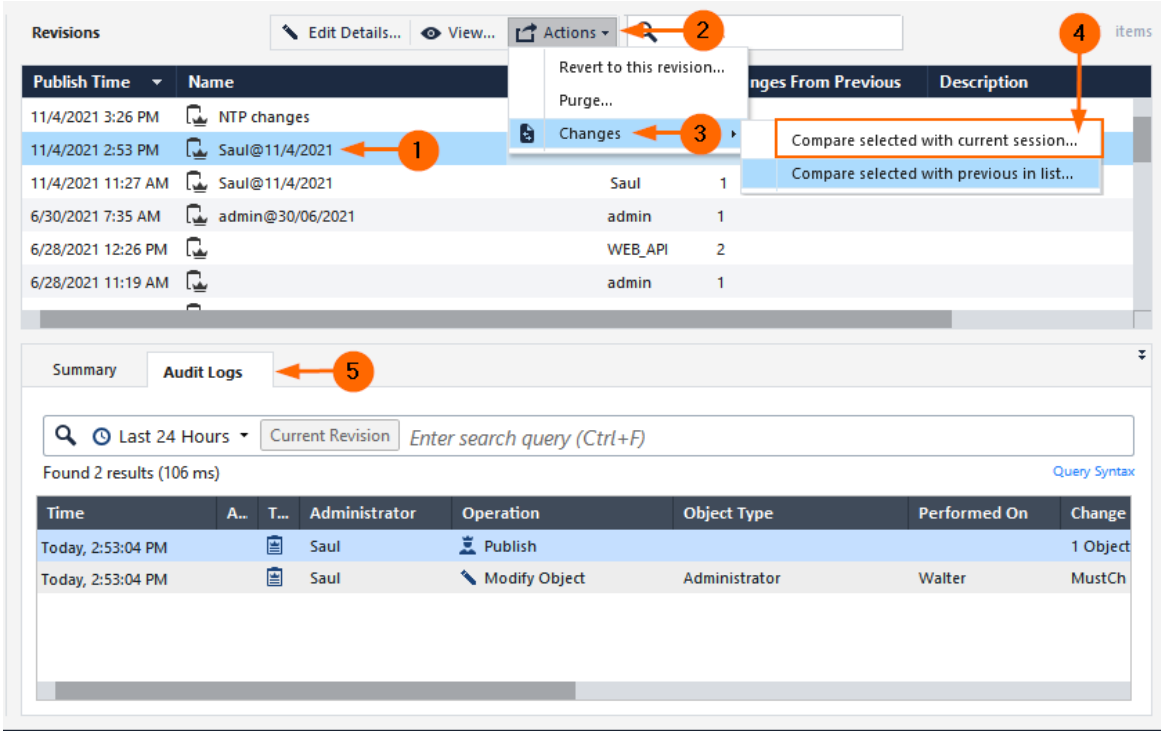
Expire At: 12/30/2030 7:00 PM

Last Modifier: System

Modified on: 6/28/2021 10:14 AM



Name	Administrator	Connected From	Connection Mode	Application	Locks	Changes	Login
NTP changes	Walter	[redacted]	Read Write	SmartConsole	3	7	11/4/2021 2:53 P
Log review (Current...	Saul	[redacted]	Read Write	SmartConsole	0	0	11/4/2021 2:53 P

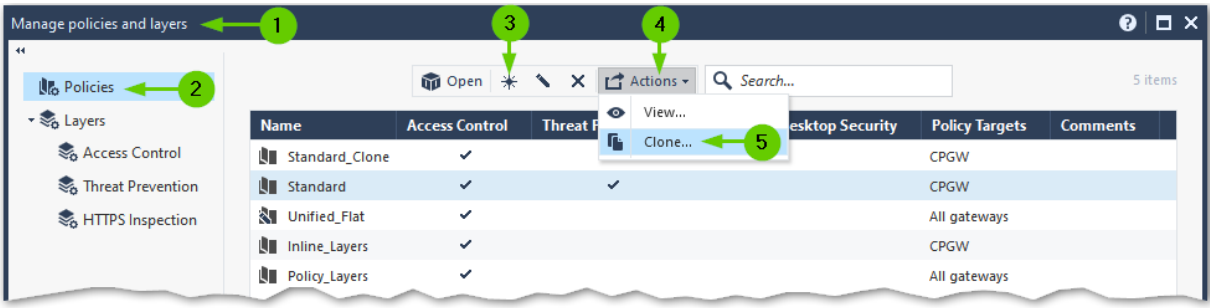


Revisions
Edit Details...
View...
Actions
items
Revert to this revision...
Purge...
Changes
Compare selected with current session...
Compare selected with previous in list...
1
2
3
4
5
Summary
Audit Logs
Last 24 Hours
Current Revision
Enter search query (Ctrl+F)
Query Syntax

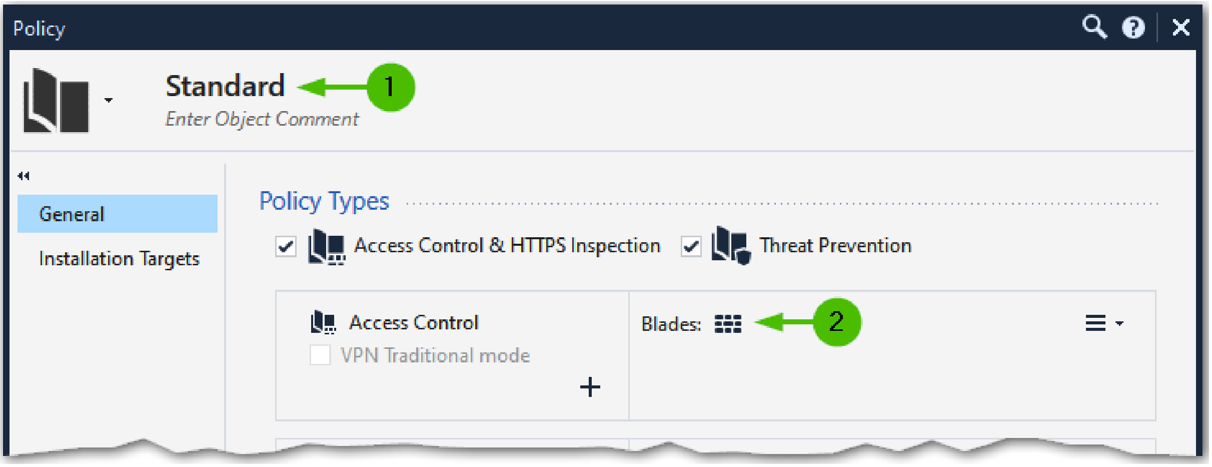
Publish Time	Name		nges From Previous	Description
11/4/2021 3:26 PM	NTP changes			
11/4/2021 2:53 PM	Saul@11/4/2021			
11/4/2021 11:27 AM	Saul@11/4/2021	Saul	1	
6/30/2021 7:35 AM	admin@30/06/2021	admin	1	
6/28/2021 12:26 PM		WEB_API	2	
6/28/2021 11:19 AM		admin	1	

Found 2 results (106 ms)

Time	A...	T...	Administrator	Operation	Object Type	Performed On	Change
Today, 2:53:04 PM			Saul	Publish			1 Object
Today, 2:53:04 PM			Saul	Modify Object	Administrator	Walter	MustCh

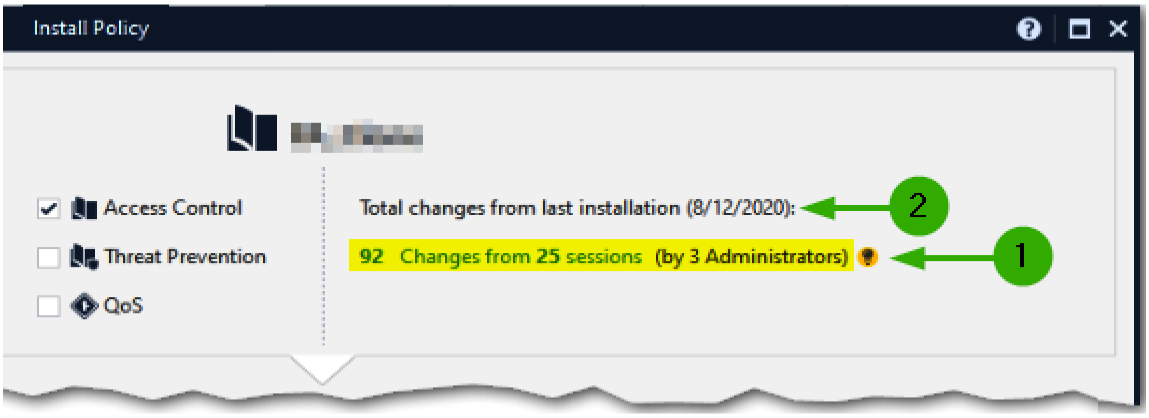


Name	Access Control	Threat P	esktop Security	Policy Targets	Comments
Standard_Clone	✓			CPGW	
Standard	✓	✓		CPGW	
Unified_Flat	✓			All gateways	
Inline_Layers	✓			CPGW	
Policy_Layers	✓			All gateways	



☑ Access Control & HTTPS Inspection ☑ Threat Prevention

□ VPN Traditional mode



[redacted]

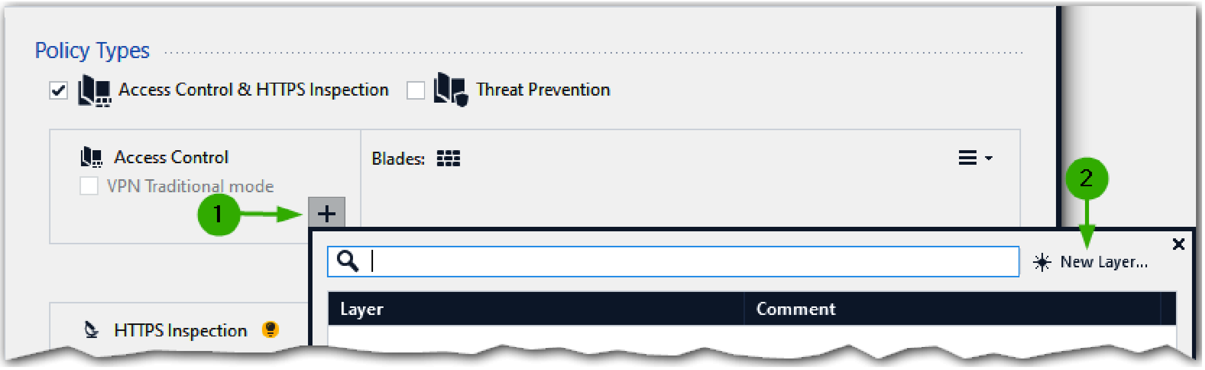
☑ Access Control

□ Threat Prevention

□ QoS

Total changes from last installation (8/12/2020):

92 Changes from 25 sessions (by 3 Administrators)



Policy Types

☑ Access Control & HTTPS Inspection □ Threat Prevention

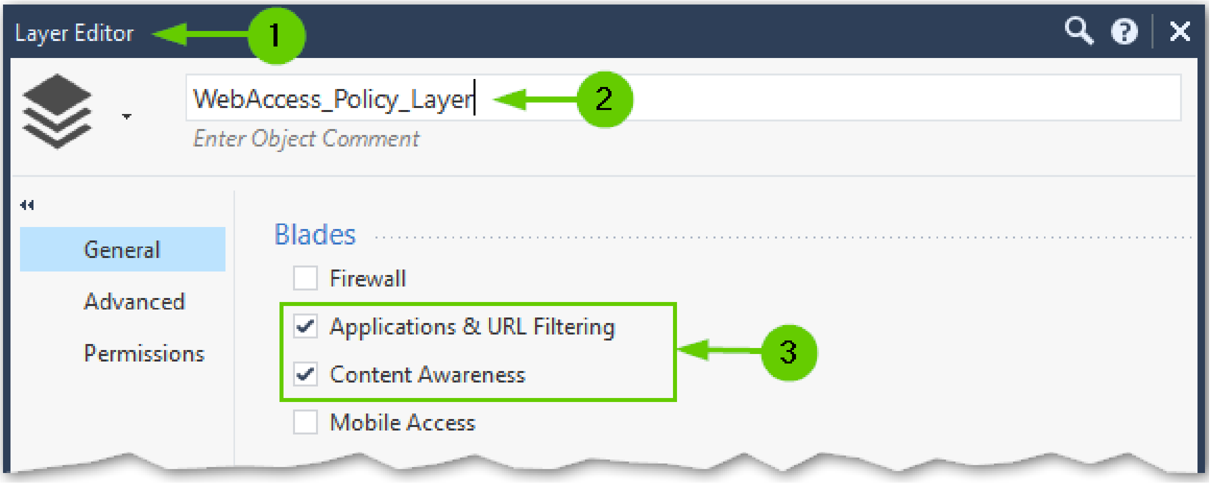
Access Control

□ VPN Traditional mode

Blades:

HTTPS Inspection

Layer	Comment



Layer Editor

WebAccess_Policy_Layer

Enter Object Comment

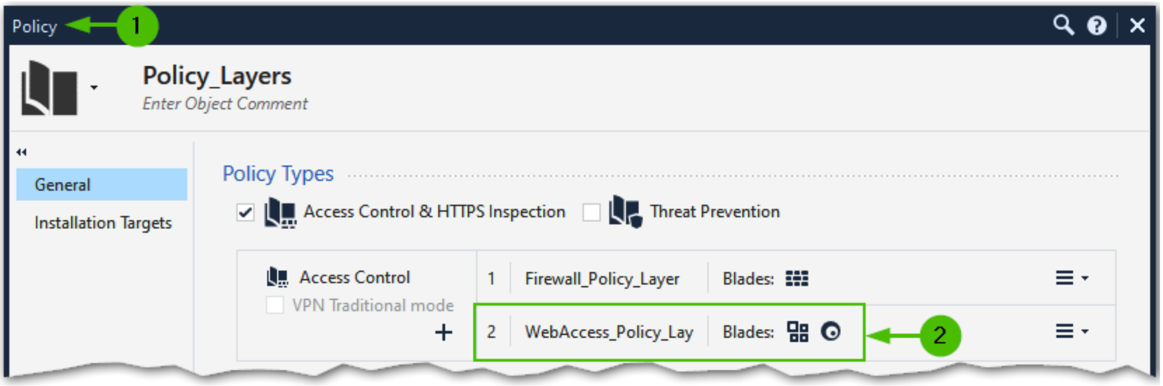
Blades

□ Firewall

☑ Applications & URL Filtering

☑ Content Awareness

□ Mobile Access



Policy

Policy_Layers

Enter Object Comment

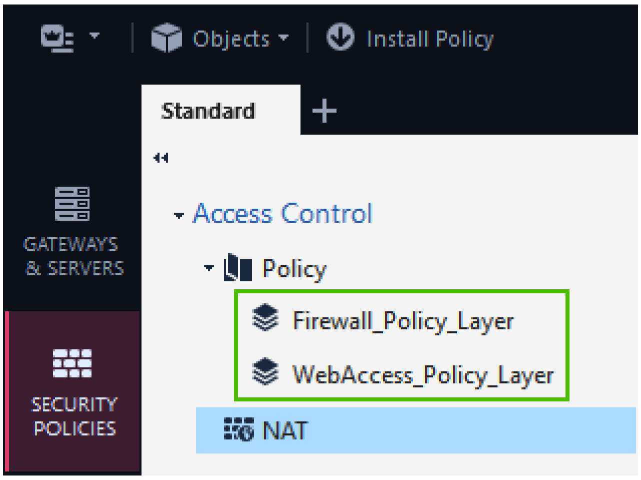
Policy Types

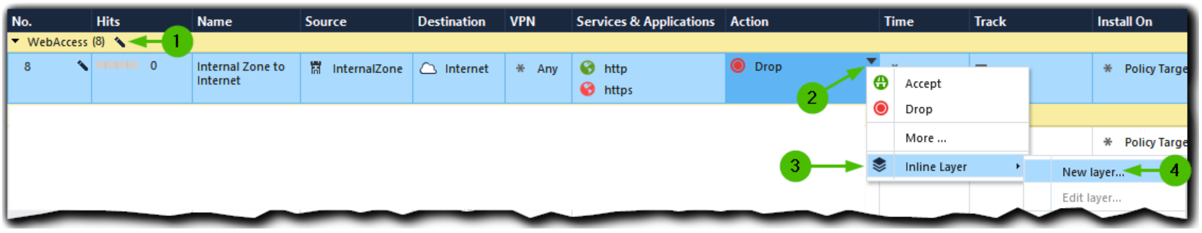
☑ Access Control & HTTPS Inspection □ Threat Prevention

Access Control

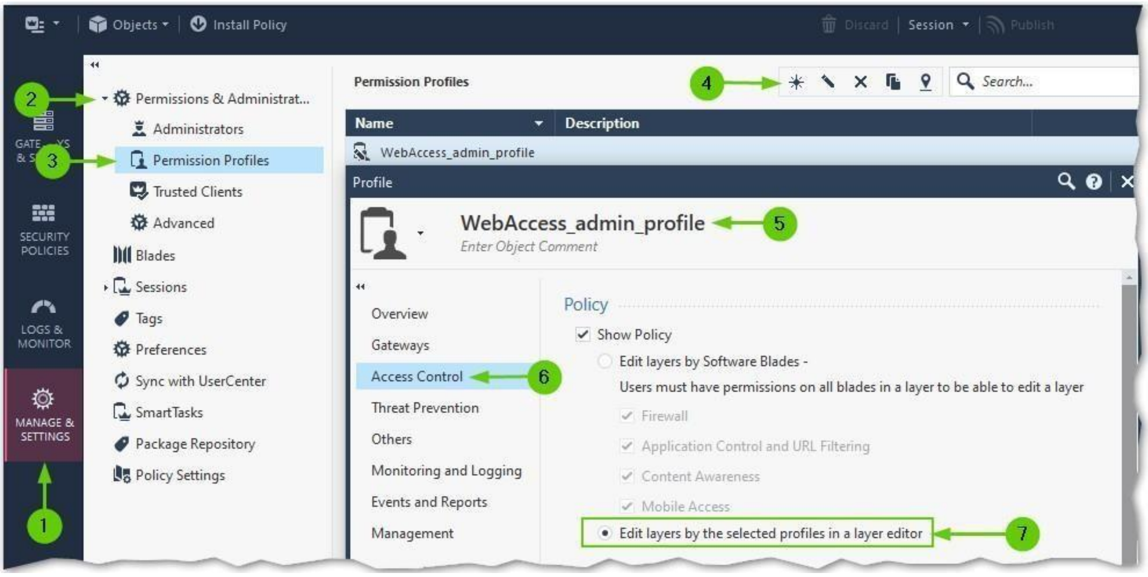
□ VPN Traditional mode

1	Firewall_Policy_Layer	Blades:
2	WebAccess_Policy_Lay	Blades:





No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Time	Track	Install On
WebAccess (8)										
8	0	Internal Zone to Internet	InternalZone	Internet	Any	http https	Drop			Policy Targe
										Policy Targe



Permission Profiles

Name	Description
WebAccess_admin_profile	

Profile

WebAccess_admin_profile
Enter Object Comment

Policy

☑ Show Policy

○ Edit layers by Software Blades -

Users must have permissions on all blades in a layer to be able to edit a layer

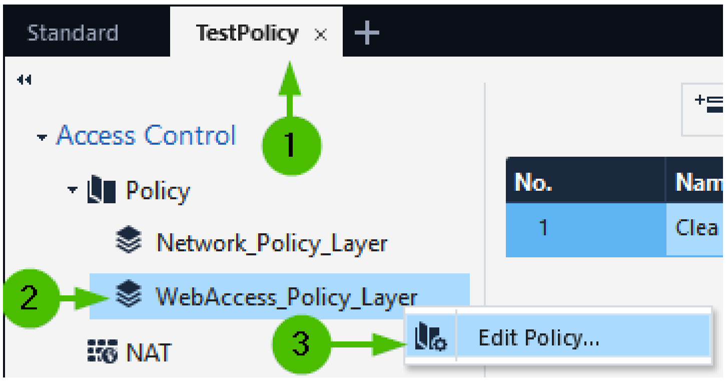
☑ Firewall

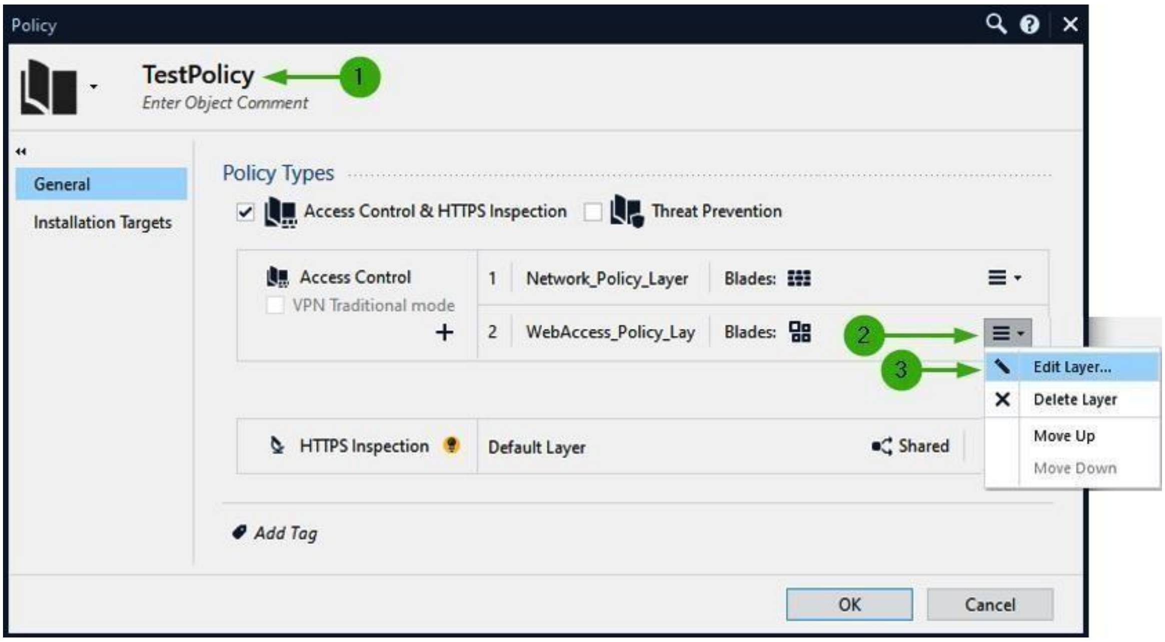
☑ Application Control and URL Filtering

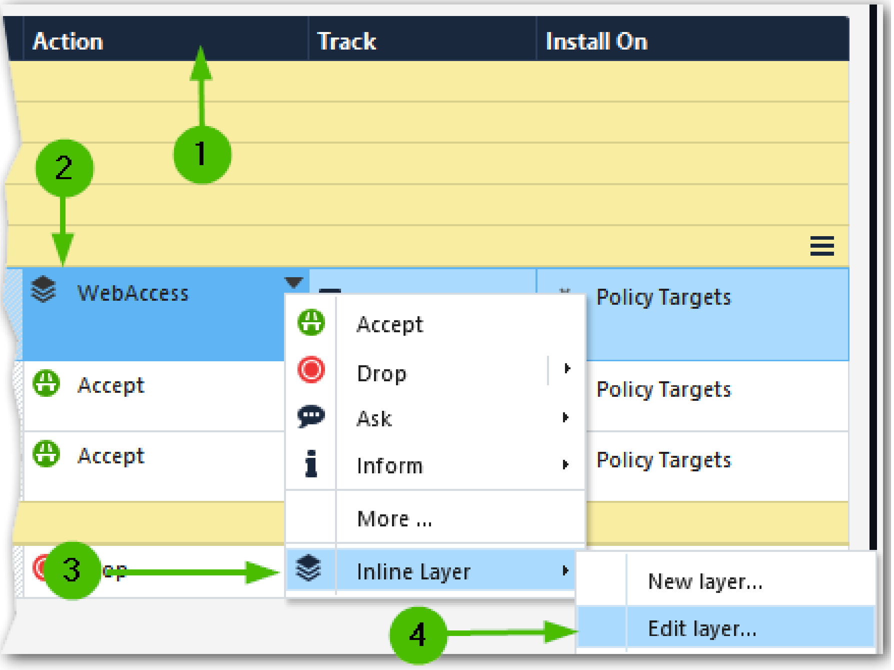
☑ Content Awareness

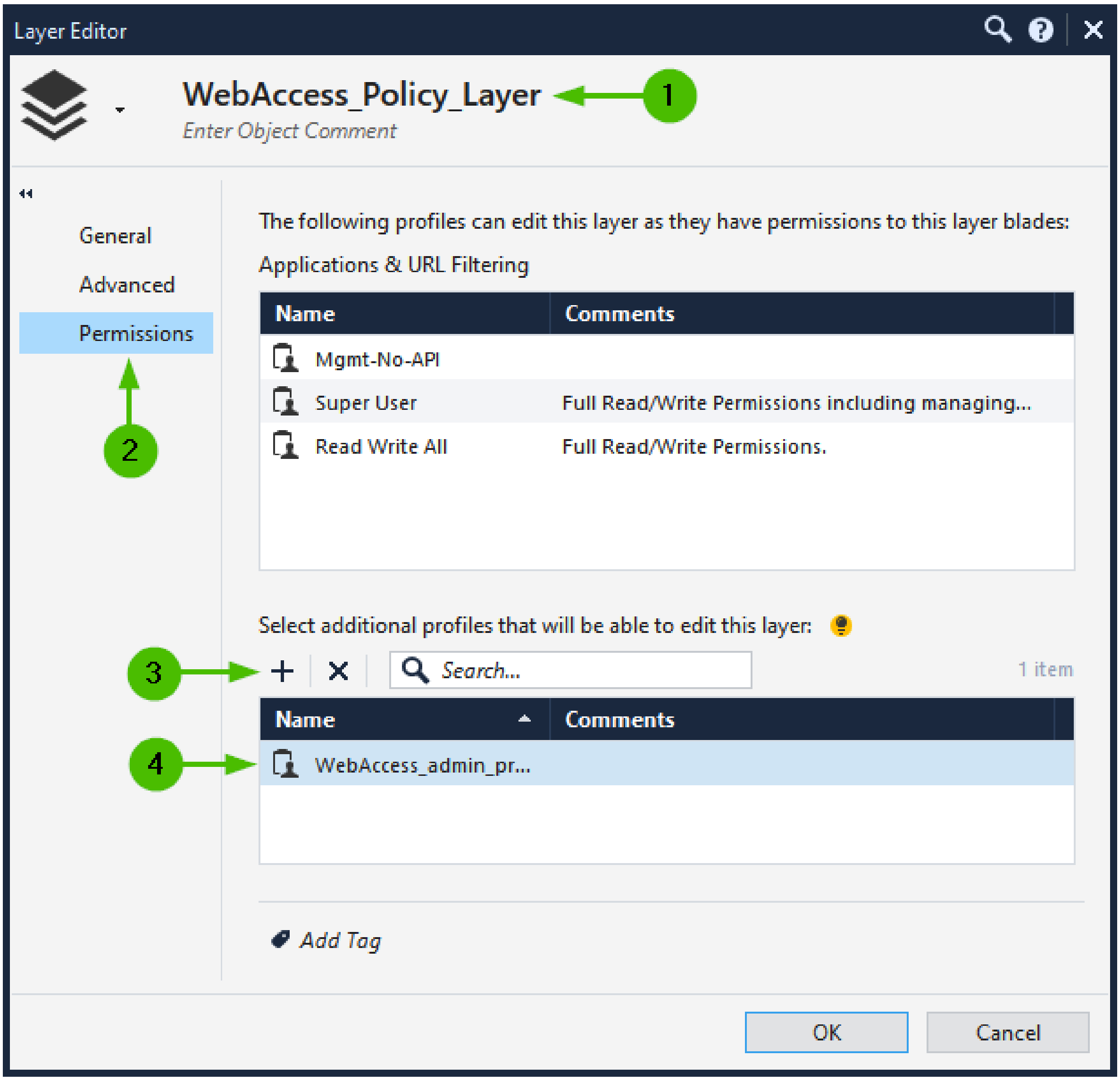
☑ Mobile Access

● Edit layers by the selected profiles in a layer editor


Standard
TestPolicy ×
1
Access Control
Policy
Network_Policy_Layer
2
WebAccess_Policy_Layer
NAT
3
Edit Policy...
No.
Nam
1
Clea


Policy
TestPolicy
1
Enter Object Comment
General
Installation Targets
Policy Types
☑ Access Control & HTTPS Inspection
□ Threat Prevention
Access Control
□ VPN Traditional mode
+
1
Network_Policy_Layer
Blades:
2
WebAccess_Policy_Lay
Blades:
2
3
Edit Layer...
Delete Layer
Move Up
Move Down
HTTPS Inspection
Default Layer
Shared
Add Tag
OK
Cancel





WebAccess_Policy_Layer

Enter Object Comment

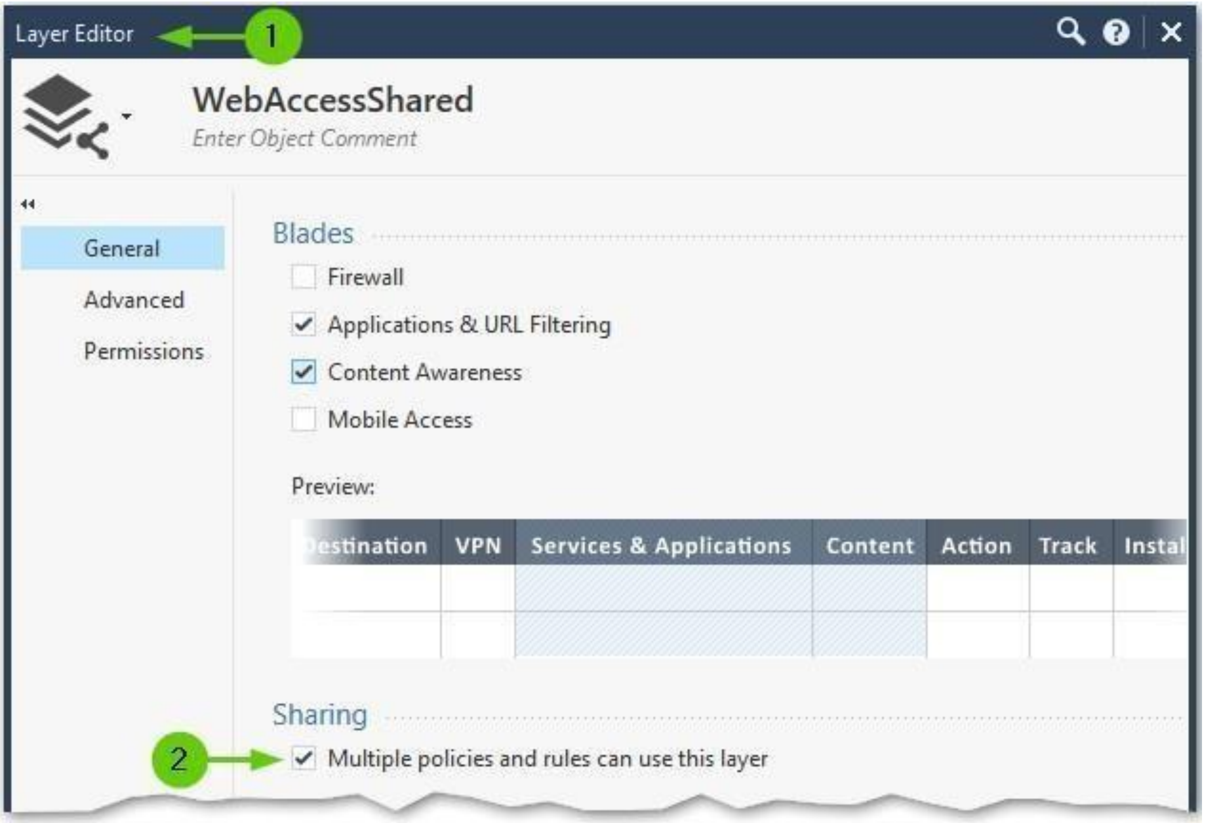
The following profiles can edit this layer as they have permissions to this layer blades:

Applications & URL Filtering

Name	Comments
Mgmt-No-API	
Super User	Full Read/Write Permissions including managing...
Read Write All	Full Read/Write Permissions.

Select additional profiles that will be able to edit this layer:

Name	Comments
WebAccess_admin_pr...	



WebAccessShared

Enter Object Comment

General | Advanced | Permissions

Blades

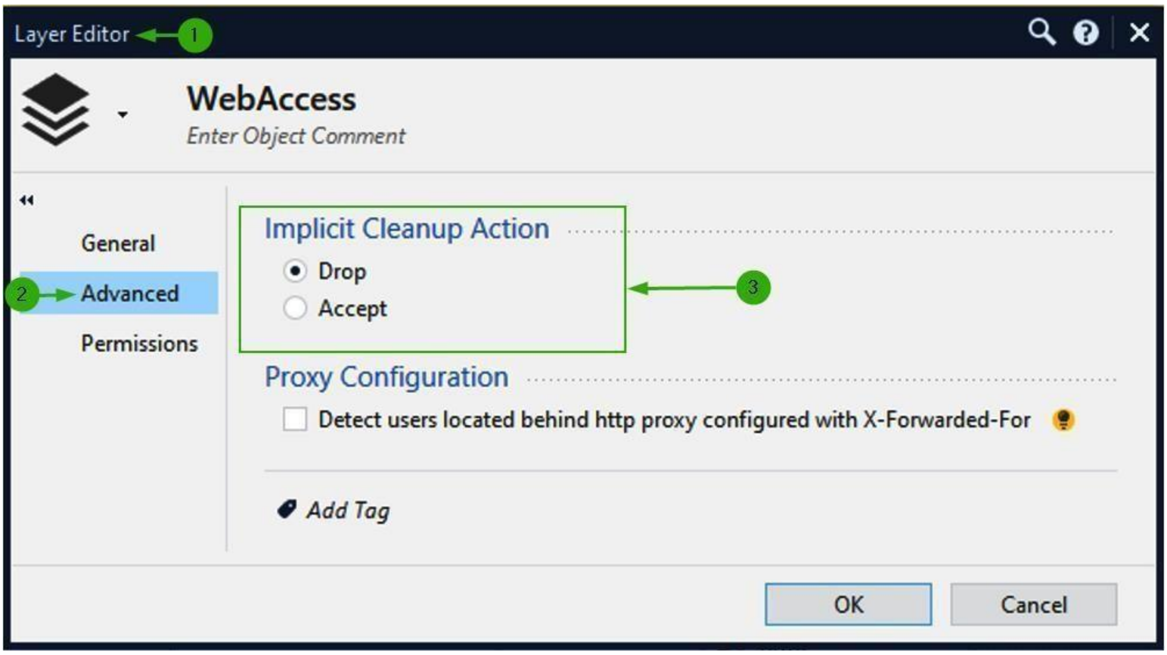
- ☐ Firewall
- ☑ Applications & URL Filtering
- ☑ Content Awareness
- ☐ Mobile Access

Preview:

Destination	VPN	Services & Applications	Content	Action	Track	Instal

Sharing

- ☑ Multiple policies and rules can use this layer



WebAccess

Enter Object Comment

General | Advanced | Permissions

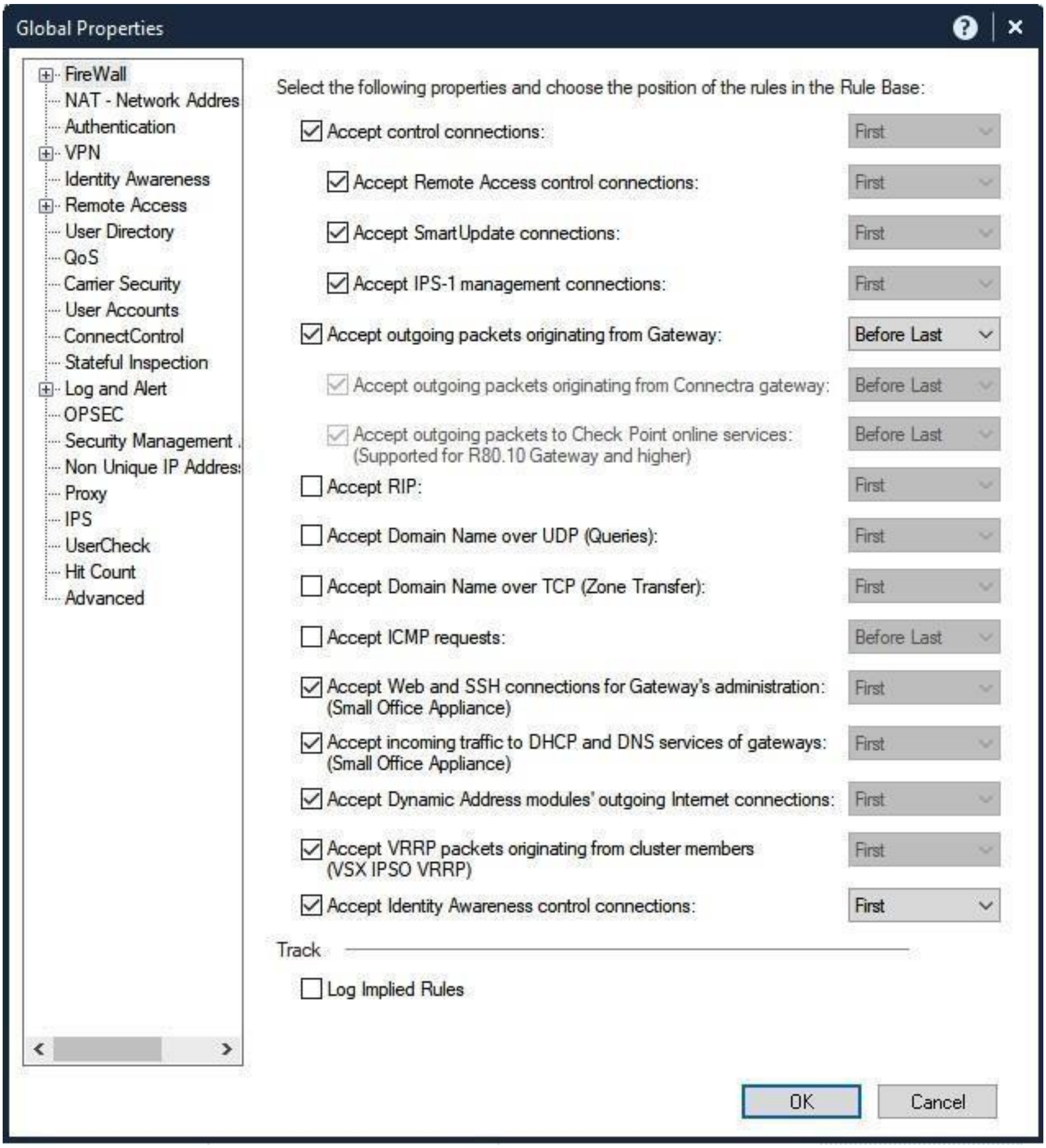
Implicit Cleanup Action

- ● Drop
- ○ Accept

Proxy Configuration

- ☐ Detect users located behind http proxy configured with X-Forwarded-For

Add Tag

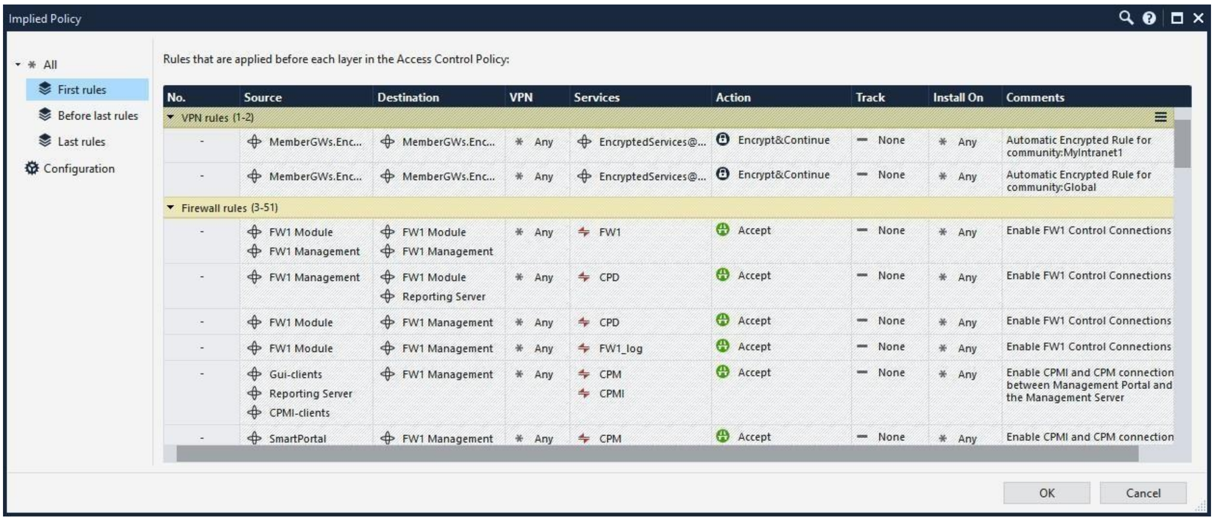


Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept control connections:	First
☑ Accept Remote Access control connections:	First
☑ Accept SmartUpdate connections:	First
☑ Accept IPS-1 management connections:	First
☑ Accept outgoing packets originating from Gateway:	Before Last
☑ Accept outgoing packets originating from Connectra gateway:	Before Last
☑ Accept outgoing packets to Check Point online services: (Supported for R80.10 Gateway and higher)	Before Last
□ Accept RIP:	First
□ Accept Domain Name over UDP (Queries):	First
□ Accept Domain Name over TCP (Zone Transfer):	First
□ Accept ICMP requests:	Before Last
☑ Accept Web and SSH connections for Gateway's administration: (Small Office Appliance)	First
☑ Accept incoming traffic to DHCP and DNS services of gateways: (Small Office Appliance)	First
☑ Accept Dynamic Address modules' outgoing Internet connections:	First
☑ Accept VRRP packets originating from cluster members (VSX IPSO VRRP)	First
☑ Accept Identity Awareness control connections:	First

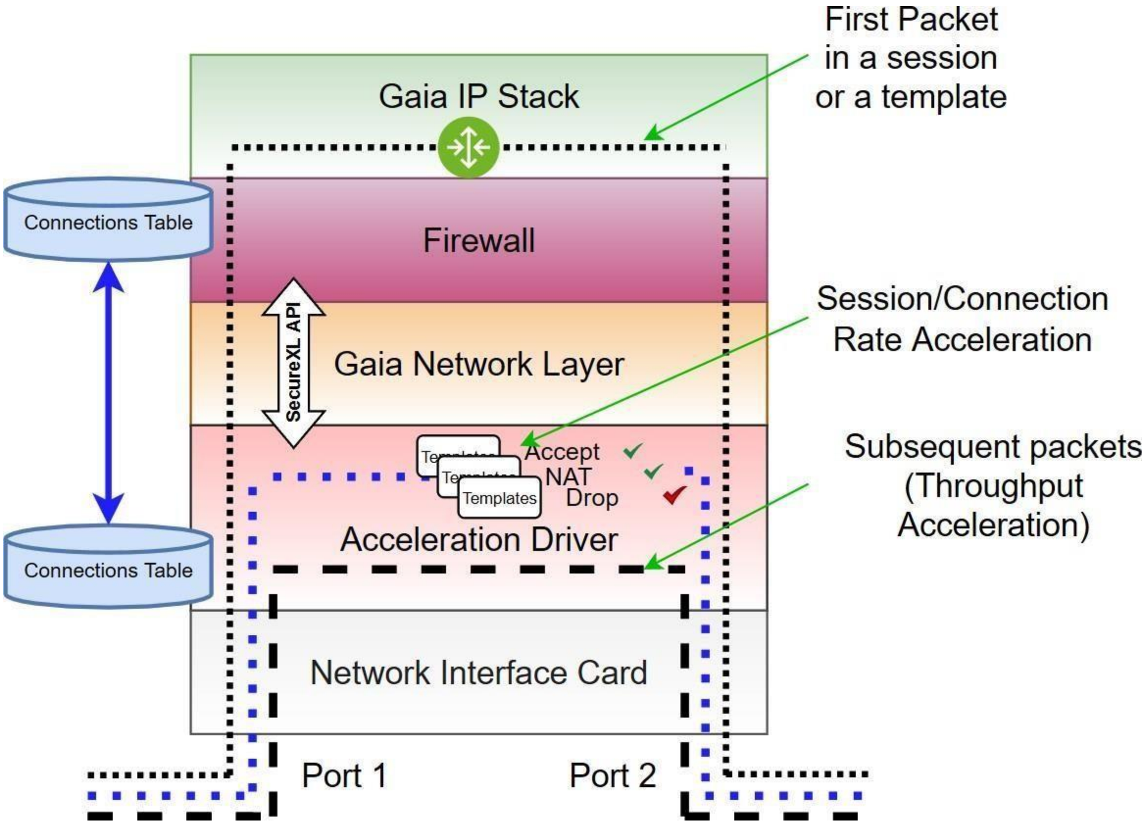
Track

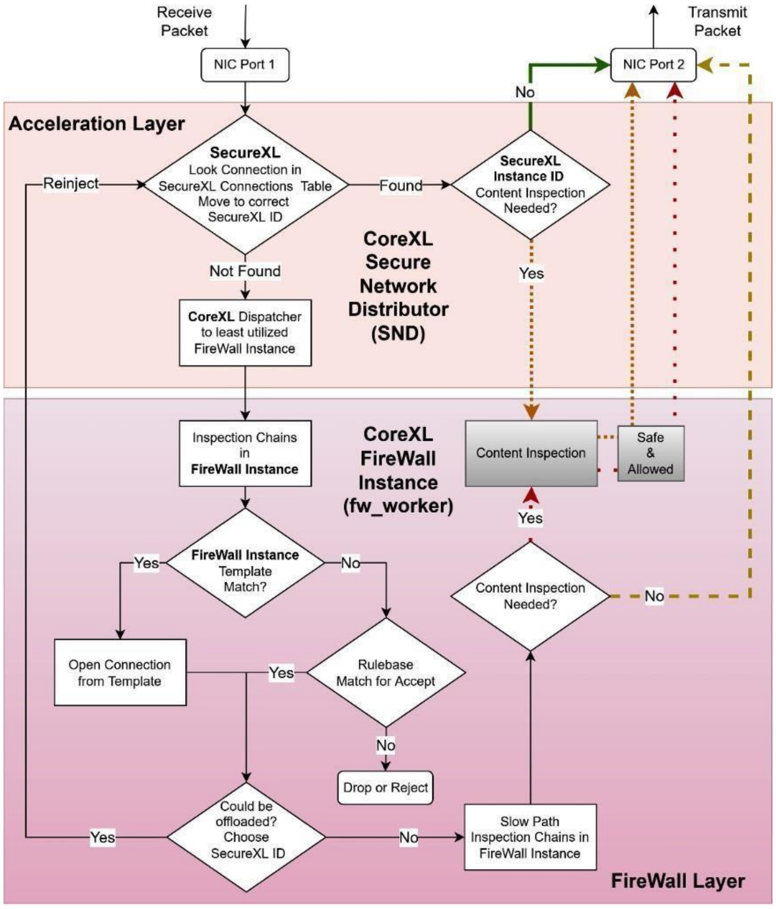
□ Log Implied Rules

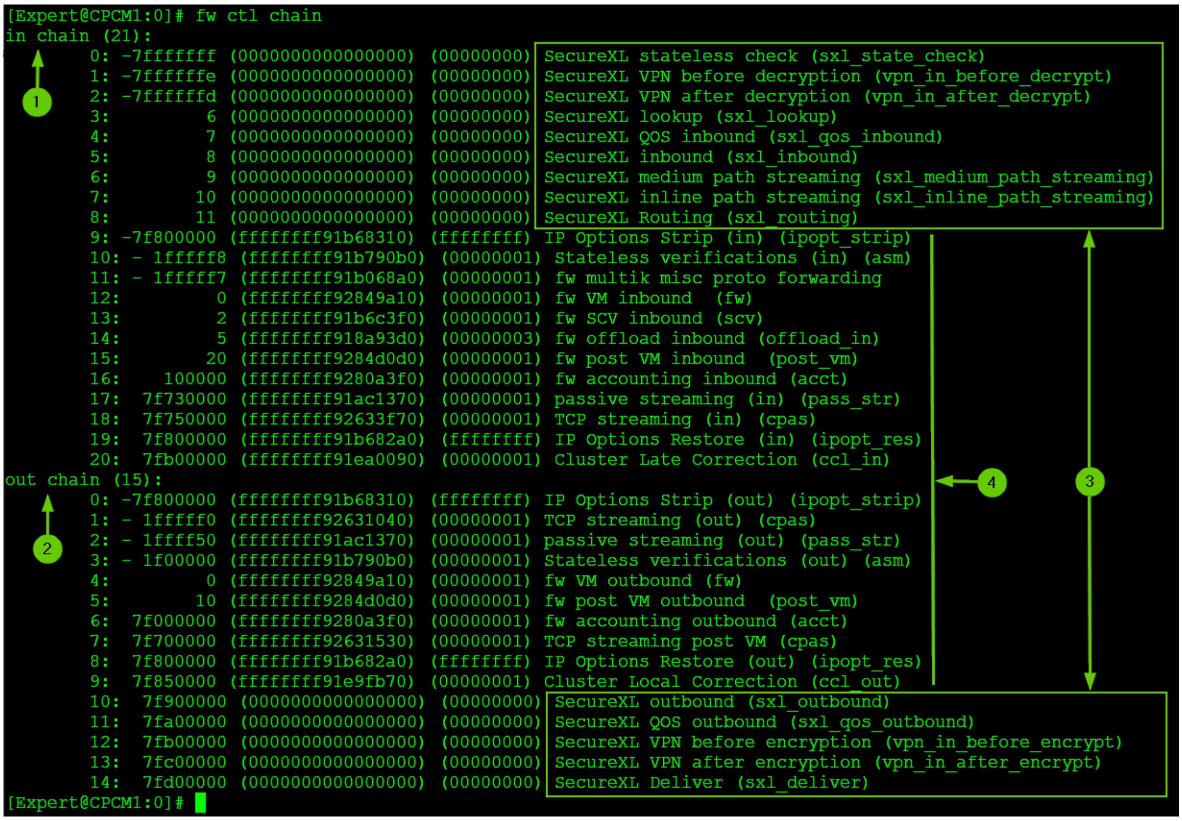


Rules that are applied before each layer in the Access Control Policy:

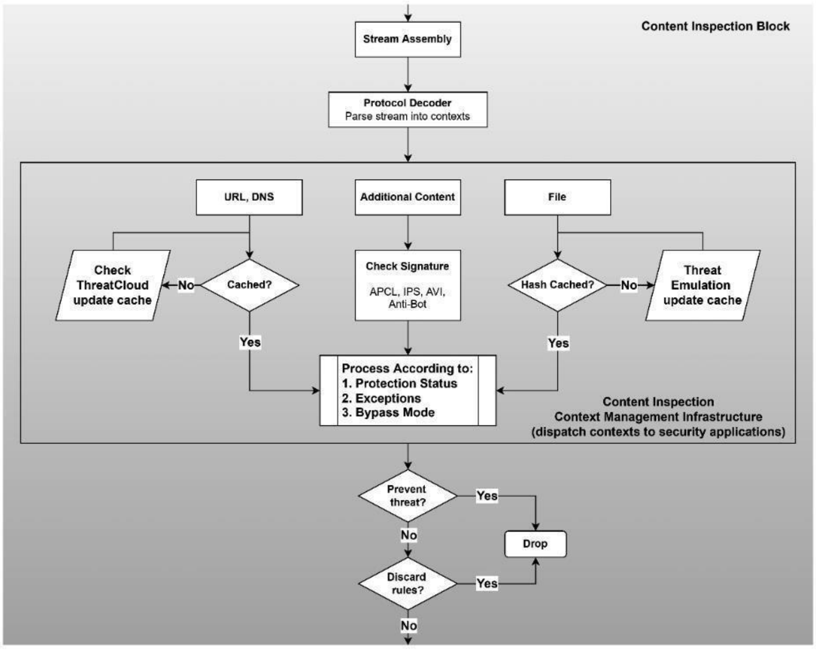
No.	Source	Destination	VPN	Services	Action	Track	Install On	Comments
VPN rules (1-2)								
-	MemberGWs.Enc...	MemberGWs.Enc...	Any	EncryptedServices@...	Encrypt&Continue	None	Any	Automatic Encrypted Rule for community:MyIntranet1
-	MemberGWs.Enc...	MemberGWs.Enc...	Any	EncryptedServices@...	Encrypt&Continue	None	Any	Automatic Encrypted Rule for community:Global
Firewall rules (3-51)								
-	FW1 Module FW1 Management	FW1 Module FW1 Management	Any	FW1	Accept	None	Any	Enable FW1 Control Connections
-	FW1 Management	FW1 Module Reporting Server	Any	CPD	Accept	None	Any	Enable FW1 Control Connections
-	FW1 Module	FW1 Management	Any	CPD	Accept	None	Any	Enable FW1 Control Connections
-	FW1 Module	FW1 Management	Any	FW1_log	Accept	None	Any	Enable FW1 Control Connections
-	Gui-clients Reporting Server CPMI-clients	FW1 Management	Any	CPM CPMI	Accept	None	Any	Enable CPMI and CPM connection between Management Portal and the Management Server
-	SmartPortal	FW1 Management	Any	CPM	Accept	None	Any	Enable CPMI and CPM connection

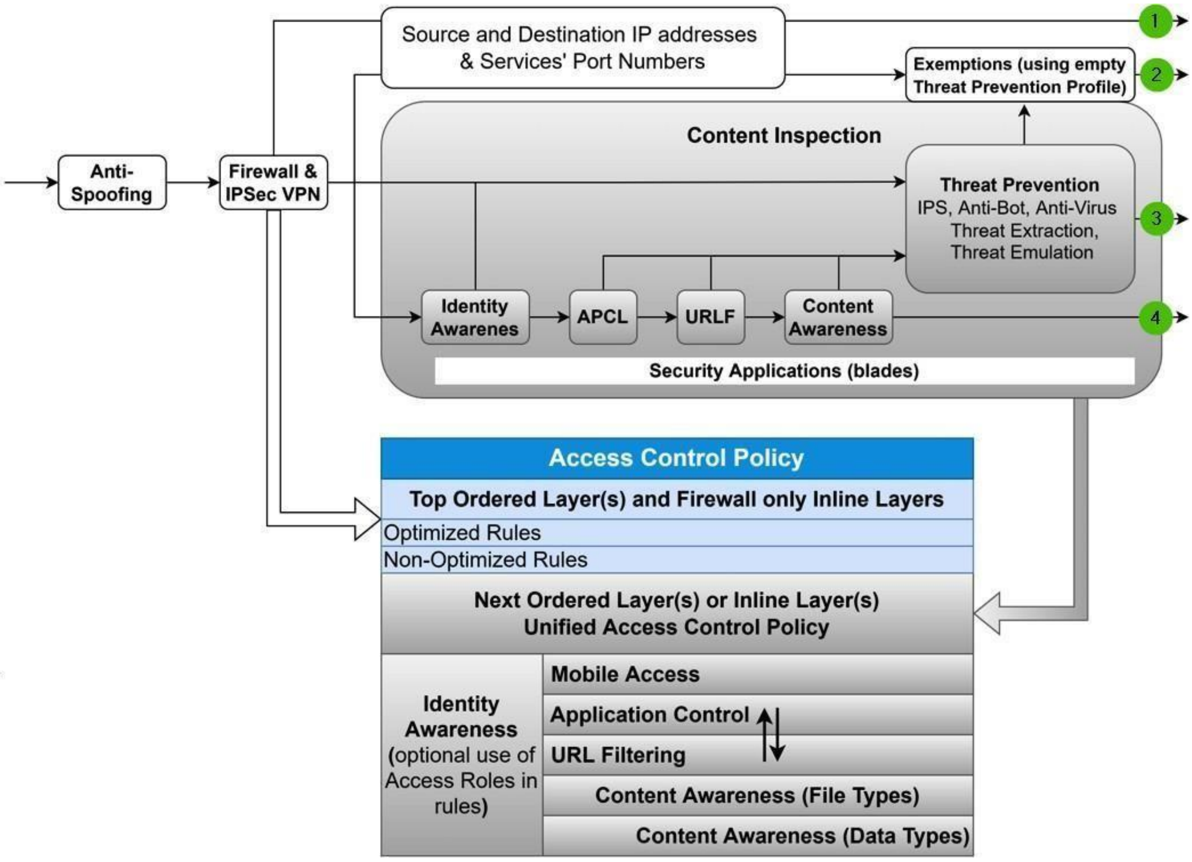


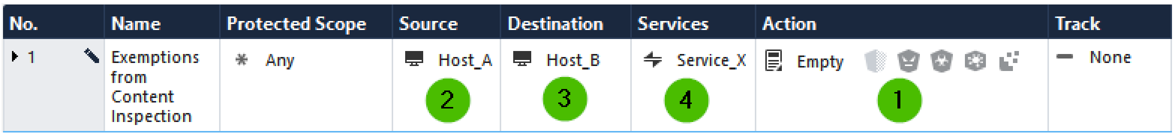

Receive Packet
Transmit Packet
NIC Port 1
NIC Port 2
Acceleration Layer
SecureXL Look Connection in SecureXL Connections Table Move to correct SecureXL ID
Reinject
Found
No
SecureXL Instance ID Content Inspection Needed?
Yes
Not Found
CoreXL Secure Network Distributor (SND)
CoreXL Dispatcher to least utilized FireWall Instance
Inspection Chains in FireWall Instance
CoreXL FireWall Instance (fw_worker)
Content Inspection
Safe & Allowed
Yes
FireWall Instance Template Match?
Yes
No
Content Inspection Needed?
No
Open Connection from Template
Yes
Rulebase Match for Accept
No
Drop or Reject
Yes
Could be offloaded? Choose SecureXL ID
No
Slow Path Inspection Chains in FireWall Instance
FireWall Layer



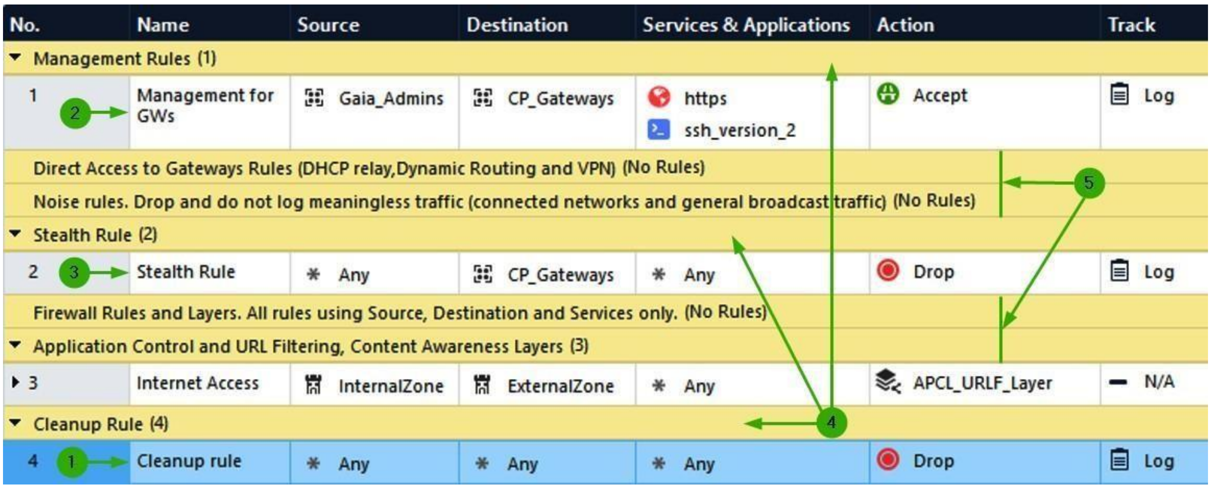
```
[Expert@CPCM1:0]# fw ctl chain
in chain (21):
        0: -7fffffff (0000000000000000) (00000000) SecureXL stateless check (sxl_state_check)
        1: -7ffffffe (0000000000000000) (00000000) SecureXL VPN before decryption (vpn_in_before_decrypt)
        2: -7ffffffd (0000000000000000) (00000000) SecureXL VPN after decryption (vpn_in_after_decrypt)
        3:         6 (0000000000000000) (00000000) SecureXL lookup (sxl_lookup)
        4:         7 (0000000000000000) (00000000) SecureXL QOS inbound (sxl_qos_inbound)
        5:         8 (0000000000000000) (00000000) SecureXL inbound (sxl_inbound)
        6:         9 (0000000000000000) (00000000) SecureXL medium path streaming (sxl_medium_path_streaming)
        7:        10 (0000000000000000) (00000000) SecureXL inline path streaming (sxl_inline_path_streaming)
        8:        11 (0000000000000000) (00000000) SecureXL Routing (sxl_routing)
        9: -7f800000 (ffffffff91b68310) (ffffffff) IP Options Strip (in) (ipopt_strip)
        10: - 1ffffff8 (ffffffff91b790b0) (00000001) Stateless verifications (in) (asm)
        11: - 1ffffff7 (ffffffff91b068a0) (00000001) fw multik misc proto forwarding
        12:         0 (ffffffff92849a10) (00000001) fw VM inbound  (fw)
        13:         2 (ffffffff91b6c3f0) (00000001) fw SCV inbound (scv)
        14:         5 (ffffffff918a93d0) (00000003) fw offload inbound (offload_in)
        15:        20 (ffffffff9284d0d0) (00000001) fw post VM inbound  (post_vm)
        16:    100000 (ffffffff9280a3f0) (00000001) fw accounting inbound (acct)
        17:  7f730000 (ffffffff91ac1370) (00000001) passive streaming (in) (pass_str)
        18:  7f750000 (ffffffff92633f70) (00000001) TCP streaming (in) (cpas)
        19:  7f800000 (ffffffff91b682a0) (ffffffff) IP Options Restore (in) (ipopt_res)
        20:  7fb00000 (ffffffff91ea0090) (00000001) Cluster Late Correction (ccl_in)
out chain (15):
        0: -7f800000 (ffffffff91b68310) (ffffffff) IP Options Strip (out) (ipopt_strip)
        1: - 1ffffff0 (ffffffff92631040) (00000001) TCP streaming (out) (cpas)
        2: - 1ffff50 (ffffffff91ac1370) (00000001) passive streaming (out) (pass_str)
        3: - 1f00000 (ffffffff91b790b0) (00000001) Stateless verifications (out) (asm)
        4:         0 (ffffffff92849a10) (00000001) fw VM outbound (fw)
        5:        10 (ffffffff9284d0d0) (00000001) fw post VM outbound  (post_vm)
        6:  7f000000 (ffffffff9280a3f0) (00000001) fw accounting outbound (acct)
        7:  7f700000 (ffffffff92631530) (00000001) TCP streaming post VM (cpas)
        8:  7f800000 (ffffffff91b682a0) (ffffffff) IP Options Restore (out) (ipopt_res)
        9:  7f850000 (ffffffff91e9fb70) (00000001) Cluster Local Correction (ccl_out)
        10:  7f900000 (0000000000000000) (00000000) SecureXL outbound (sxl_outbound)
        11:  7fa00000 (0000000000000000) (00000000) SecureXL QOS outbound (sxl_qos_outbound)
        12:  7fb00000 (0000000000000000) (00000000) SecureXL VPN before encryption (vpn_in_before_encrypt)
        13:  7fc00000 (0000000000000000) (00000000) SecureXL VPN after encryption (vpn_in_after_encrypt)
        14:  7fd00000 (0000000000000000) (00000000) SecureXL Deliver (sxl_deliver)
[Expert@CPCM1:0]#
```



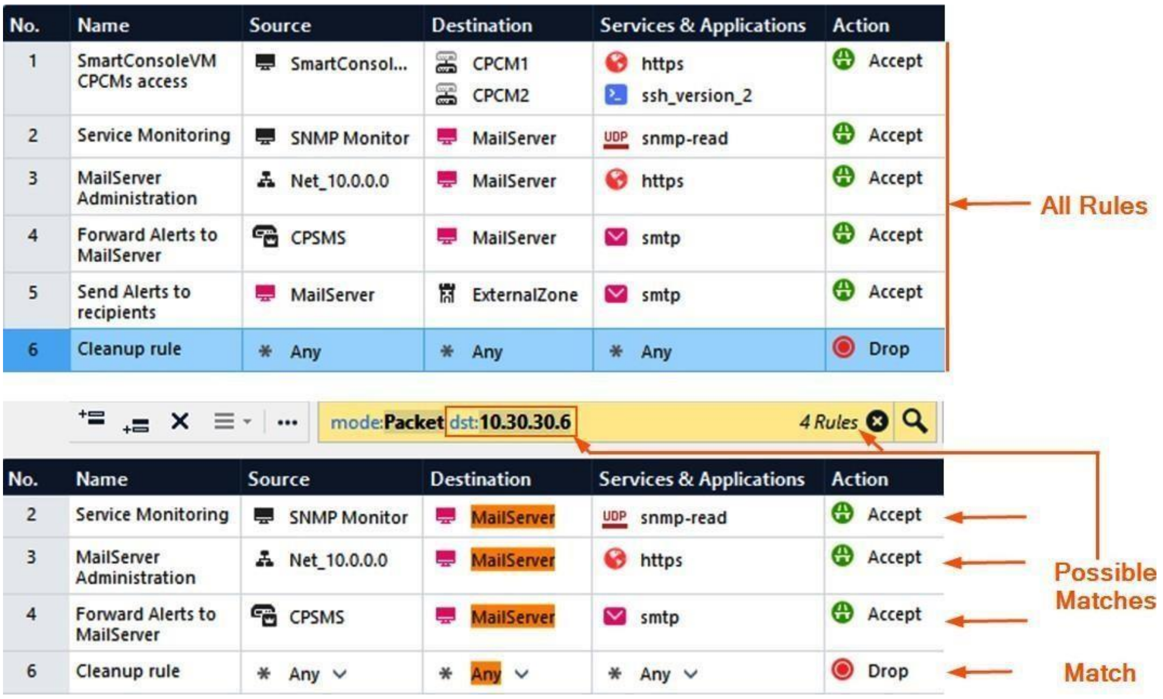

Source and Destination IP addresses & Services' Port Numbers
1
Exemptions (using empty Threat Prevention Profile)
2
Anti-Spoofing
Firewall & IPSec VPN
Content Inspection
Threat Prevention
IPS, Anti-Bot, Anti-Virus
Threat Extraction,
Threat Emulation
3
Identity Awarenes
APCL
URLF
Content Awareness
4
Security Applications (blades)
Access Control Policy
Top Ordered Layer(s) and Firewall only Inline Layers
Optimized Rules
Non-Optimized Rules
Next Ordered Layer(s) or Inline Layer(s)
Unified Access Control Policy
Identity Awareness (optional use of Access Roles in rules)
Mobile Access
Application Control
URL Filtering
Content Awareness (File Types)
Content Awareness (Data Types)



No.	Name	Protected Scope	Source	Destination	Services	Action	Track
1	Exemptions from Content Inspection	Any	Host_A 2	Host_B 3	Service_X 4	Empty 1	None



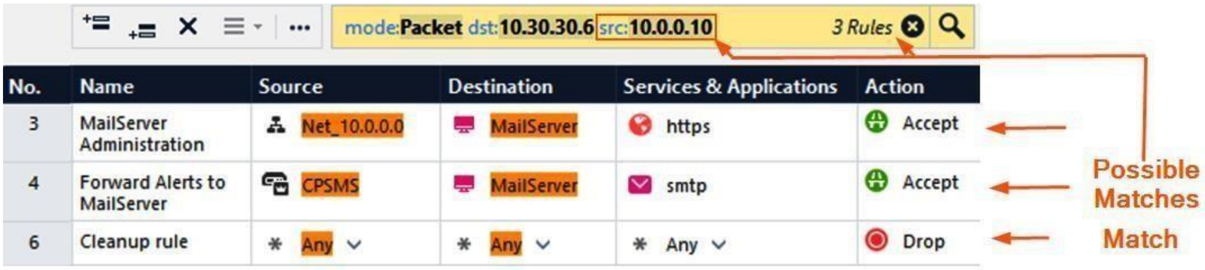
No.	Name	Source	Destination	Services & Applications	Action	Track
Management Rules (1)						
1	Management for GWs	Gaia_Admins	CP_Gateways	https ssh_version_2	Accept	Log
Direct Access to Gateways Rules (DHCP relay,Dynamic Routing and VPN) (No Rules)						
Noise rules. Drop and do not log meaningless traffic (connected networks and general broadcast traffic) (No Rules)						
Stealth Rule (2)						
2	Stealth Rule	Any	CP_Gateways	Any	Drop	Log
Firewall Rules and Layers. All rules using Source, Destination and Services only. (No Rules)						
Application Control and URL Filtering, Content Awareness Layers (3)						
3	Internet Access	InternalZone	ExternalZone	Any	APCL_URLF_Layer	N/A
Cleanup Rule (4)						
4	Cleanup rule	Any	Any	Any	Drop	Log



No.	Name	Source	Destination	Services & Applications	Action
1	SmartConsoleVM CPCMs access	SmartConsol...	CPCM1 CPCM2	https ssh_version_2	Accept
2	Service Monitoring	SNMP Monitor	MailServer	snmp-read	Accept
3	MailServer Administration	Net_10.0.0.0	MailServer	https	Accept
4	Forward Alerts to MailServer	CPSMS	MailServer	smtp	Accept
5	Send Alerts to recipients	MailServer	ExternalZone	smtp	Accept
6	Cleanup rule	Any	Any	Any	Drop

mode:Packet dst:10.30.30.6 4 Rules

No.	Name	Source	Destination	Services & Applications	Action
2	Service Monitoring	SNMP Monitor	MailServer	snmp-read	Accept
3	MailServer Administration	Net_10.0.0.0	MailServer	https	Accept
4	Forward Alerts to MailServer	CPSMS	MailServer	smtp	Accept
6	Cleanup rule	Any	Any	Any	Drop

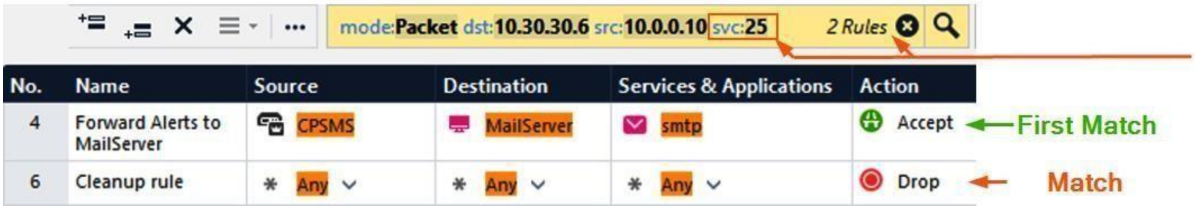


mode:Packet dst:10.30.30.6 src:10.0.0.10 — 3 Rules

No.	Name	Source	Destination	Services & Applications	Action
3	MailServer Administration	Net_10.0.0.0	MailServer	https	Accept
4	Forward Alerts to MailServer	CPSMS	MailServer	smtp	Accept
6	Cleanup rule	* Any	* Any	* Any	Drop

Possible Matches

Match

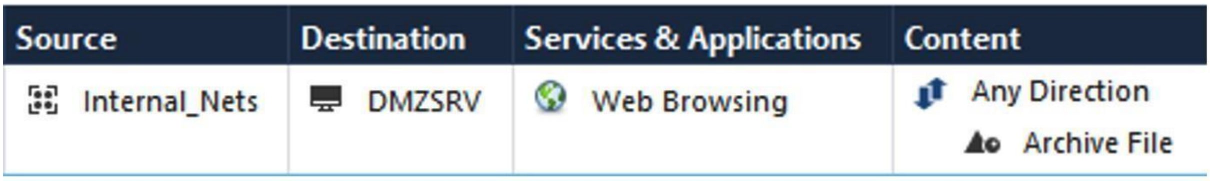


mode:Packet dst:10.30.30.6 src:10.0.0.10 svc:25 — 2 Rules

No.	Name	Source	Destination	Services & Applications	Action
4	Forward Alerts to MailServer	CPSMS	MailServer	smtp	Accept
6	Cleanup rule	* Any	* Any	* Any	Drop

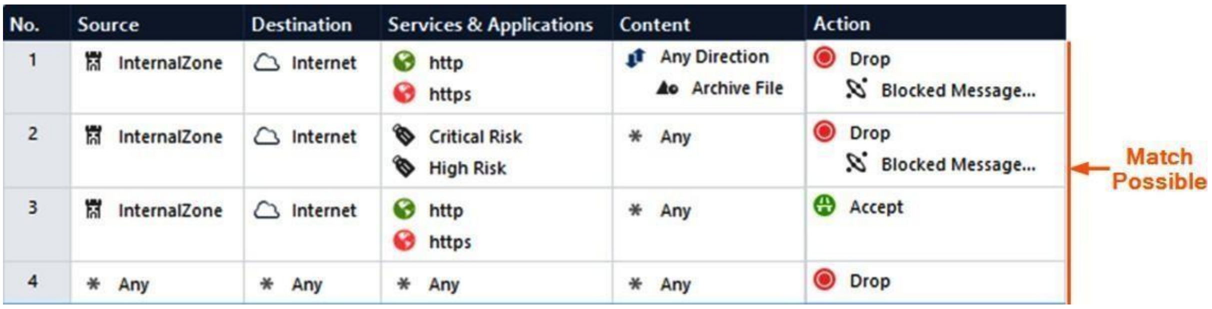
First Match

Match



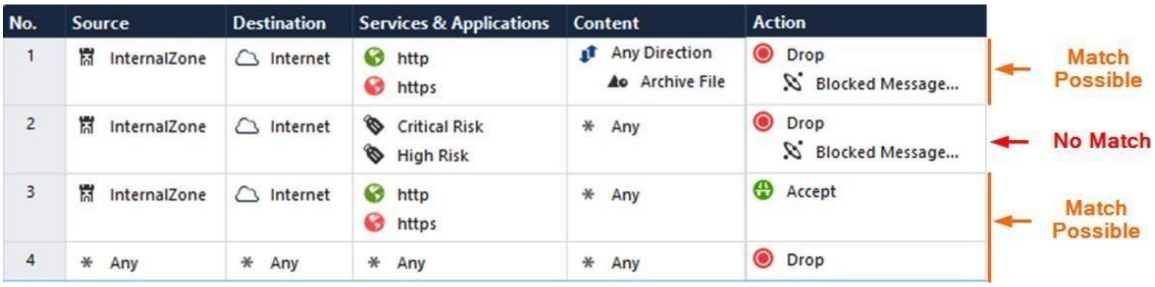
Source	Destination	Services & Applications	Content
Internal_Nets	DMZSRV	Web Browsing	Any Direction Archive File

Source Access Roles Destination User at Location Mobile Access Application	Service Application Protocol	File Content Direction



No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	http https	Any Direction Archive File	Drop Blocked Message...
2	InternalZone	Internet	Critical Risk High Risk	* Any	Drop Blocked Message...
3	InternalZone	Internet	http https	* Any	Accept
4	* Any	* Any	* Any	* Any	Drop

Match Possible

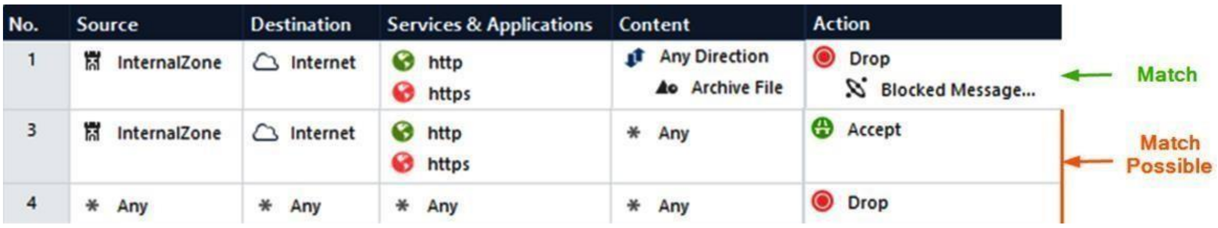


No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	http https	Any Direction Archive File	Drop Blocked Message...
2	InternalZone	Internet	Critical Risk High Risk	* Any	Drop Blocked Message...
3	InternalZone	Internet	http https	* Any	Accept
4	* Any	* Any	* Any	* Any	Drop

Match Possible

No Match

Match Possible



No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	http https	Any Direction Archive File	Drop Blocked Message...
3	InternalZone	Internet	http https	Any	Accept
4	Any	Any	Any	Any	Drop

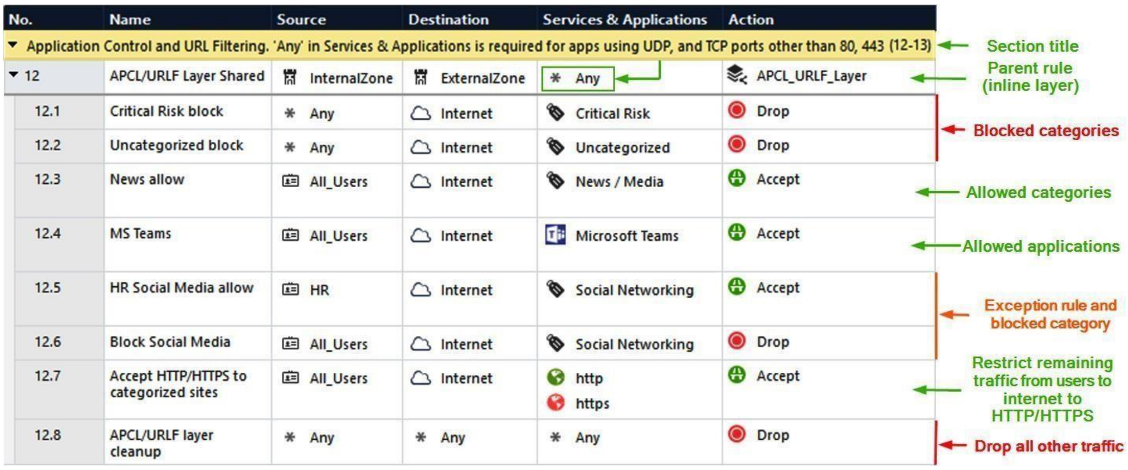
Match

Match Possible

Best Practices for Access Control Rules

1. Make sure you have these rules:
   - Stealth rule that prevents direct access to the Security Gateway
   - Cleanup rule that drops all traffic that is not allowed by the earlier rules in the policy.
2. Use Layers to add structure and hierarchy of rules in the Rule Base.
3. Add all rules that are based only on source and destination IP addresses and ports, in a Firewall/Network Ordered Layer at the top of the Rule Base.
4. Create Firewall/Network rules to explicitly accept safe traffic, and add an *explicit cleanup rule* at the bottom of the Ordered Layer to drop everything else.
5. Create an Application Control Ordered Layer after the Firewall/Network Ordered Layer. Add rules to explicitly drop unwanted or unsafe traffic. Add an explicit cleanup rule at the bottom of the Ordered Layer to accept everything else.

   Alternatively, put Application Control rules in an Inline Layer as part of the Firewall/Network rules. In the parent rule of the Inline Layer, define the Source and Destination.
6. Share Ordered Layers and Inline Layers when possible.
7. For Security Gateways R80.10 and higher: If you have one Ordered Layer for Firewall/Network rules, and another Ordered Layer for Application Control - Add all rules that examine applications, Data Type, or Mobile Access elements, to the Application Control Ordered Layer, or to an Ordered Layer after it.
8. Turn off the XFF inspection, unless the Security Gateway is behind a proxy server. For more, see sk92839.
9. Disable a rule when working on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Security Gateway. To disable a rule, right-click in the **No** column of the rule and select **Disable**.



No.	Name	Source	Destination	Services & Applications	Action
Application Control and URL Filtering. 'Any' in Services & Applications is required for apps using UDP, and TCP ports other than 80, 443 (12-13)					
12	APCL/URLF Layer Shared	InternalZone	ExternalZone	Any	APCL_URLF_Layer
12.1	Critical Risk block	Any	Internet	Critical Risk	Drop
12.2	Uncategorized block	Any	Internet	Uncategorized	Drop
12.3	News allow	All_Users	Internet	News / Media	Accept
12.4	MS Teams	All_Users	Internet	Microsoft Teams	Accept
12.5	HR Social Media allow	HR	Internet	Social Networking	Accept
12.6	Block Social Media	All_Users	Internet	Social Networking	Drop
12.7	Accept HTTP/HTTPS to categorized sites	All_Users	Internet	http https	Accept
12.8	APCL/URLF layer cleanup	Any	Any	Any	Drop

Section title

Parent rule (inline layer)

Blocked categories

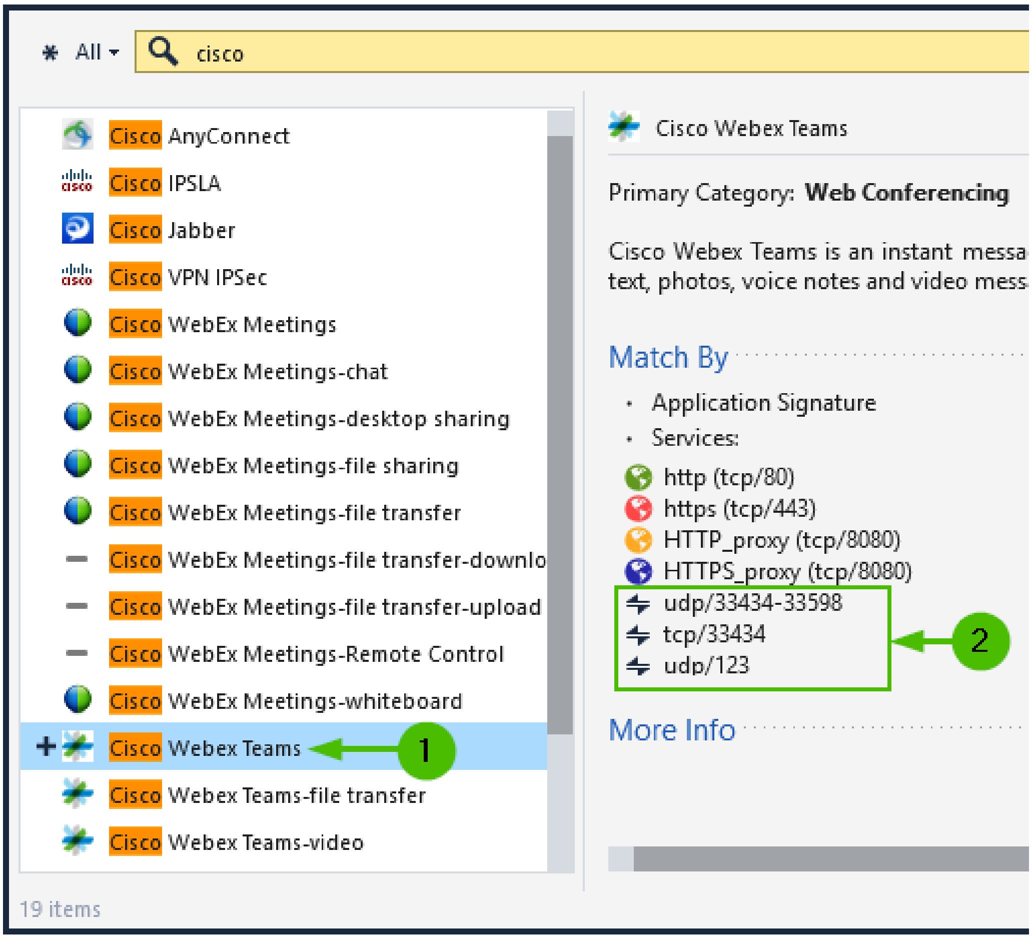
Allowed categories

Allowed applications

Exception rule and blocked category

Restrict remaining traffic from users to internet to HTTP/HTTPS

Drop all other traffic



cisco

- Cisco AnyConnect
- Cisco IPSLA
- Cisco Jabber
- Cisco VPN IPSec
- Cisco WebEx Meetings
- Cisco WebEx Meetings-chat
- Cisco WebEx Meetings-desktop sharing
- Cisco WebEx Meetings-file sharing
- Cisco WebEx Meetings-file transfer
- Cisco WebEx Meetings-file transfer-downlo
- Cisco WebEx Meetings-file transfer-upload
- Cisco WebEx Meetings-Remote Control
- Cisco WebEx Meetings-whiteboard
- Cisco Webex Teams
- Cisco Webex Teams-file transfer
- Cisco Webex Teams-video

19 items

Cisco Webex Teams

Primary Category: **Web Conferencing**

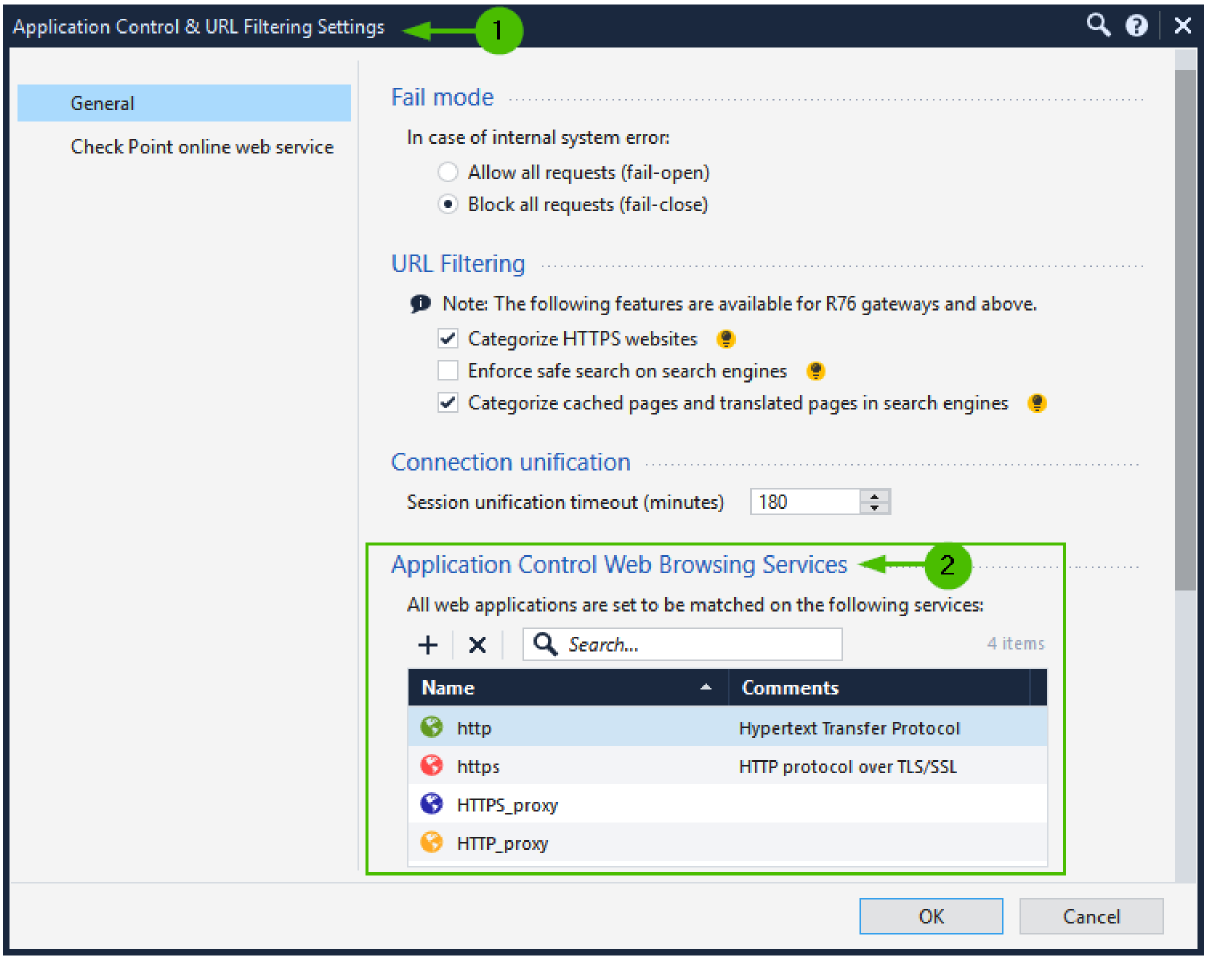
Cisco Webex Teams is an instant messa
text, photos, voice notes and video mess

Match By

- Application Signature
- Services:

http (tcp/80)
https (tcp/443)
HTTP_proxy (tcp/8080)
HTTPS_proxy (tcp/8080)
udp/33434-33598
tcp/33434
udp/123

More Info



Application Control & URL Filtering Settings

General

Check Point online web service

Fail mode

In case of internal system error:

○ Allow all requests (fail-open)
● Block all requests (fail-close)

URL Filtering

Note: The following features are available for R76 gateways and above.

☑ Categorize HTTPS websites
□ Enforce safe search on search engines
☑ Categorize cached pages and translated pages in search engines

Connection unification

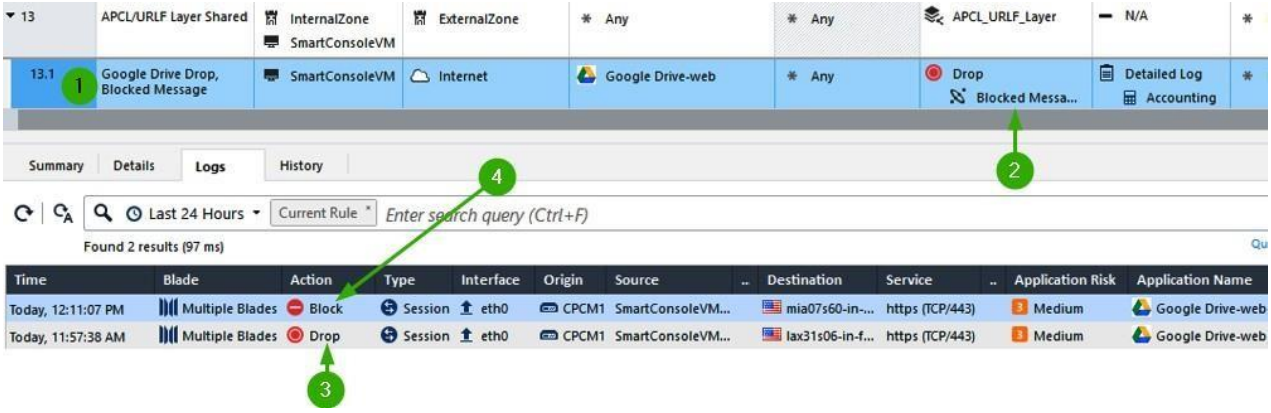
Session unification timeout (minutes) 180

Application Control Web Browsing Services

All web applications are set to be matched on the following services:

Search... 4 items

Name	Comments
http	Hypertext Transfer Protocol
https	HTTP protocol over TLS/SSL
HTTPS_proxy	
HTTP_proxy	

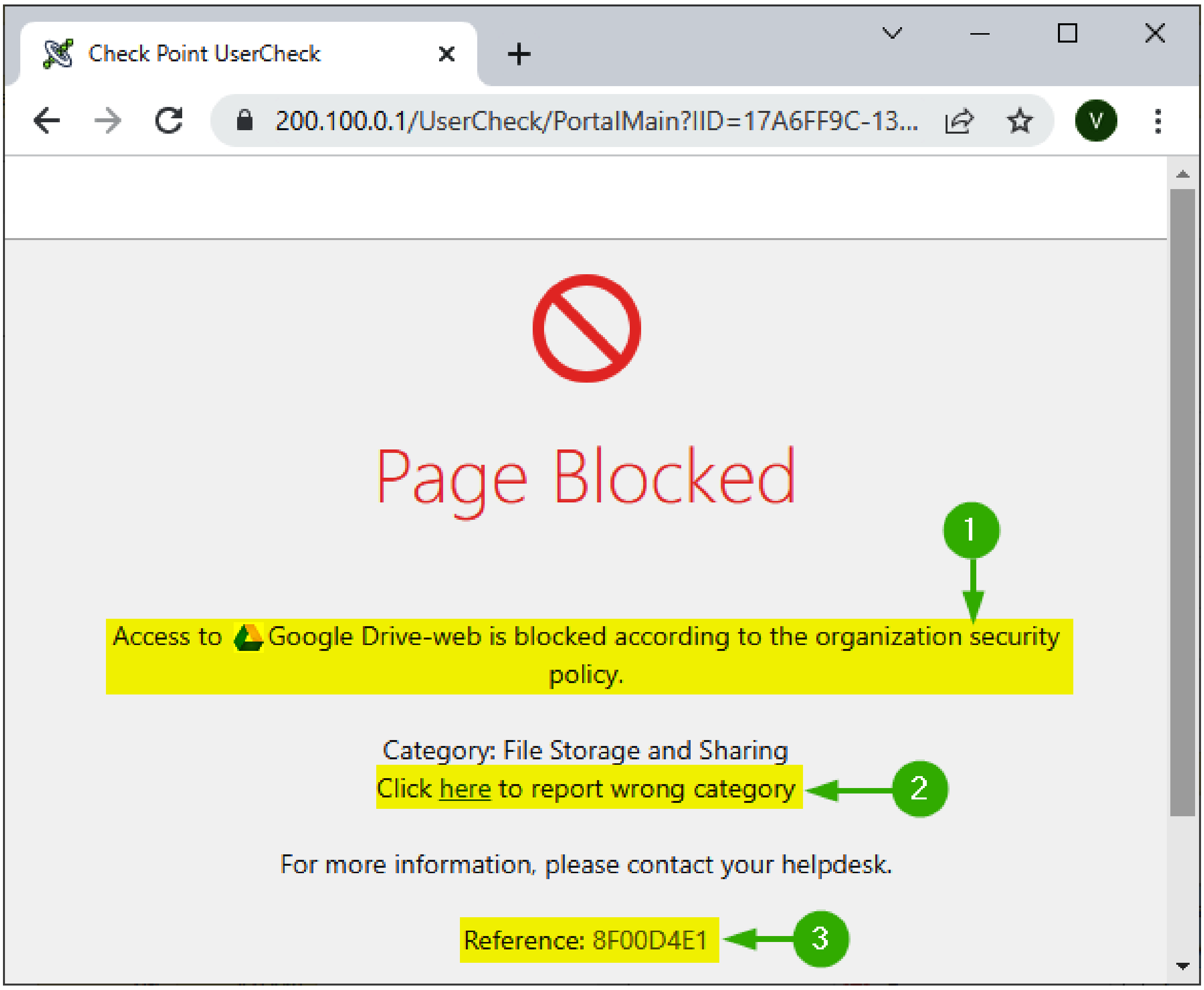


13	APCL/URLF Layer Shared	InternalZone SmartConsoleVM	ExternalZone	Any	Any	APCL_URLF_Layer	N/A	*
13.1	Google Drive Drop, Blocked Message	SmartConsoleVM	Internet	Google Drive-web	Any	Drop Blocked Messa...	Detailed Log Accounting	*

Last 24 Hours | Current Rule | Enter search query (Ctrl+F)

Found 2 results (97 ms)

Time	Blade	Action	Type	Interface	Origin	Source	..	Destination	Service	..	Application Risk	Application Name
Today, 12:11:07 PM	Multiple Blades	Block	Session	eth0	CPCM1	SmartConsoleVM...		mia07s60-in-...	https (TCP/443)		Medium	Google Drive-web
Today, 11:57:38 AM	Multiple Blades	Drop	Session	eth0	CPCM1	SmartConsoleVM...		lax31s06-in-f...	https (TCP/443)		Medium	Google Drive-web



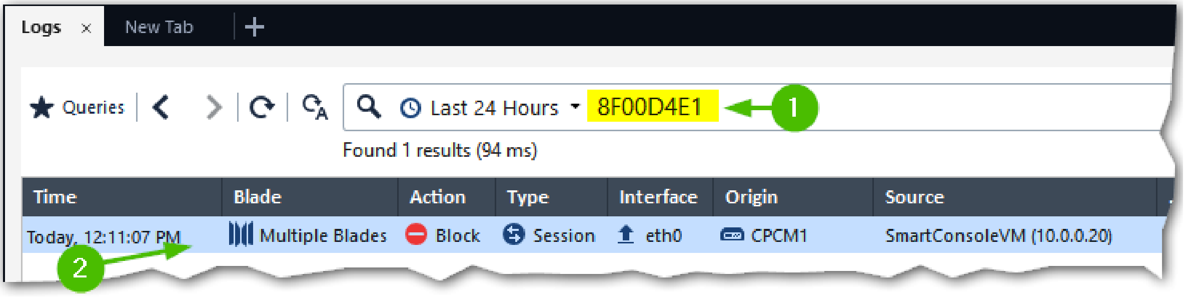
Page Blocked

Access to Google Drive-web is blocked according to the organization security policy.

Category: File Storage and Sharing
Click here to report wrong category

For more information, please contact your helpdesk.

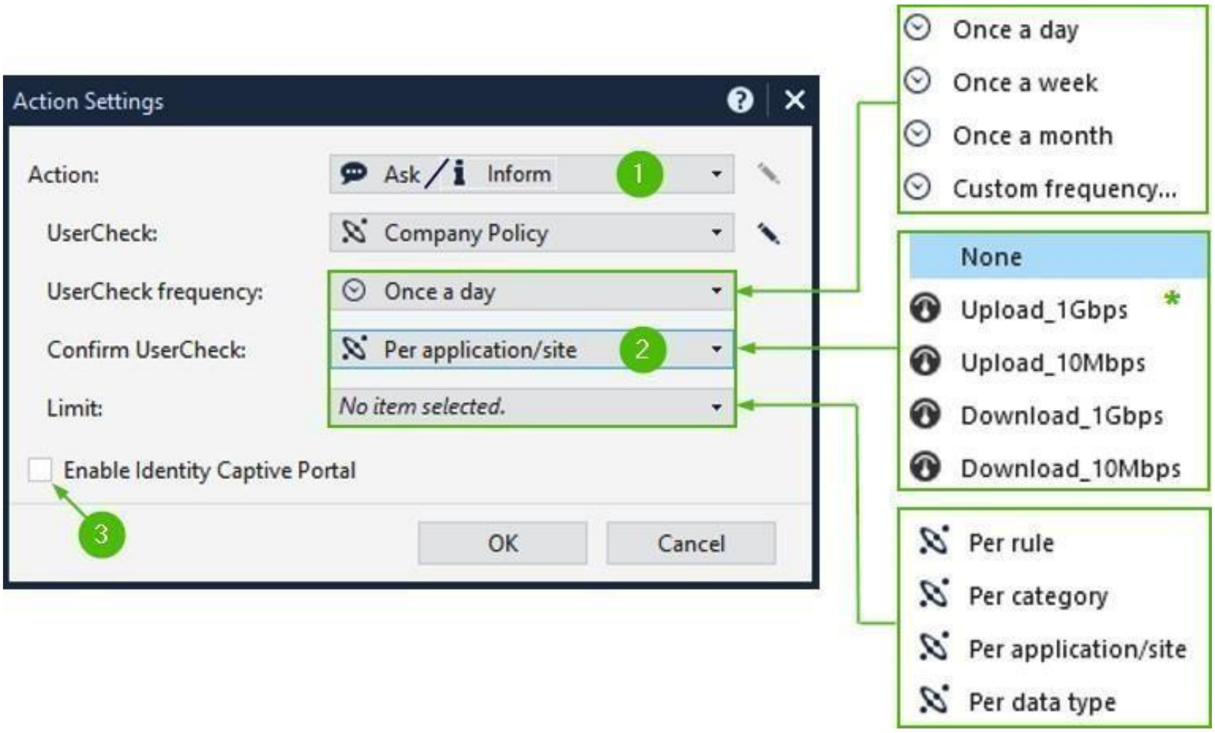
Reference: 8F00D4E1



8F00D4E1

Found 1 results (94 ms)

Time	Blade	Action	Type	Interface	Origin	Source
Today, 12:11:07 PM	Multiple Blades	Block	Session	eth0	CPCM1	SmartConsoleVM (10.0.0.20)



Action Settings

Action: Ask / Inform

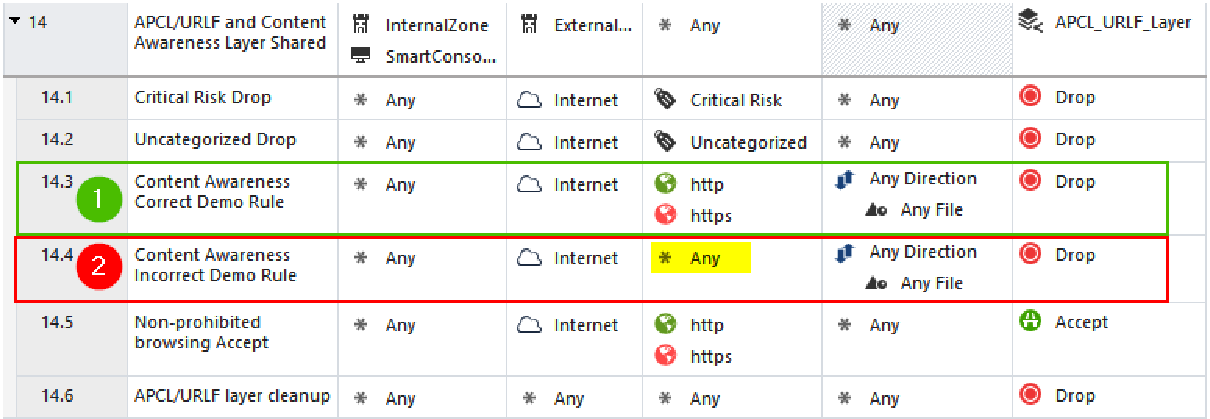
UserCheck: Company Policy

UserCheck frequency: Once a day

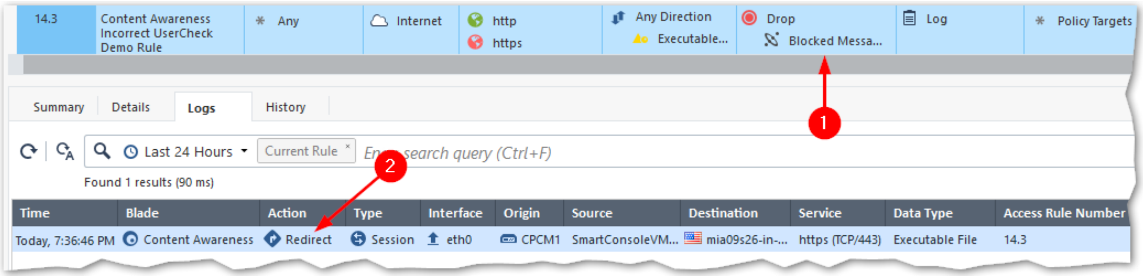
Confirm UserCheck: Per application/site

Limit: *No item selected.*

□ Enable Identity Captive Portal



14	APCL/URLF and Content Awareness Layer Shared	InternalZone SmartConso...	External...	Any	Any	APCL_URLF_Layer
14.1	Critical Risk Drop	Any	Internet	Critical Risk	Any	Drop
14.2	Uncategorized Drop	Any	Internet	Uncategorized	Any	Drop
14.3	Content Awareness Correct Demo Rule	Any	Internet	http https	Any Direction Any File	Drop
14.4	Content Awareness Incorrect Demo Rule	Any	Internet	Any	Any Direction Any File	Drop
14.5	Non-prohibited browsing Accept	Any	Internet	http https	Any	Accept
14.6	APCL/URLF layer cleanup	Any	Any	Any	Any	Drop



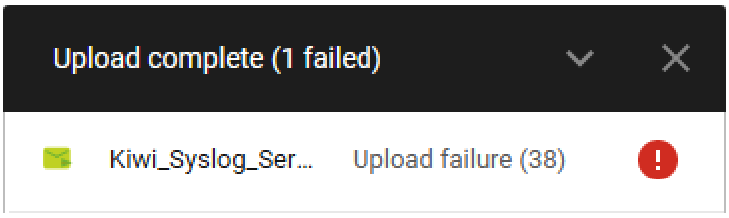
14.3	Content Awareness Incorrect UserCheck Demo Rule	Any	Internet	http https	Any Direction Executable...	Drop Blocked Messa...	Log	Policy Targets

Summary | Details | Logs | History

Last 24 Hours | Current Rule | En search query (Ctrl+F)

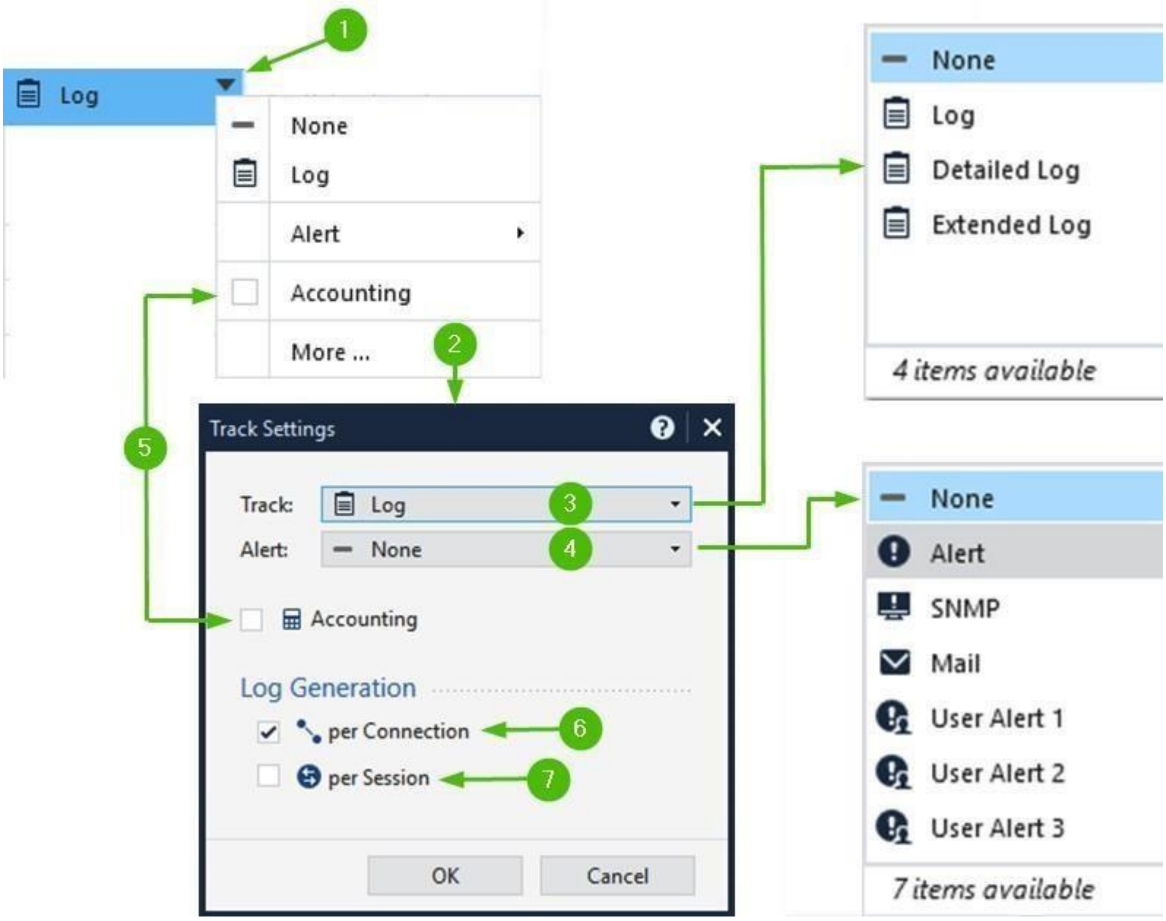
Found 1 results (90 ms)

Time	Blade	Action	Type	Interface	Origin	Source	Destination	Service	Data Type	Access Rule Number
Today, 7:36:46 PM	Content Awareness	Redirect	Session	eth0	CPCM1	SmartConsoleVM...	mia09s26-in-...	https (TCP/443)	Executable File	14.3



Upload complete (1 failed)

Kiwi_Syslog_Ser... Upload failure (38)



Track: Log

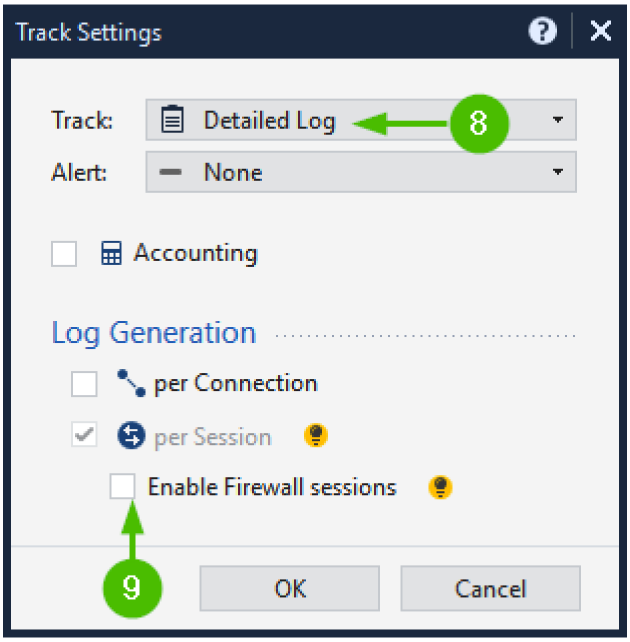
Alert: None

☐ Accounting

Log Generation

☑ per Connection

☐ per Session



Track: Detailed Log ▾

Alert: None ▾

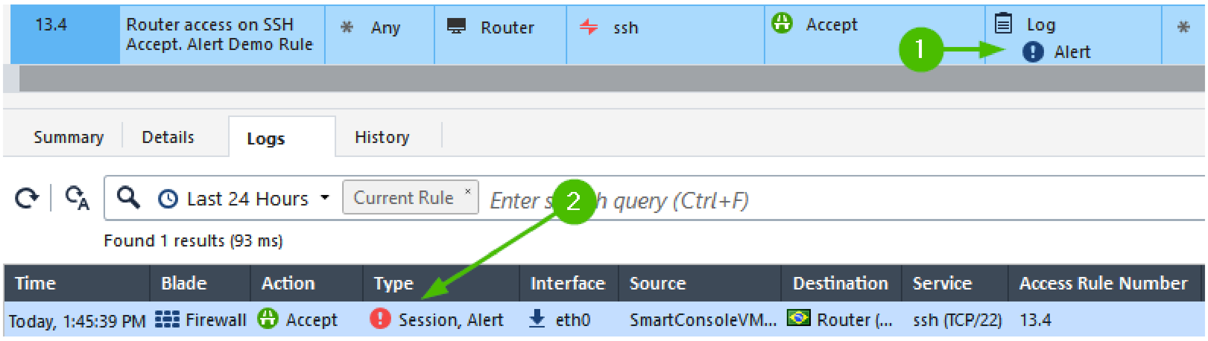
☐ Accounting

Log Generation

☐ per Connection

☑ per Session

☐ Enable Firewall sessions

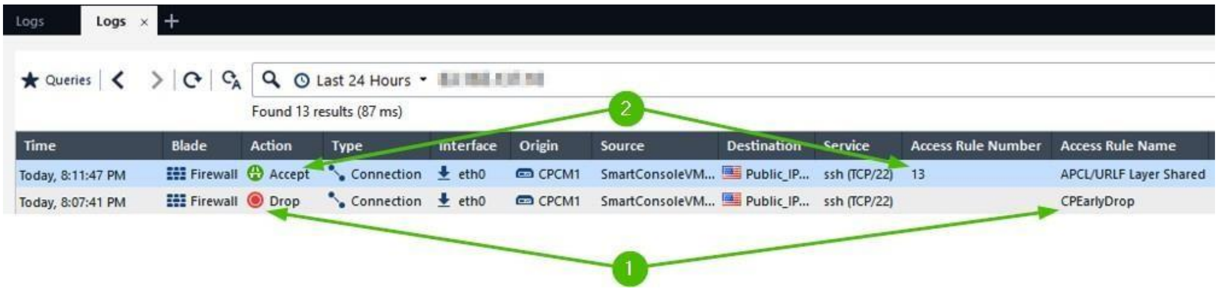


13.4	Router access on SSH Accept. Alert Demo Rule	* Any	Router	ssh	Accept	Log Alert	*

Found 1 results (93 ms)

Time	Blade	Action	Type	Interface	Source	Destination	Service	Access Rule Number
Today, 1:45:39 PM	Firewall	Accept	Session, Alert	eth0	SmartConsoleVM...	Router (...	ssh (TCP/22)	13.4

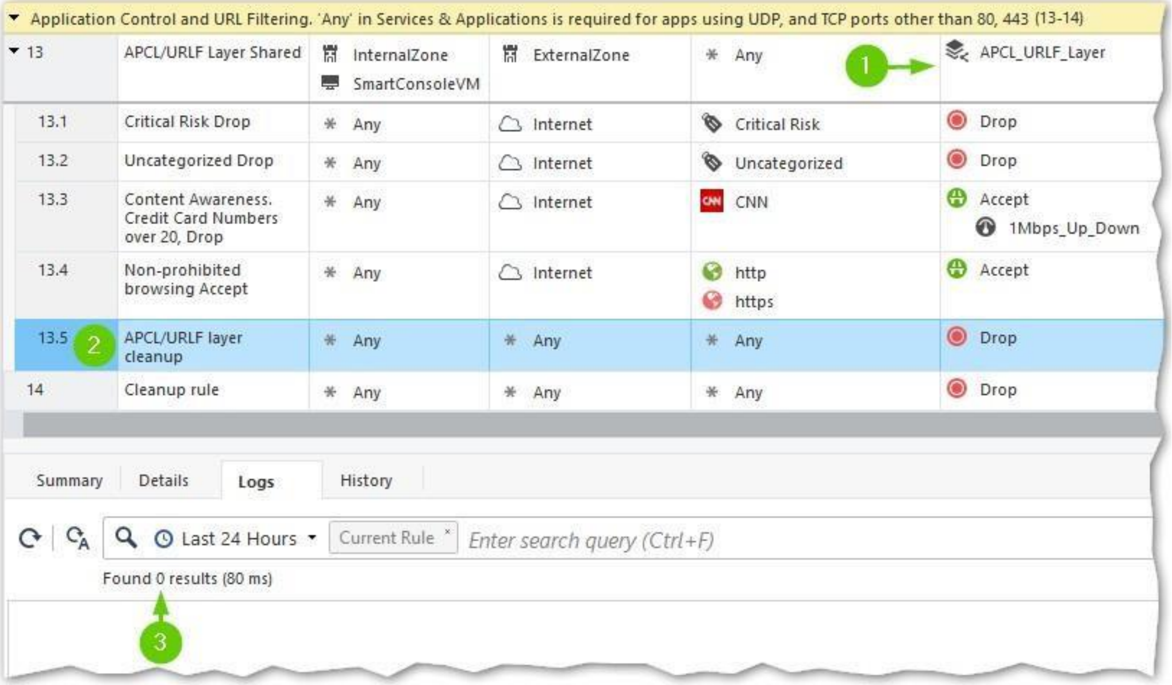
Tracking Settings Recommendations					
Blade(s)	**Track**	**Accounting**	**Per Connection**	**Per Session**	**Enable Firewall Sessions**
Firewall Only	Log	Optional	Yes	No	N/A
Content Awareness	Log	No	No	Yes	Yes
APCL/URLF with or without Content Awareness	Detailed Log	Yes	No	Yes	Yes



[redacted]

Found 13 results (87 ms)

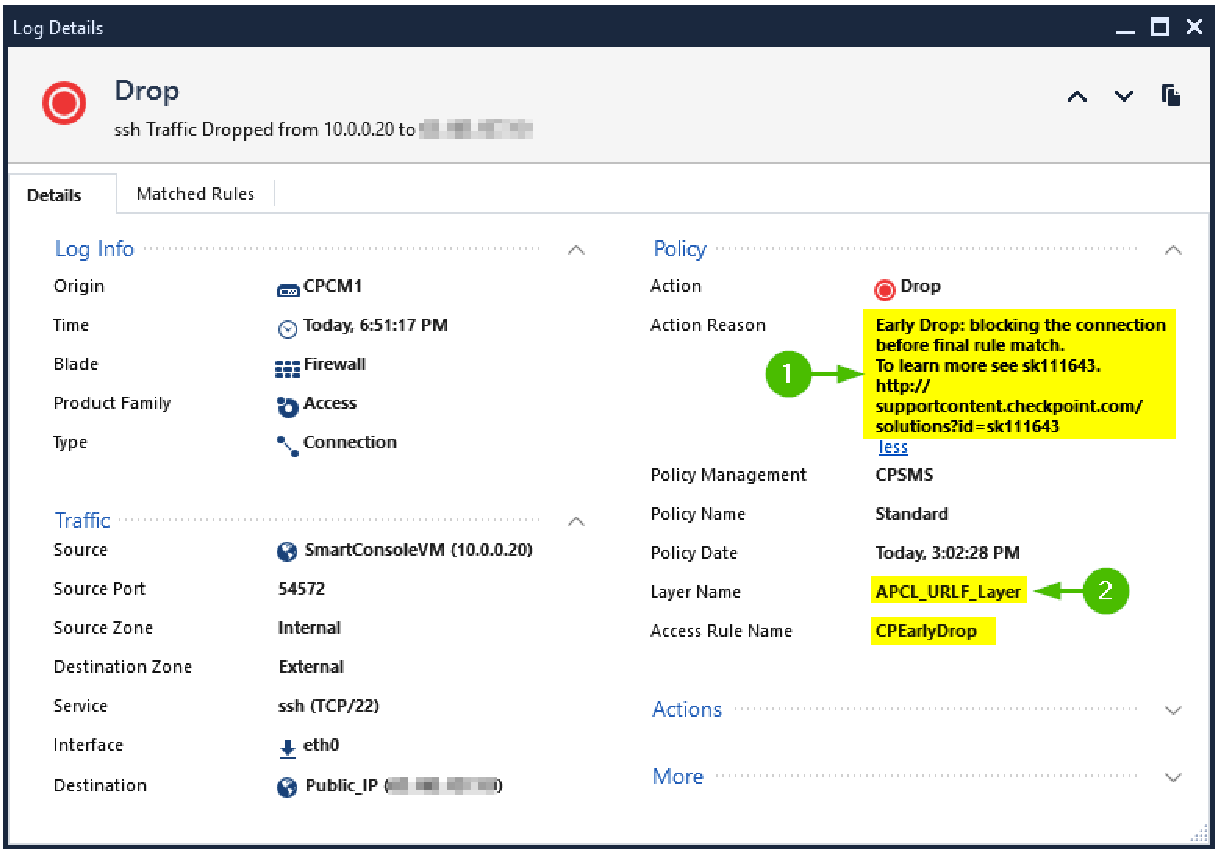
Time	Blade	Action	Type	Interface	Origin	Source	Destination	Service	Access Rule Number	Access Rule Name
Today, 8:11:47 PM	Firewall	Accept	Connection	eth0	CPCM1	SmartConsoleVM...	Public_IP...	ssh (TCP/22)	13	APCL/URLF Layer Shared
Today, 8:07:41 PM	Firewall	Drop	Connection	eth0	CPCM1	SmartConsoleVM...	Public_IP...	ssh (TCP/22)		CPEarlyDrop



Application Control and URL Filtering. 'Any' in Services & Applications is required for apps using UDP, and TCP ports other than 80, 443 (13-14)

13	APCL/URLF Layer Shared	InternalZone SmartConsoleVM	ExternalZone	Any	APCL_URLF_Layer
13.1	Critical Risk Drop	Any	Internet	Critical Risk	Drop
13.2	Uncategorized Drop	Any	Internet	Uncategorized	Drop
13.3	Content Awareness. Credit Card Numbers over 20, Drop	Any	Internet	CNN	Accept 1Mbps_Up_Down
13.4	Non-prohibited browsing Accept	Any	Internet	http https	Accept
13.5	APCL/URLF layer cleanup	Any	Any	Any	Drop
14	Cleanup rule	Any	Any	Any	Drop

Found 0 results (80 ms)



Drop

ssh Traffic Dropped from 10.0.0.20 to [redacted]

Details | Matched Rules

Log Info

Origin	CPCM1
Time	Today, 6:51:17 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

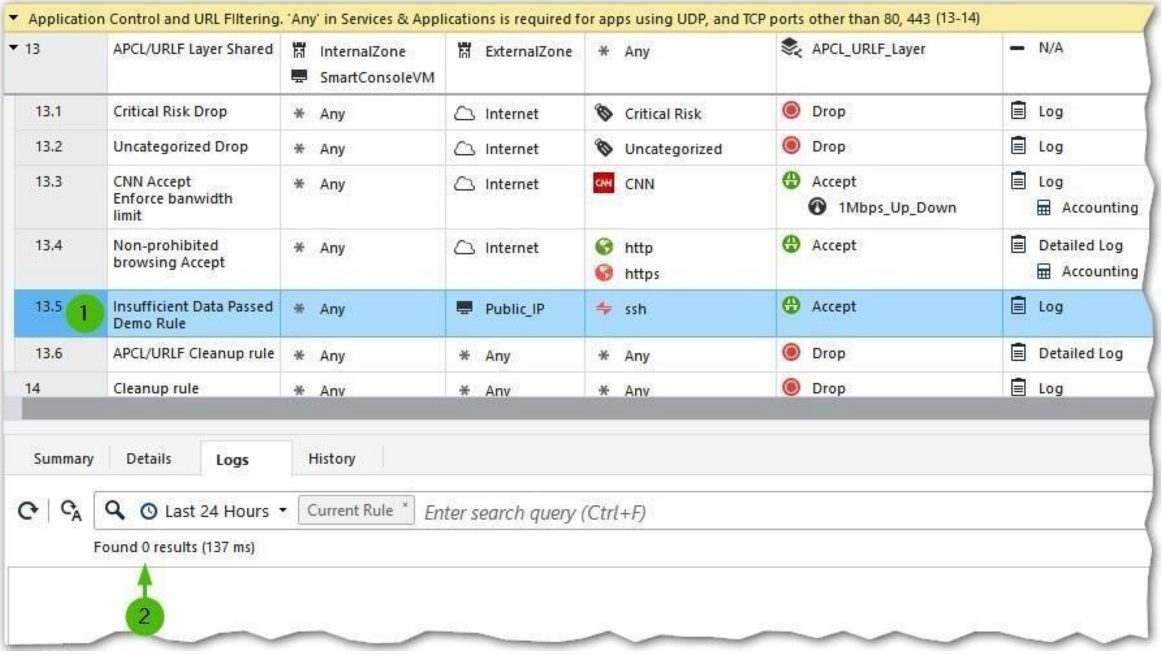
Source	SmartConsoleVM (10.0.0.20)
Source Port	54572
Source Zone	Internal
Destination Zone	External
Service	ssh (TCP/22)
Interface	eth0
Destination	Public_IP ([redacted])

Policy

Action	Drop
Action Reason	Early Drop: blocking the connection before final rule match. To learn more see sk111643. http://supportcontent.checkpoint.com/solutions?id=sk111643 less
Policy Management	CPSMS
Policy Name	Standard
Policy Date	Today, 3:02:28 PM
Layer Name	APCL_URLF_Layer
Access Rule Name	CPEarlyDrop

Actions

More



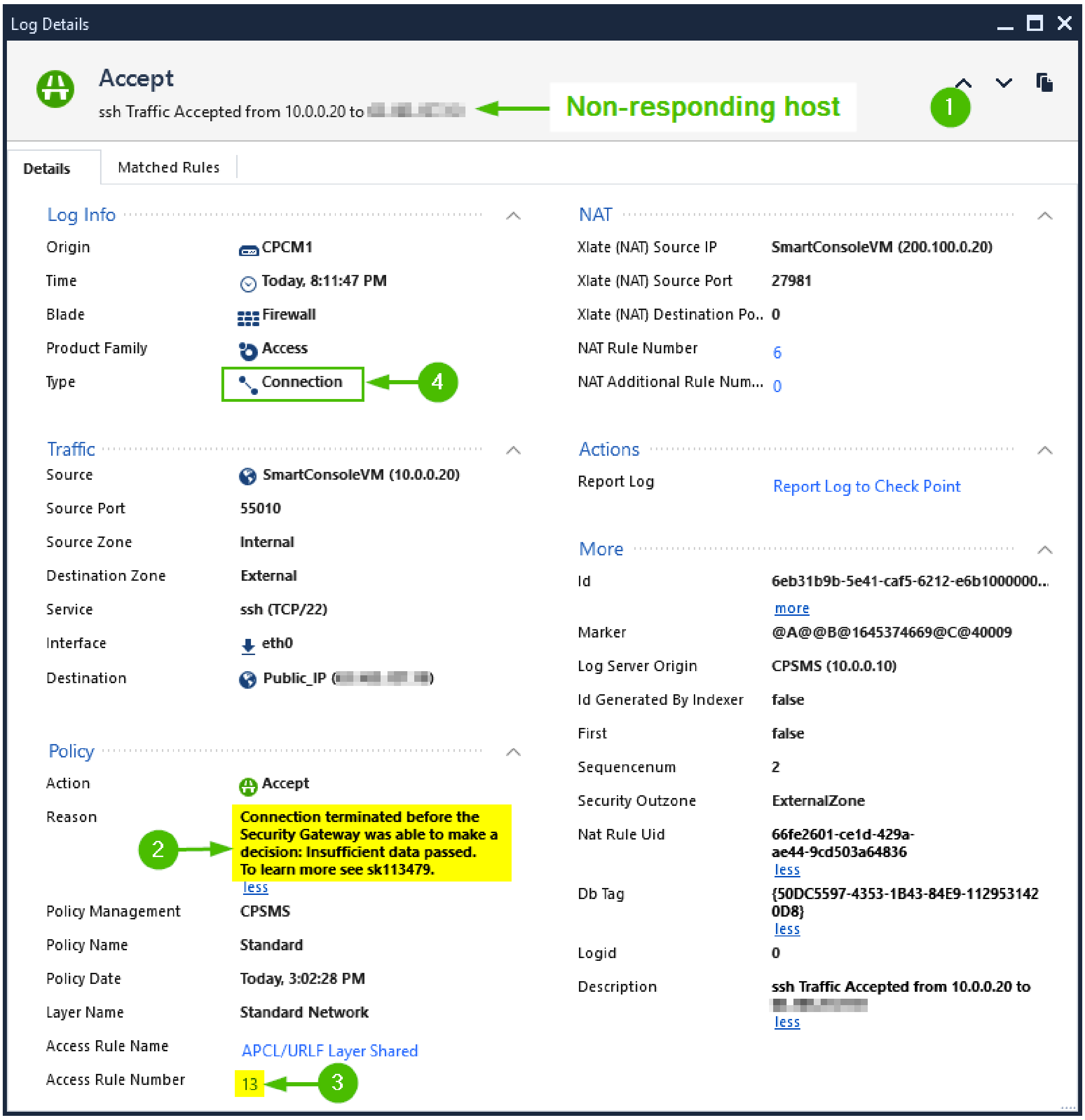
Application Control and URL Filtering. 'Any' in Services & Applications is required for apps using UDP, and TCP ports other than 80, 443 (13-14)

13	APCL/URLF Layer Shared	InternalZone SmartConsoleVM	ExternalZone	Any	APCL_URLF_Layer	N/A
13.1	Critical Risk Drop	Any	Internet	Critical Risk	Drop	Log
13.2	Uncategorized Drop	Any	Internet	Uncategorized	Drop	Log
13.3	CNN Accept Enforce banwidth limit	Any	Internet	CNN	Accept 1Mbps_Up_Down	Log Accounting
13.4	Non-prohibited browsing Accept	Any	Internet	http https	Accept	Detailed Log Accounting
13.5	Insufficient Data Passed Demo Rule	Any	Public_IP	ssh	Accept	Log
13.6	APCL/URLF Cleanup rule	Any	Any	Any	Drop	Detailed Log
14	Cleanup rule	Any	Any	Any	Drop	Log

Summary | Details | Logs | History

Last 24 Hours | Current Rule | Enter search query (Ctrl+F)

Found 0 results (137 ms)



Accept

ssh Traffic Accepted from 10.0.0.20 to [redacted]

Log Info

Origin	CPCM1
Time	Today, 8:11:47 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	SmartConsoleVM (10.0.0.20)
Source Port	55010
Source Zone	Internal
Destination Zone	External
Service	ssh (TCP/22)
Interface	eth0
Destination	Public_IP ([redacted])

Policy

Action	Accept
Reason	Connection terminated before the Security Gateway was able to make a decision: Insufficient data passed. To learn more see sk113479. less
Policy Management	CPSMS
Policy Name	Standard
Policy Date	Today, 3:02:28 PM
Layer Name	Standard Network
Access Rule Name	APCL/URLF Layer Shared
Access Rule Number	13

NAT

Xlate (NAT) Source IP	SmartConsoleVM (200.100.0.20)
Xlate (NAT) Source Port	27981
Xlate (NAT) Destination Po...	0
NAT Rule Number	6
NAT Additional Rule Num...	0

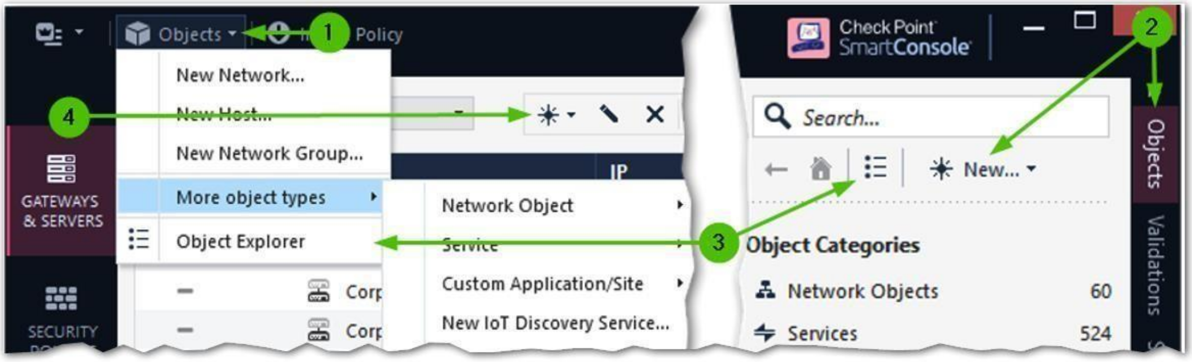
Actions

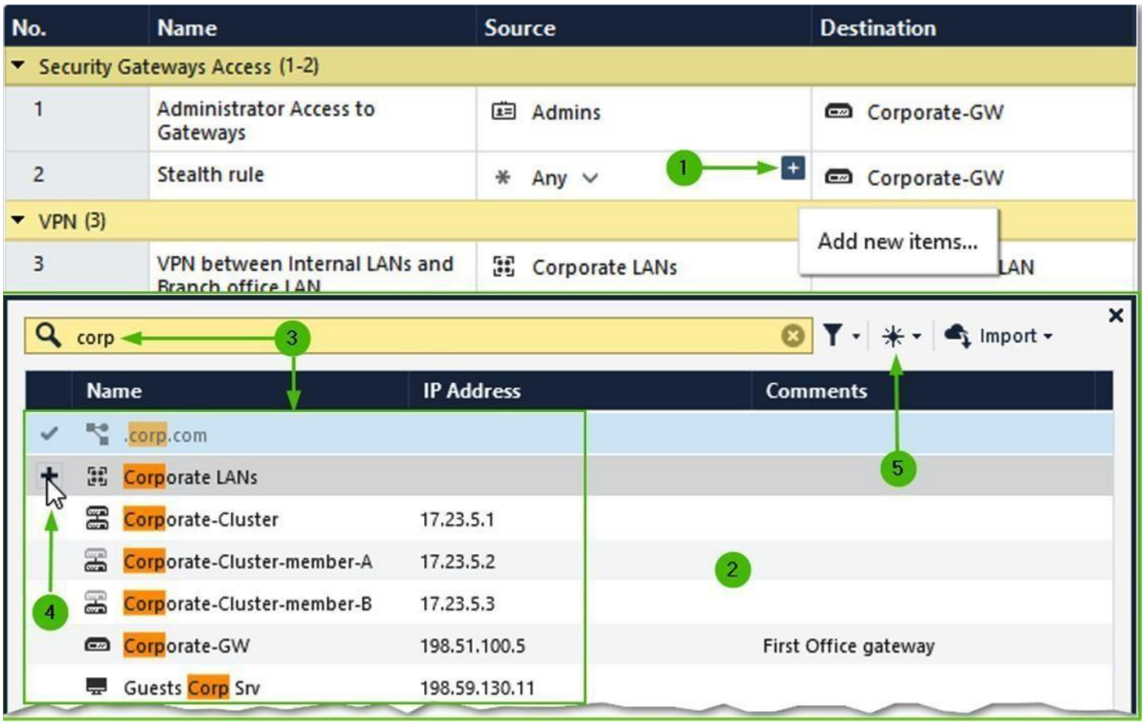
Report Log	Report Log to Check Point

More

Id	6eb31b9b-5e41-caf5-6212-e6b1000000... more
Marker	@A@@B@1645374669@C@40009
Log Server Origin	CPSMS (10.0.0.10)
Id Generated By Indexer	false
First	false
Sequencenum	2
Security Outzone	ExternalZone
Nat Rule Uid	66fe2601-ce1d-429a-ae44-9cd503a64836 less
Db Tag	{50DC5597-4353-1B43-84E9-112953142 0D8} less
Logid	0
Description	ssh Traffic Accepted from 10.0.0.20 to [redacted] less

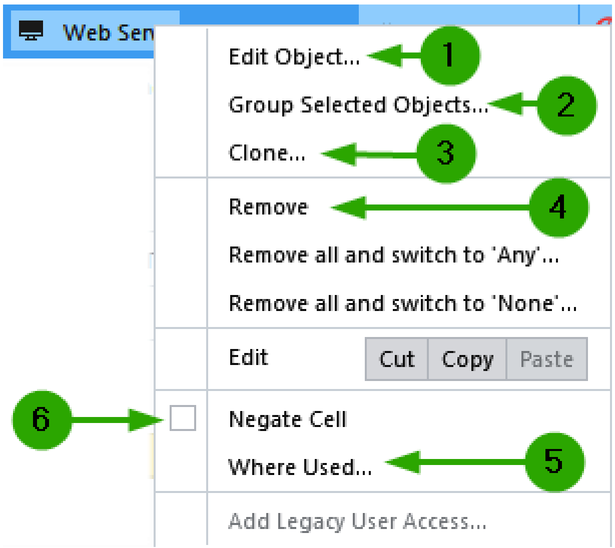
Chapter 9: Working with Objects – ICA, SIC, Managed, Static, and Variable Objects

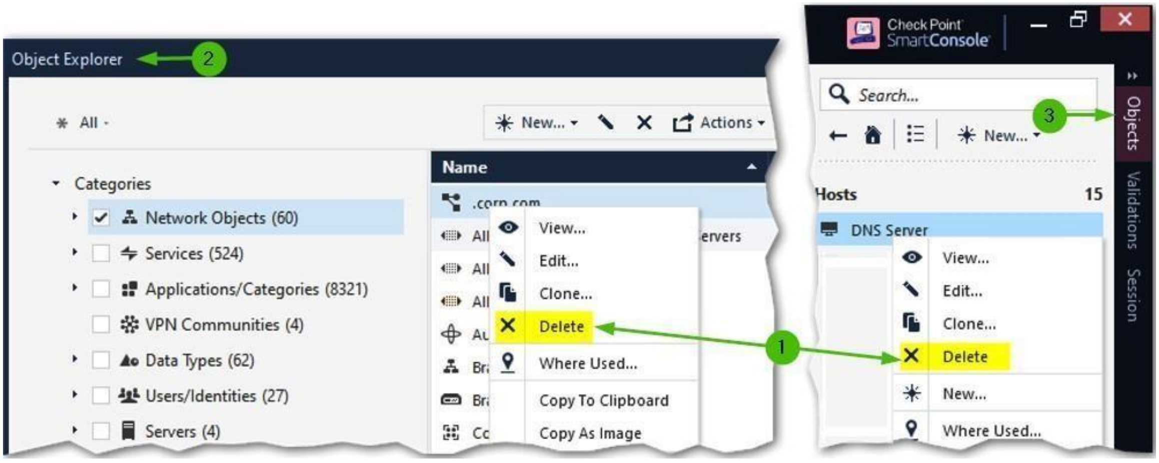


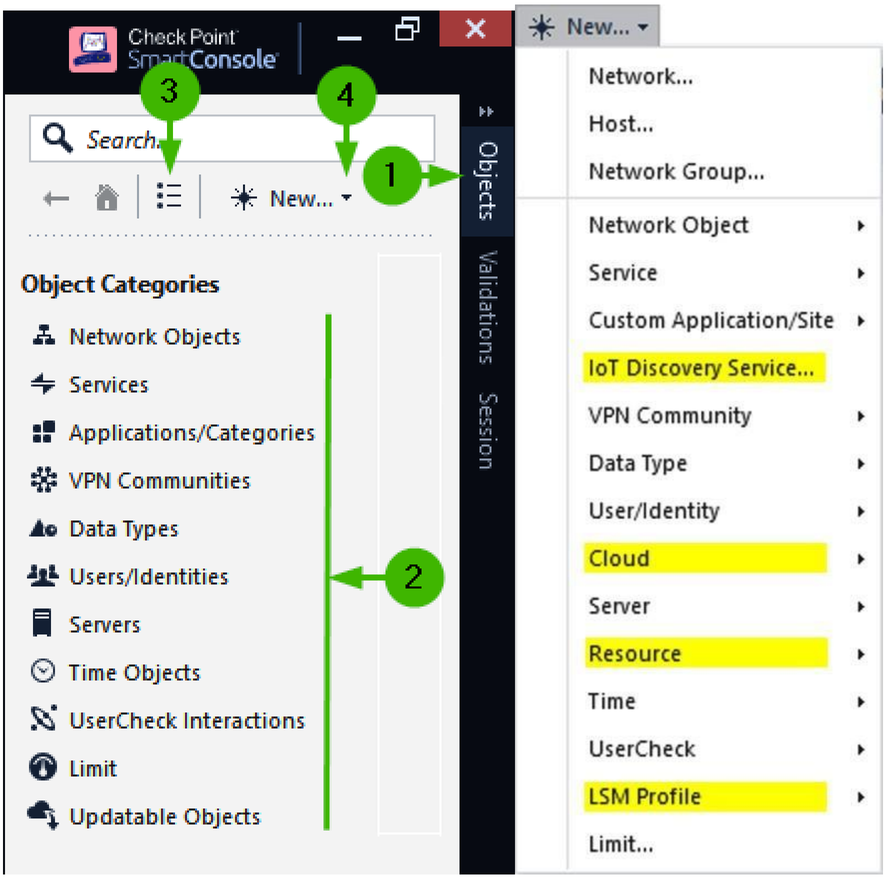


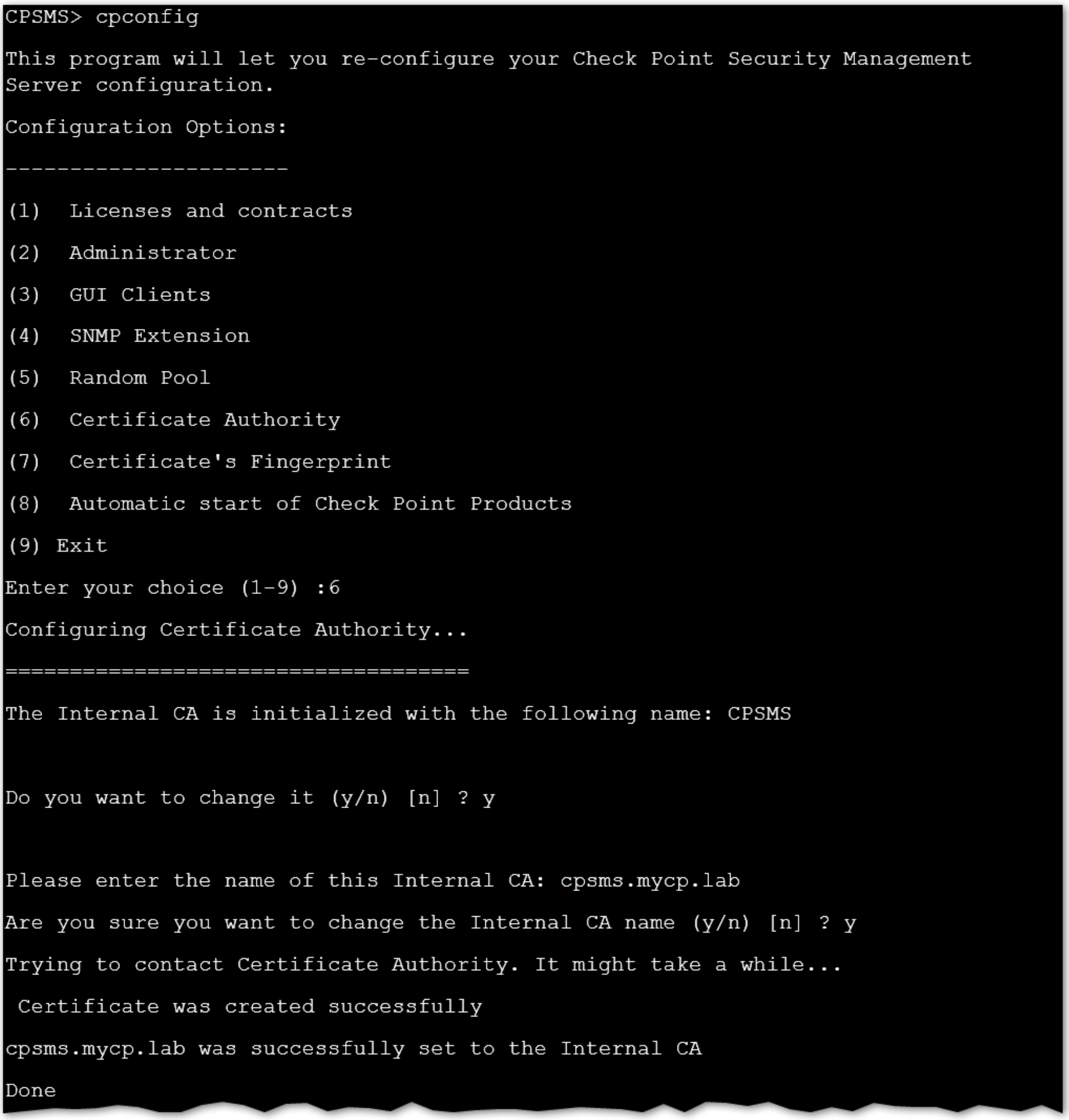
No.	Name	Source	Destination
Security Gateways Access (1-2)			
1	Administrator Access to Gateways	Admins	Corporate-GW
2	Stealth rule	Any	Corporate-GW
VPN (3)			
3	VPN between Internal LANs and Branch office LAN	Corporate LANs	LAN

Name	IP Address	Comments
.corp.com		
Corporate LANs		
Corporate-Cluster	17.23.5.1	
Corporate-Cluster-member-A	17.23.5.2	
Corporate-Cluster-member-B	17.23.5.3	
Corporate-GW	198.51.100.5	First Office gateway
Guests Corp Srv	198.59.130.11	

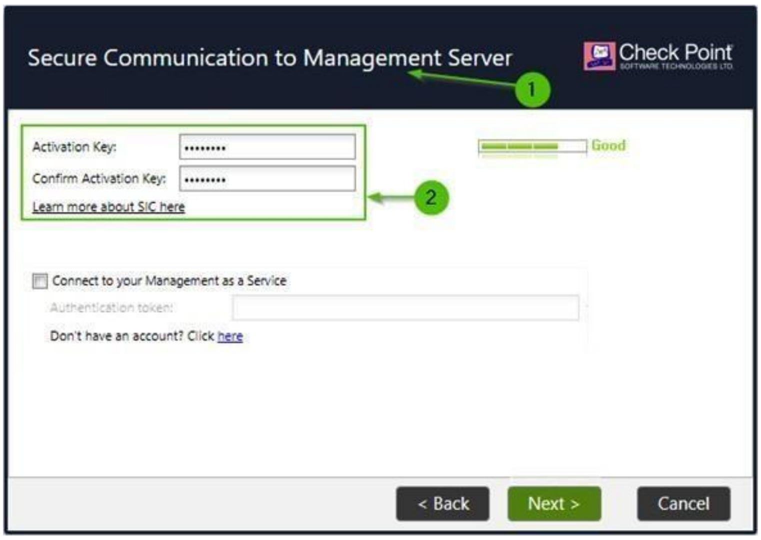

Web Ser
Edit Object...
1
Group Selected Objects...
2
Clone...
3
Remove
4
Remove all and switch to 'Any'...
Remove all and switch to 'None'...
Edit
Cut
Copy
Paste
6
Negate Cell
Where Used...
5
Add Legacy User Access...


Object Explorer
2
All
New...
Actions
Categories
Network Objects (60)
Services (524)
Applications/Categories (8321)
VPN Communities (4)
Data Types (62)
Users/Identities (27)
Servers (4)
Name
.corp.com
View...
Edit...
Clone...
Delete
Where Used...
Copy To Clipboard
Copy As Image
ervers
1
Check Point SmartConsole
Search...
New...
3
Objects
Validations
Session
Hosts
15
DNS Server
View...
Edit...
Clone...
Delete
New...
Where Used...


Check Point SmartConsole
Search...
New...
Objects
Validations
Session
1
2
3
4
Object Categories
Network Objects
Services
Applications/Categories
VPN Communities
Data Types
Users/Identities
Servers
Time Objects
UserCheck Interactions
Limit
Updatable Objects
New...
Network...
Host...
Network Group...
Network Object
Service
Custom Application/Site
IoT Discovery Service...
VPN Community
Data Type
User/Identity
Cloud
Server
Resource
Time
UserCheck
LSM Profile
Limit...



```
CPSMS> cpconfig

This program will let you re-configure your Check Point Security Management
Server configuration.

Configuration Options:

----------------------

(1)  Licenses and contracts

(2)  Administrator

(3)  GUI Clients

(4)  SNMP Extension

(5)  Random Pool

(6)  Certificate Authority

(7)  Certificate's Fingerprint

(8)  Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :6

Configuring Certificate Authority...

====================================

The Internal CA is initialized with the following name: CPSMS


Do you want to change it (y/n) [n] ? y


Please enter the name of this Internal CA: cpsms.mycp.lab

Are you sure you want to change the Internal CA name (y/n) [n] ? y

Trying to contact Certificate Authority. It might take a while...

 Certificate was created successfully

cpsms.mycp.lab was successfully set to the Internal CA

Done
```



Secure Communication to Management Server

Activation Key: ••••••••

Confirm Activation Key: ••••••••

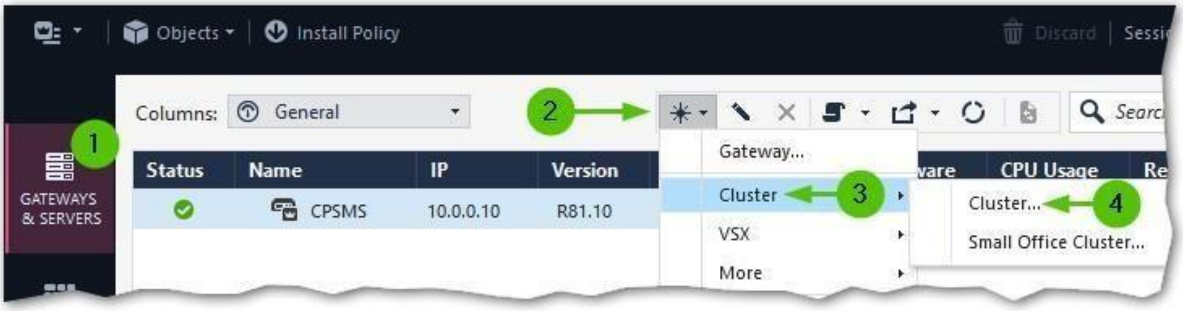
Learn more about SIC here

Good

☐ Connect to your Management as a Service

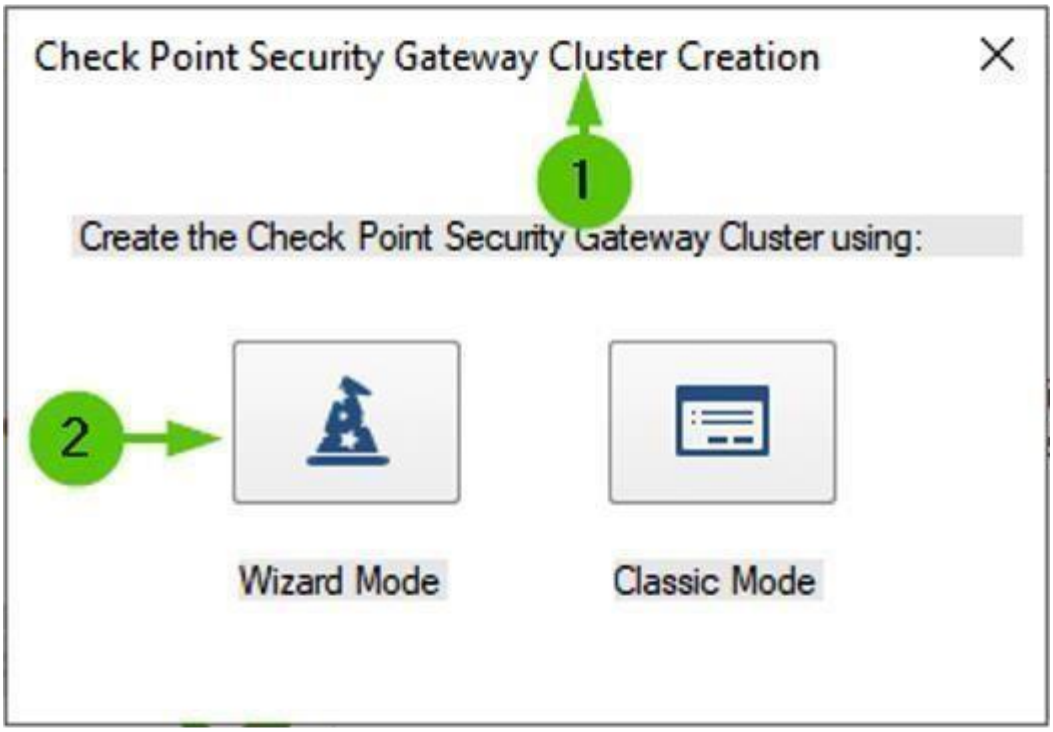
Authentication token:

Don't have an account? Click here



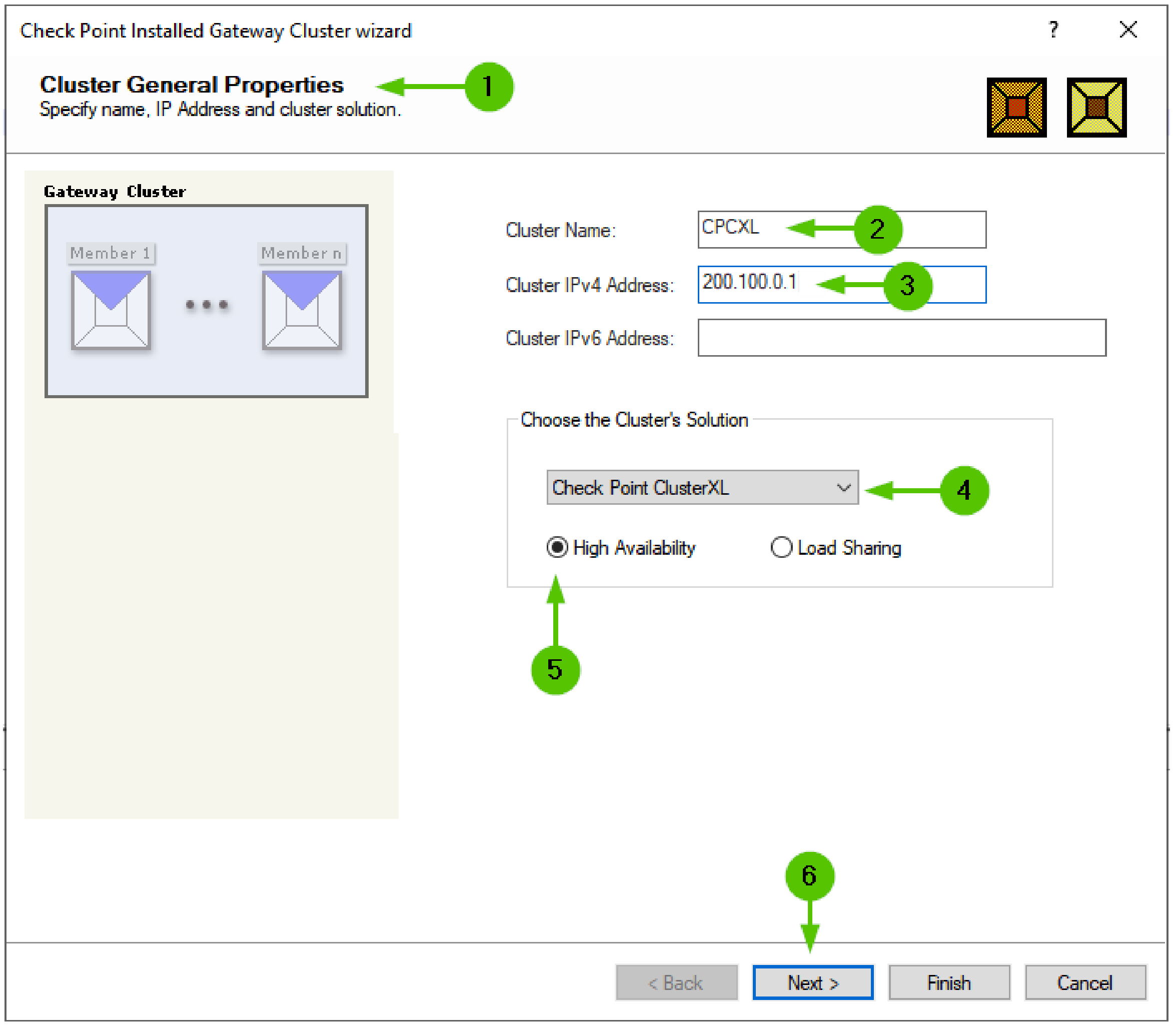
Columns: General

Status	Name	IP	Version
✓	CPSMS	10.0.0.10	R81.10



Check Point Security Gateway Cluster Creation

Create the Check Point Security Gateway Cluster using:



Check Point Installed Gateway Cluster wizard

Cluster General Properties

Specify name, IP Address and cluster solution.

1

Cluster Name: CPCXL

2

Cluster IPv4 Address: 200.100.0.1

3

Cluster IPv6 Address:

Choose the Cluster's Solution

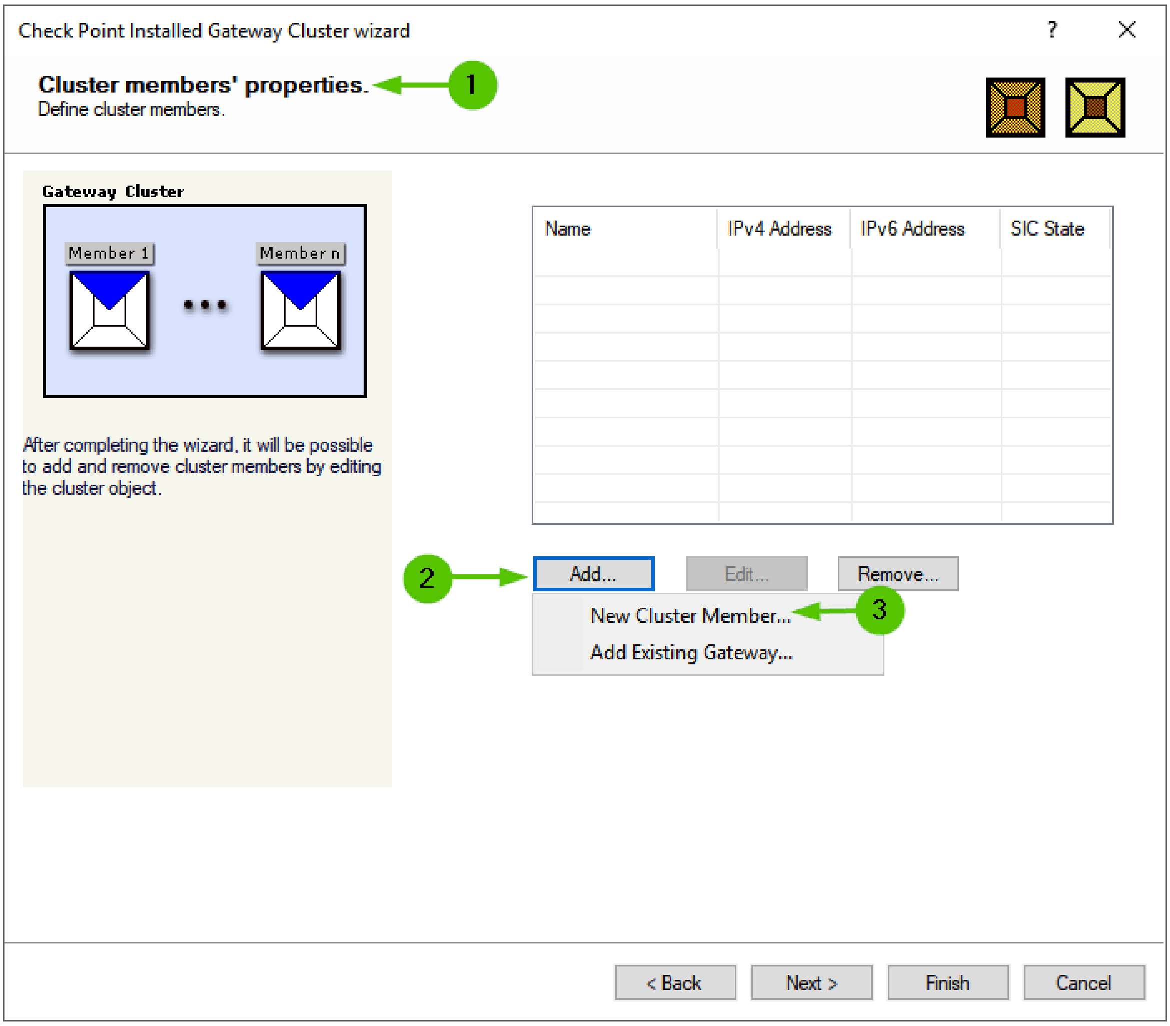
Check Point ClusterXL

4

● High Availability ○ Load Sharing

5

6

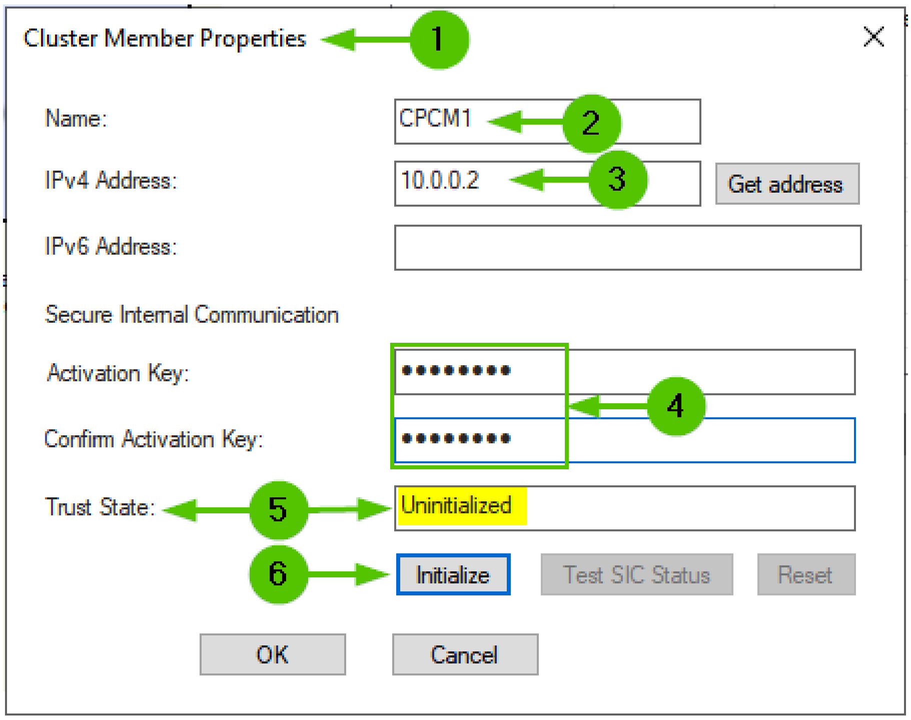


Check Point Installed Gateway Cluster wizard

Cluster members' properties.
Define cluster members.

After completing the wizard, it will be possible to add and remove cluster members by editing the cluster object.

Name	IPv4 Address	IPv6 Address	SIC State



Cluster Member Properties

Name: CPCM1

IPv4 Address: 10.0.0.2

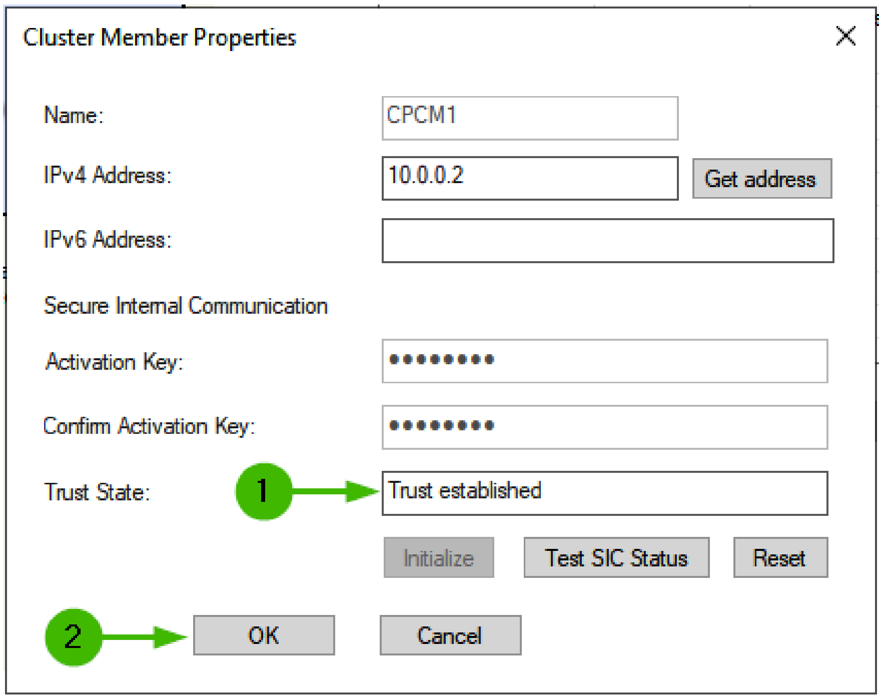
IPv6 Address:

Secure Internal Communication

Activation Key: ••••••••

Confirm Activation Key: ••••••••

Trust State: Uninitialized



Cluster Member Properties

Name: CPCM1

IPv4 Address: 10.0.0.2

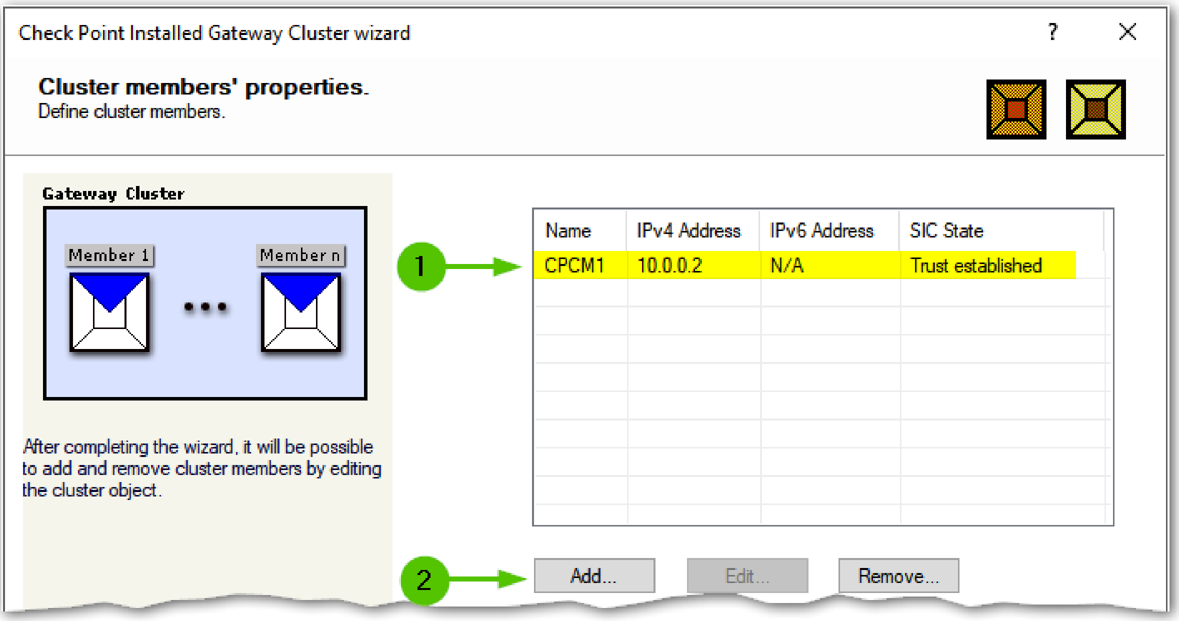
IPv6 Address:

Secure Internal Communication

Activation Key: ••••••••

Confirm Activation Key: ••••••••

Trust State: Trust established

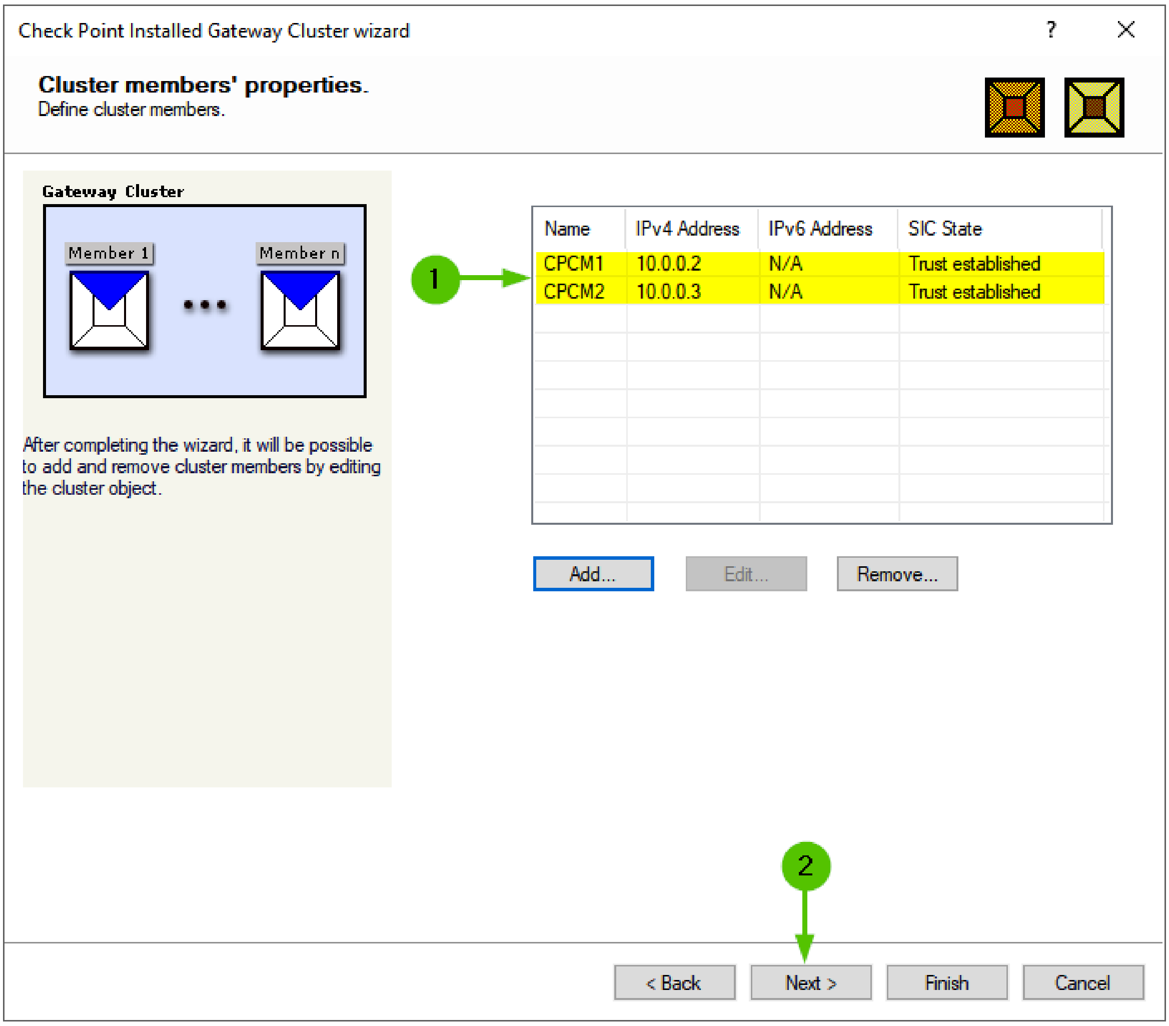


Check Point Installed Gateway Cluster wizard

Cluster members' properties.
Define cluster members.

After completing the wizard, it will be possible to add and remove cluster members by editing the cluster object.

Name	IPv4 Address	IPv6 Address	SIC State
CPCM1	10.0.0.2	N/A	Trust established

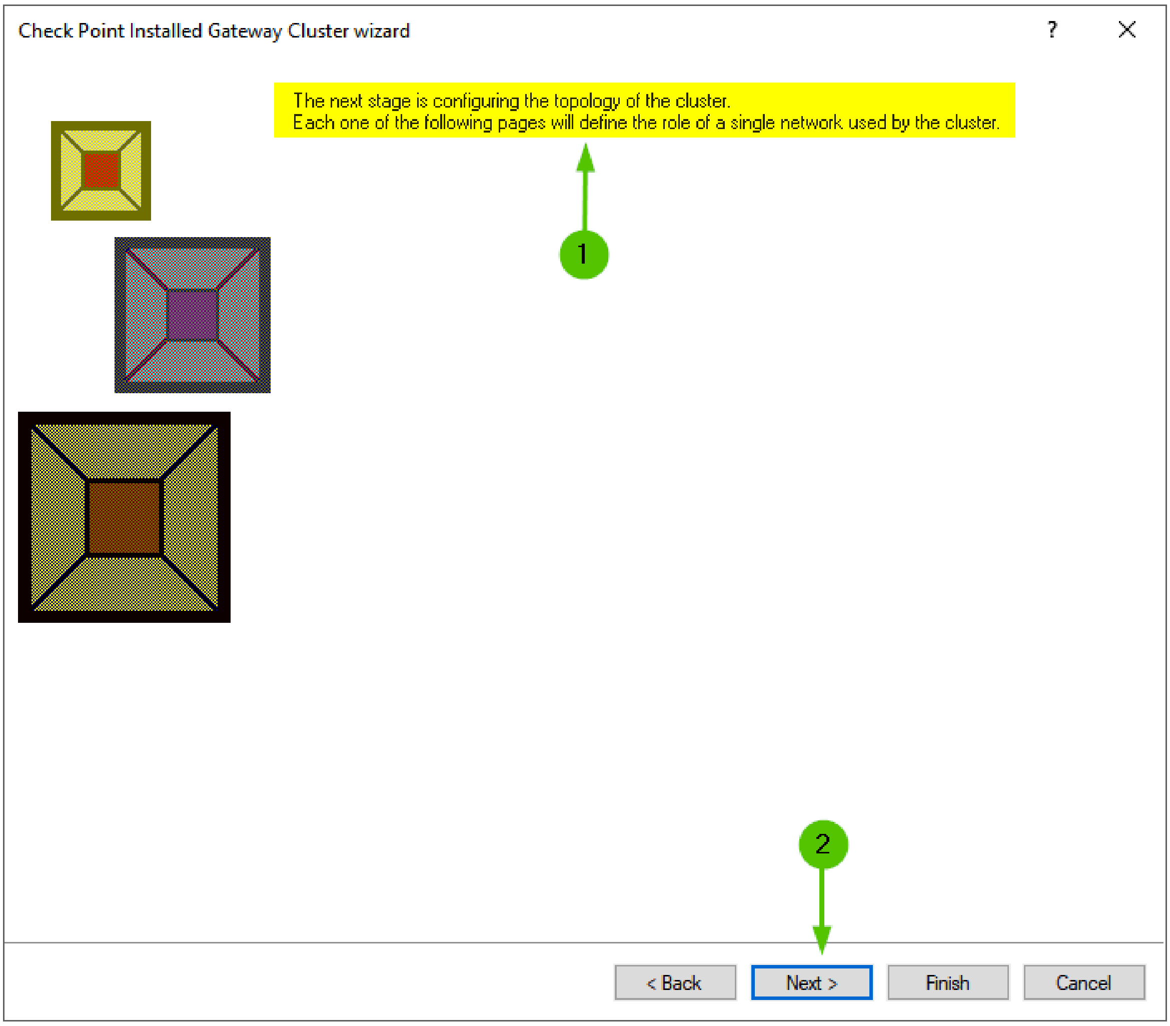


Check Point Installed Gateway Cluster wizard

Cluster members' properties.
Define cluster members.

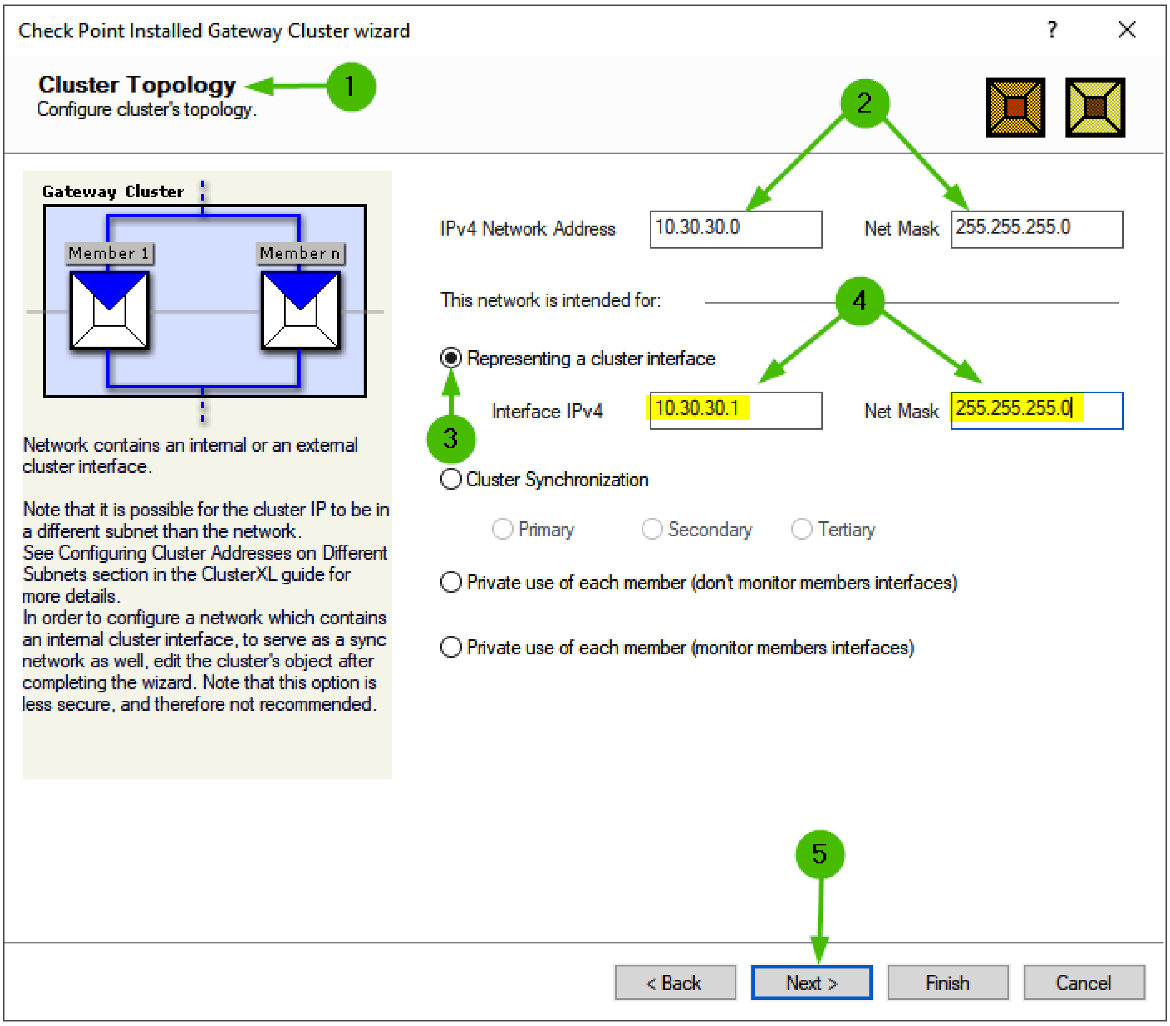
After completing the wizard, it will be possible to add and remove cluster members by editing the cluster object.

Name	IPv4 Address	IPv6 Address	SIC State
CPCM1	10.0.0.2	N/A	Trust established
CPCM2	10.0.0.3	N/A	Trust established



Check Point Installed Gateway Cluster wizard

The next stage is configuring the topology of the cluster.
Each one of the following pages will define the role of a single network used by the cluster.



Check Point Installed Gateway Cluster wizard

Cluster Topology

Configure cluster's topology.

Network contains an internal or an external cluster interface.

Note that it is possible for the cluster IP to be in a different subnet than the network.
See Configuring Cluster Addresses on Different Subnets section in the ClusterXL guide for more details.
In order to configure a network which contains an internal cluster interface, to serve as a sync network as well, edit the cluster's object after completing the wizard. Note that this option is less secure, and therefore not recommended.

IPv4 Network Address: 10.30.30.0 Net Mask: 255.255.255.0

This network is intended for:

● Representing a cluster interface

Interface IPv4: 10.30.30.1 Net Mask: 255.255.255.0

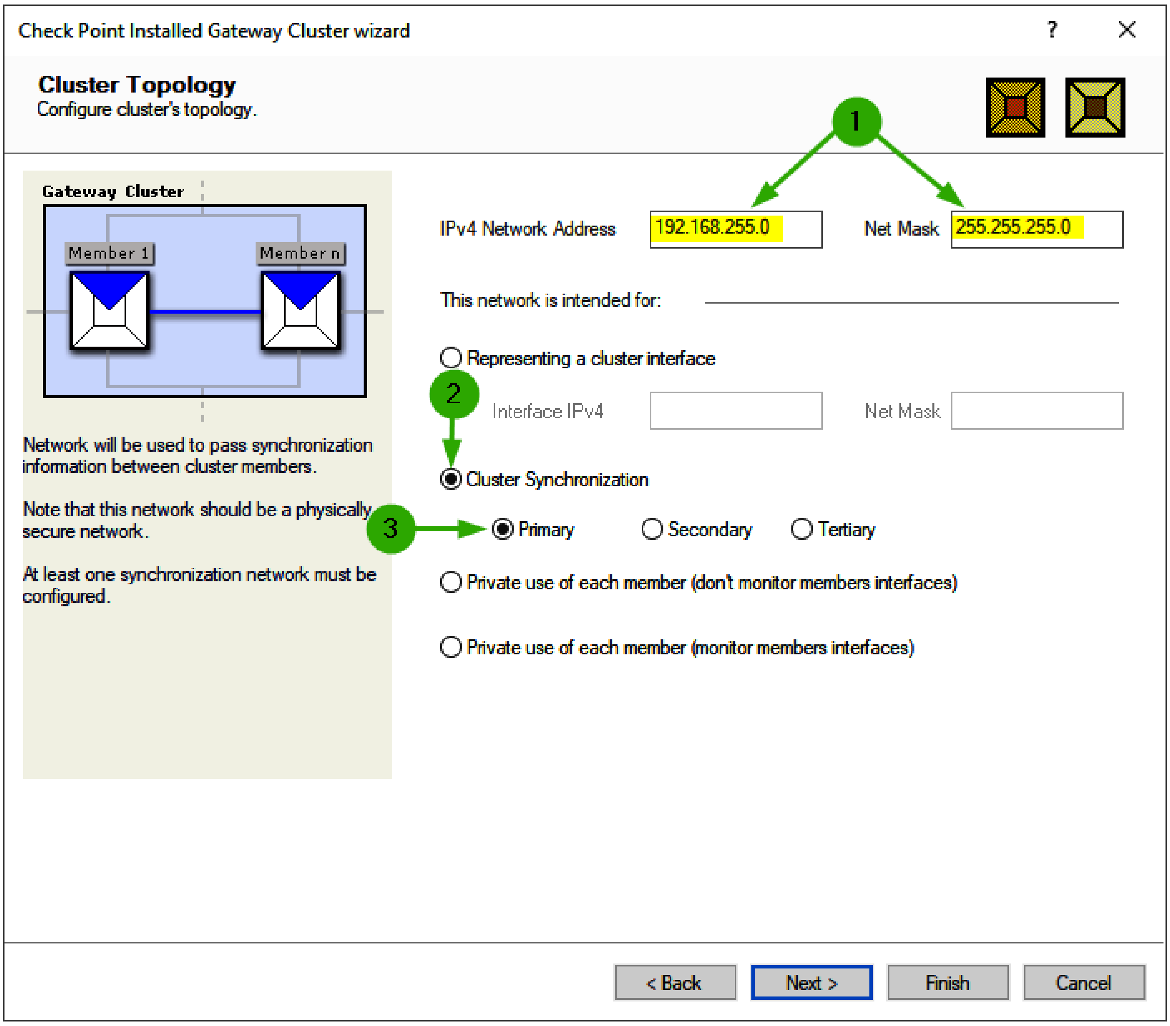
○ Cluster Synchronization

○ Primary ○ Secondary ○ Tertiary

○ Private use of each member (don't monitor members interfaces)

○ Private use of each member (monitor members interfaces)

< Back | Next > | Finish | Cancel



Check Point Installed Gateway Cluster wizard

Cluster Topology

Configure cluster's topology.

Network will be used to pass synchronization information between cluster members.

Note that this network should be a physically secure network.

At least one synchronization network must be configured.

IPv4 Network Address: 192.168.255.0   Net Mask: 255.255.255.0

This network is intended for:

○ Representing a cluster interface

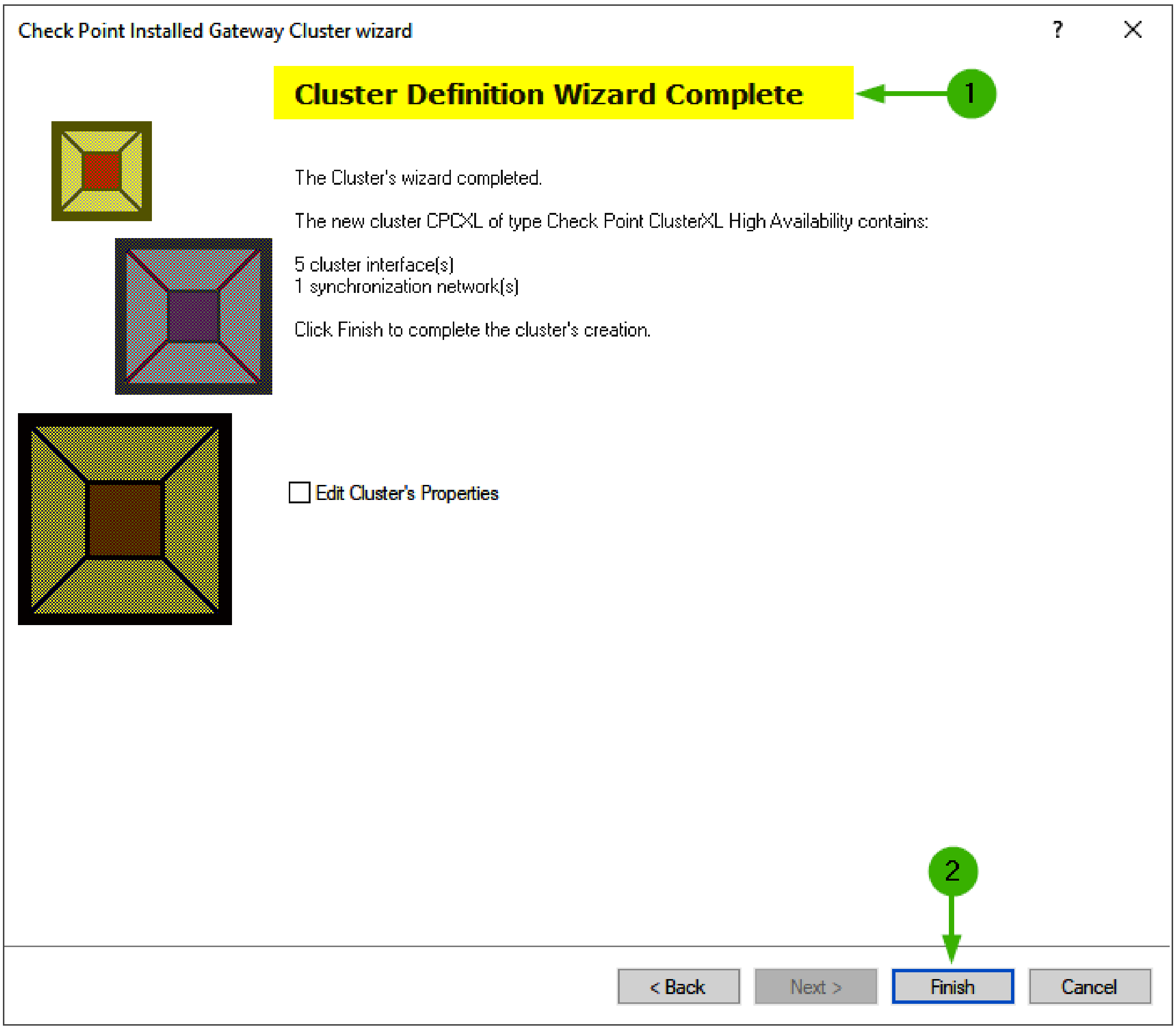
Interface IPv4   Net Mask

● Cluster Synchronization

● Primary ○ Secondary ○ Tertiary

○ Private use of each member (don't monitor members interfaces)

○ Private use of each member (monitor members interfaces)



Check Point Installed Gateway Cluster wizard

Cluster Definition Wizard Complete

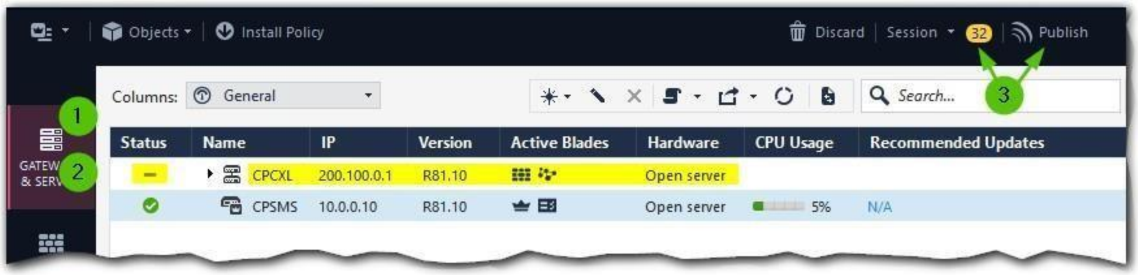
The Cluster's wizard completed.

The new cluster CPCXL of type Check Point ClusterXL High Availability contains:

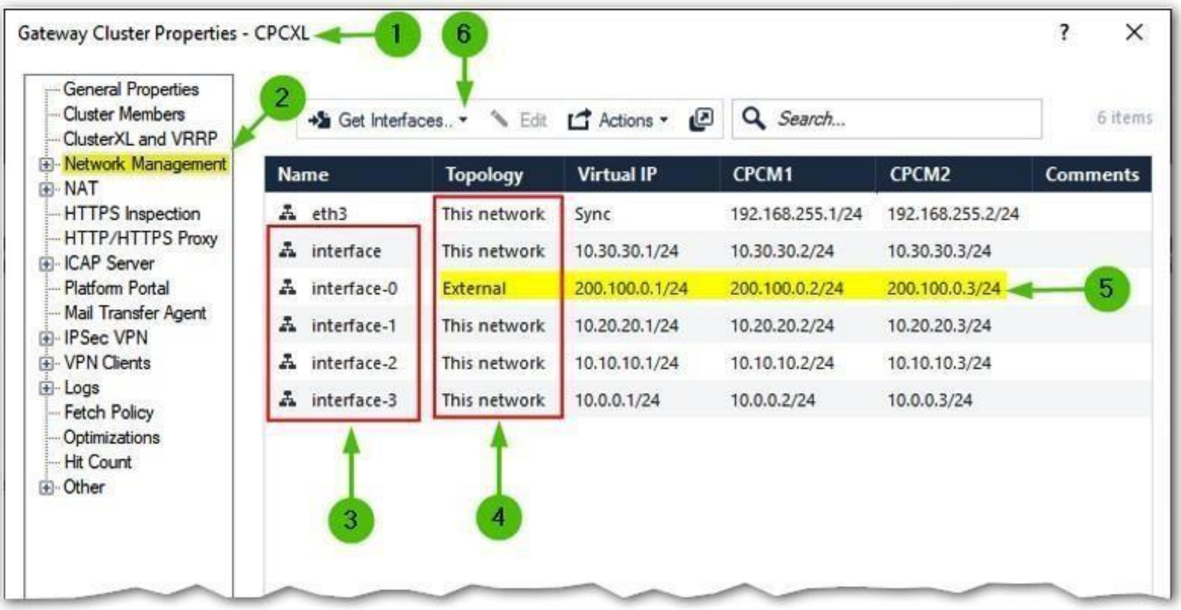
5 cluster interface(s)
1 synchronization network(s)

Click Finish to complete the cluster's creation.

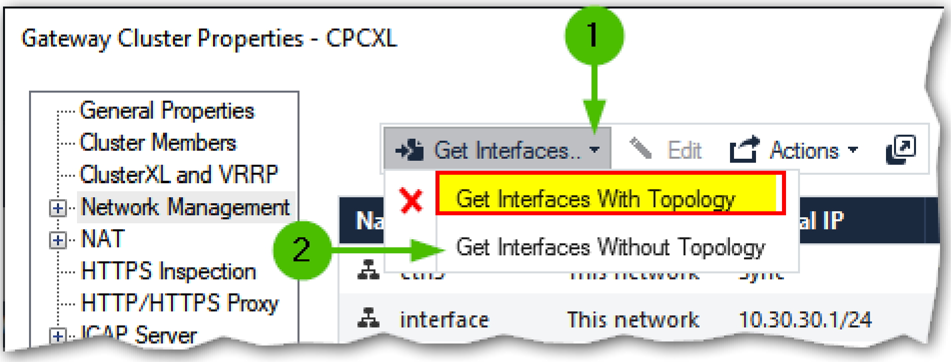
□ Edit Cluster's Properties

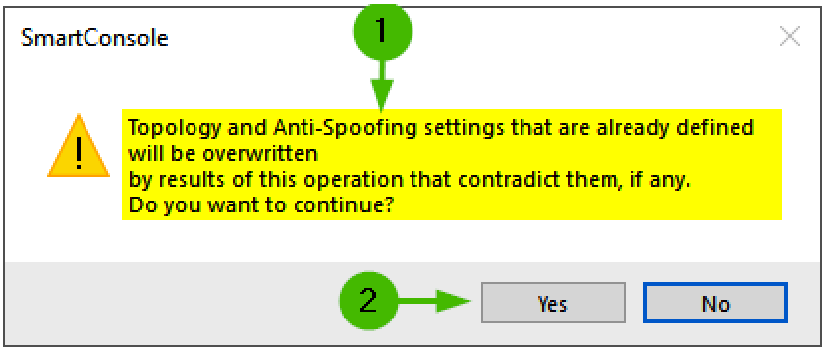


Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates
—	CPCXL	200.100.0.1	R81.10		Open server		
✓	CPSMS	10.0.0.10	R81.10		Open server	5%	N/A

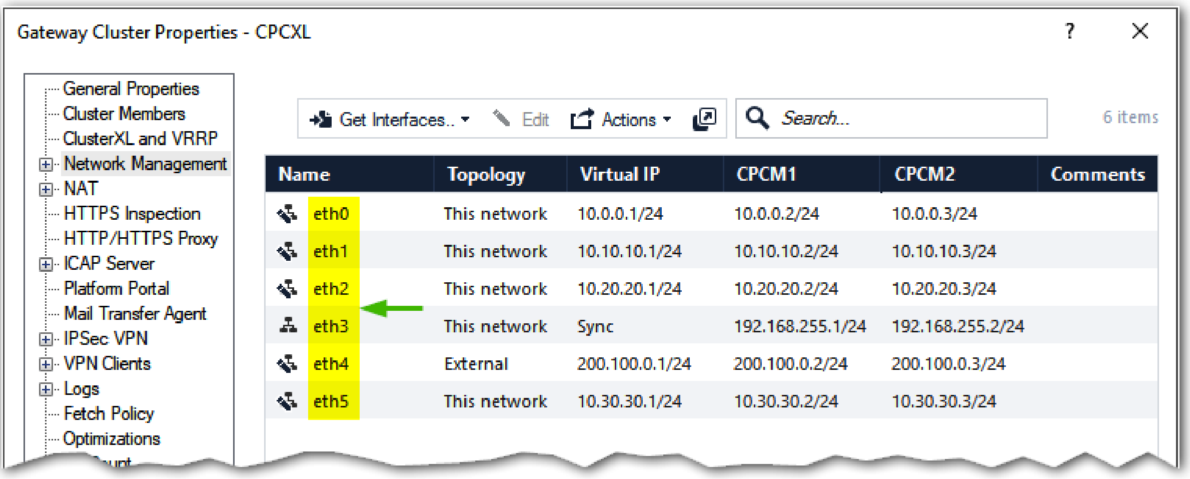


Name	Topology	Virtual IP	CPCM1	CPCM2	Comments
eth3	This network	Sync	192.168.255.1/24	192.168.255.2/24	
interface	This network	10.30.30.1/24	10.30.30.2/24	10.30.30.3/24	
interface-0	External	200.100.0.1/24	200.100.0.2/24	200.100.0.3/24	
interface-1	This network	10.20.20.1/24	10.20.20.2/24	10.20.20.3/24	
interface-2	This network	10.10.10.1/24	10.10.10.2/24	10.10.10.3/24	
interface-3	This network	10.0.0.1/24	10.0.0.2/24	10.0.0.3/24	



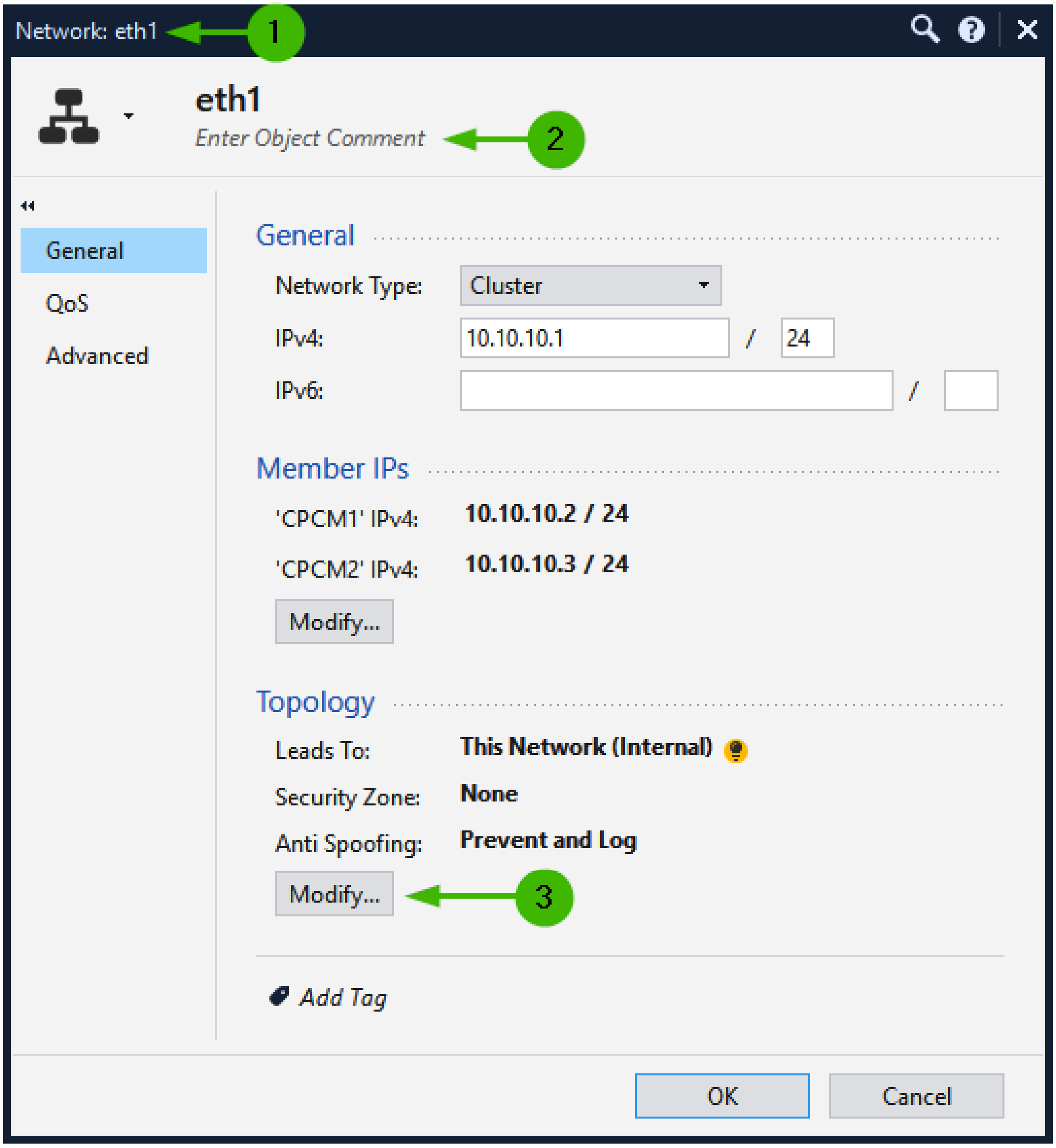


Topology and Anti-Spoofing settings that are already defined will be overwritten
by results of this operation that contradict them, if any.
Do you want to continue?



Gateway Cluster Properties - CPCXL

Name	Topology	Virtual IP	CPCM1	CPCM2	Comments
eth0	This network	10.0.0.1/24	10.0.0.2/24	10.0.0.3/24	
eth1	This network	10.10.10.1/24	10.10.10.2/24	10.10.10.3/24	
eth2	This network	10.20.20.1/24	10.20.20.2/24	10.20.20.3/24	
eth3	This network	Sync	192.168.255.1/24	192.168.255.2/24	
eth4	External	200.100.0.1/24	200.100.0.2/24	200.100.0.3/24	
eth5	This network	10.30.30.1/24	10.30.30.2/24	10.30.30.3/24	



Network: eth1

eth1

Enter Object Comment

General

Network Type: Cluster

IPv4: 10.10.10.1 / 24

IPv6: /

Member IPs

'CPCM1' IPv4: **10.10.10.2 / 24**

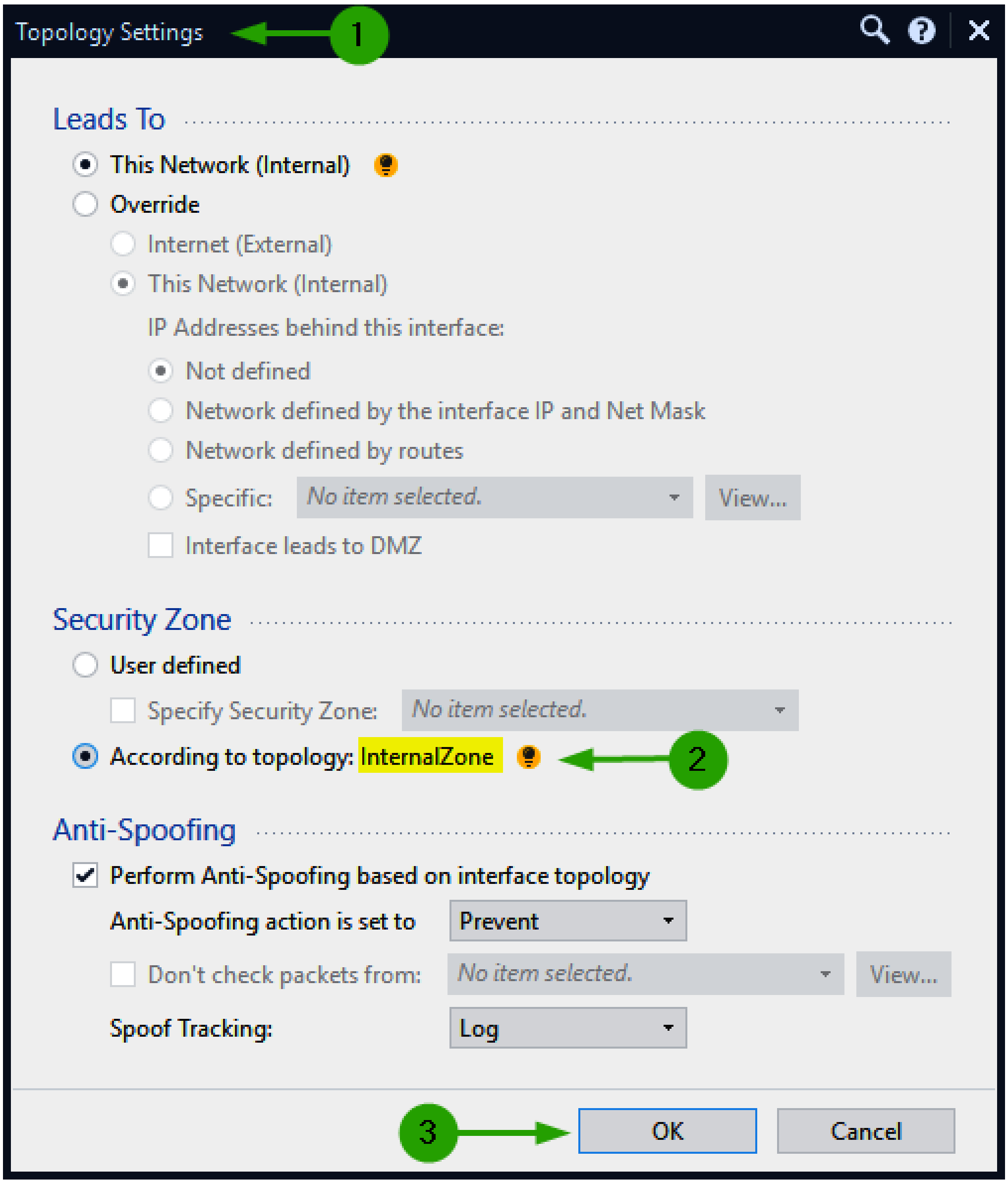
'CPCM2' IPv4: **10.10.10.3 / 24**

Topology

Leads To: **This Network (Internal)**

Security Zone: **None**

Anti Spoofing: **Prevent and Log**



Topology Settings

Leads To

● This Network (Internal)

○ Override

○ Internet (External)

● This Network (Internal)

IP Addresses behind this interface:

● Not defined

○ Network defined by the interface IP and Net Mask

○ Network defined by routes

○ Specific: No item selected. View...

□ Interface leads to DMZ

Security Zone

○ User defined

□ Specify Security Zone: No item selected.

● According to topology: InternalZone

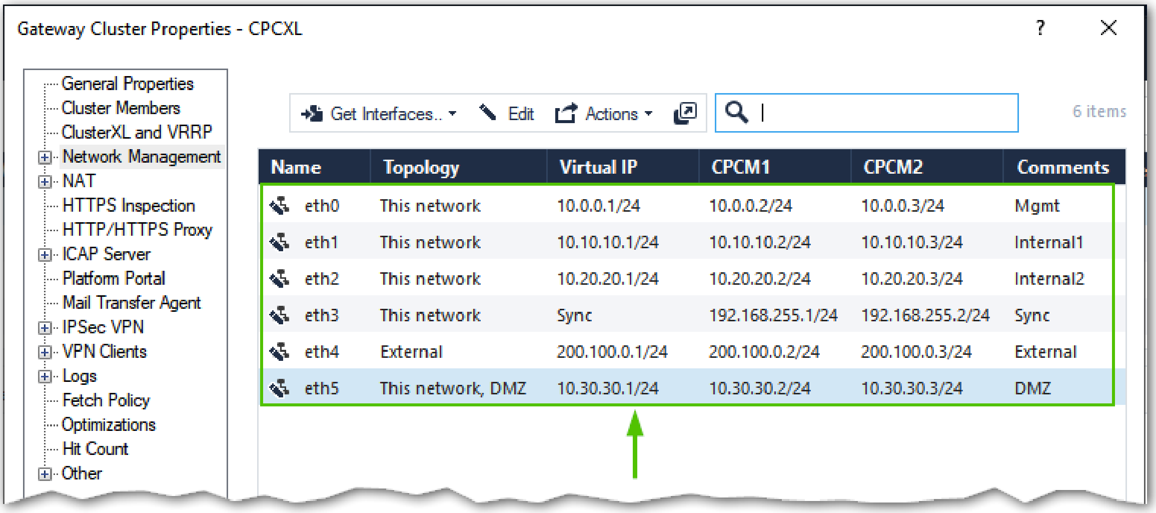
Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to: Prevent

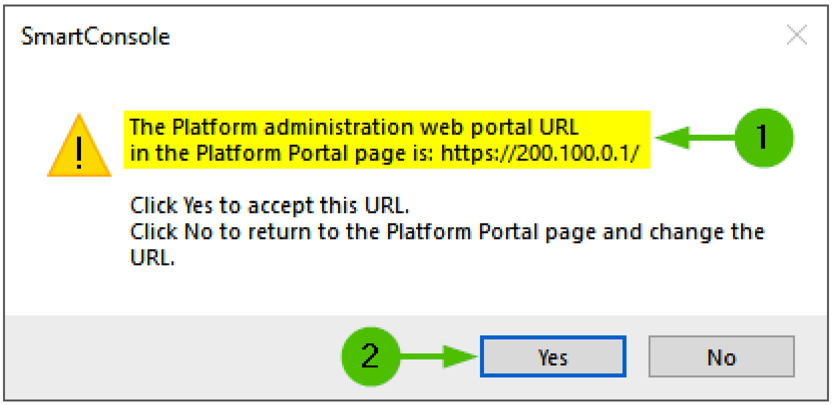
□ Don't check packets from: No item selected. View...

Spoof Tracking: Log



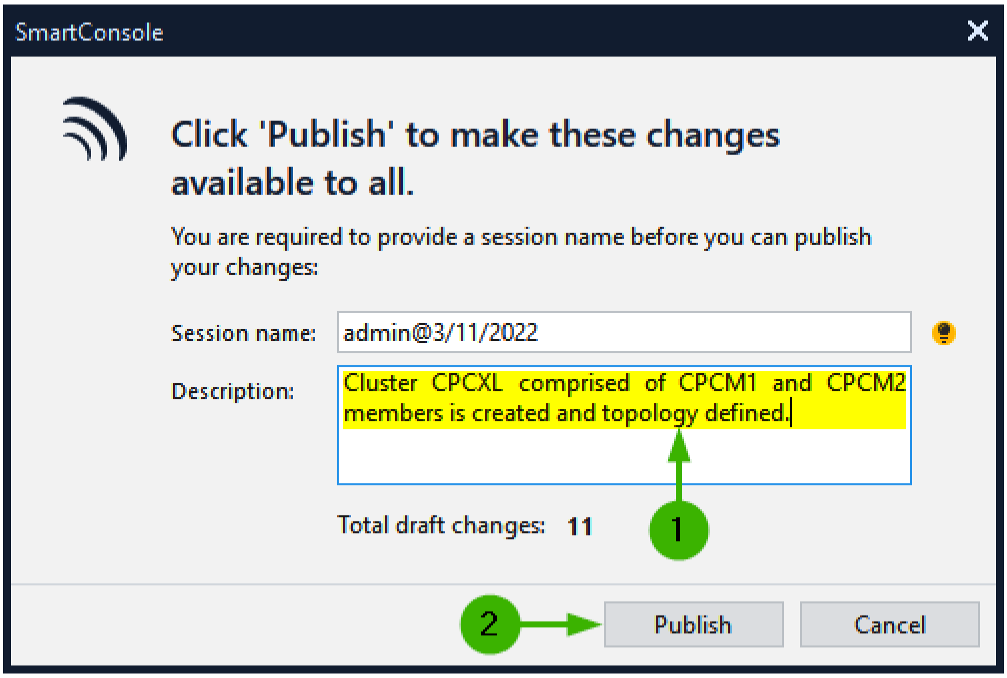
Gateway Cluster Properties - CPCXL

Name	Topology	Virtual IP	CPCM1	CPCM2	Comments
eth0	This network	10.0.0.1/24	10.0.0.2/24	10.0.0.3/24	Mgmt
eth1	This network	10.10.10.1/24	10.10.10.2/24	10.10.10.3/24	Internal1
eth2	This network	10.20.20.1/24	10.20.20.2/24	10.20.20.3/24	Internal2
eth3	This network	Sync	192.168.255.1/24	192.168.255.2/24	Sync
eth4	External	200.100.0.1/24	200.100.0.2/24	200.100.0.3/24	External
eth5	This network, DMZ	10.30.30.1/24	10.30.30.2/24	10.30.30.3/24	DMZ


SmartConsole

The Platform administration web portal URL in the Platform Portal page is: https://200.100.0.1/

Click Yes to accept this URL.
Click No to return to the Platform Portal page and change the URL.


SmartConsole

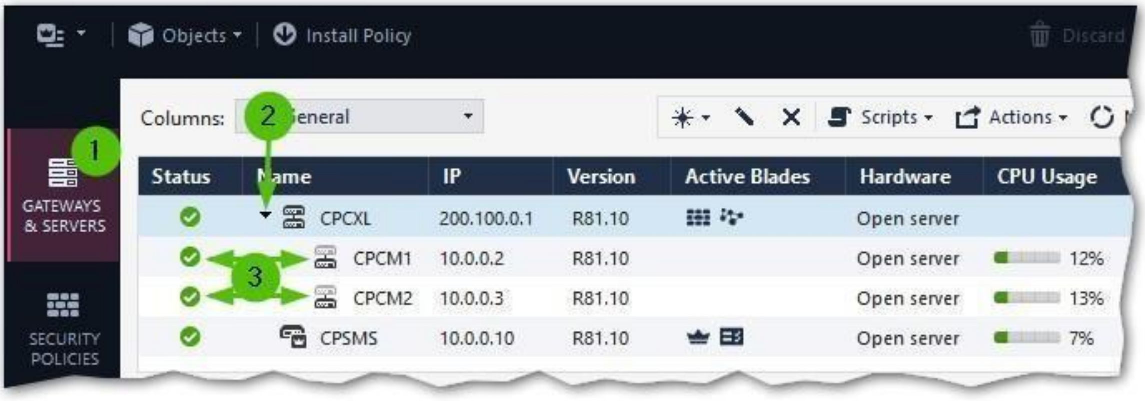
Click 'Publish' to make these changes available to all.

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

Session name: admin@3/11/2022

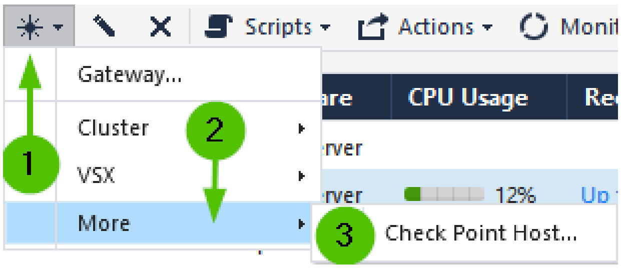
Description: Cluster CPCXL comprised of CPCM1 and CPCM2 members is created and topology defined.

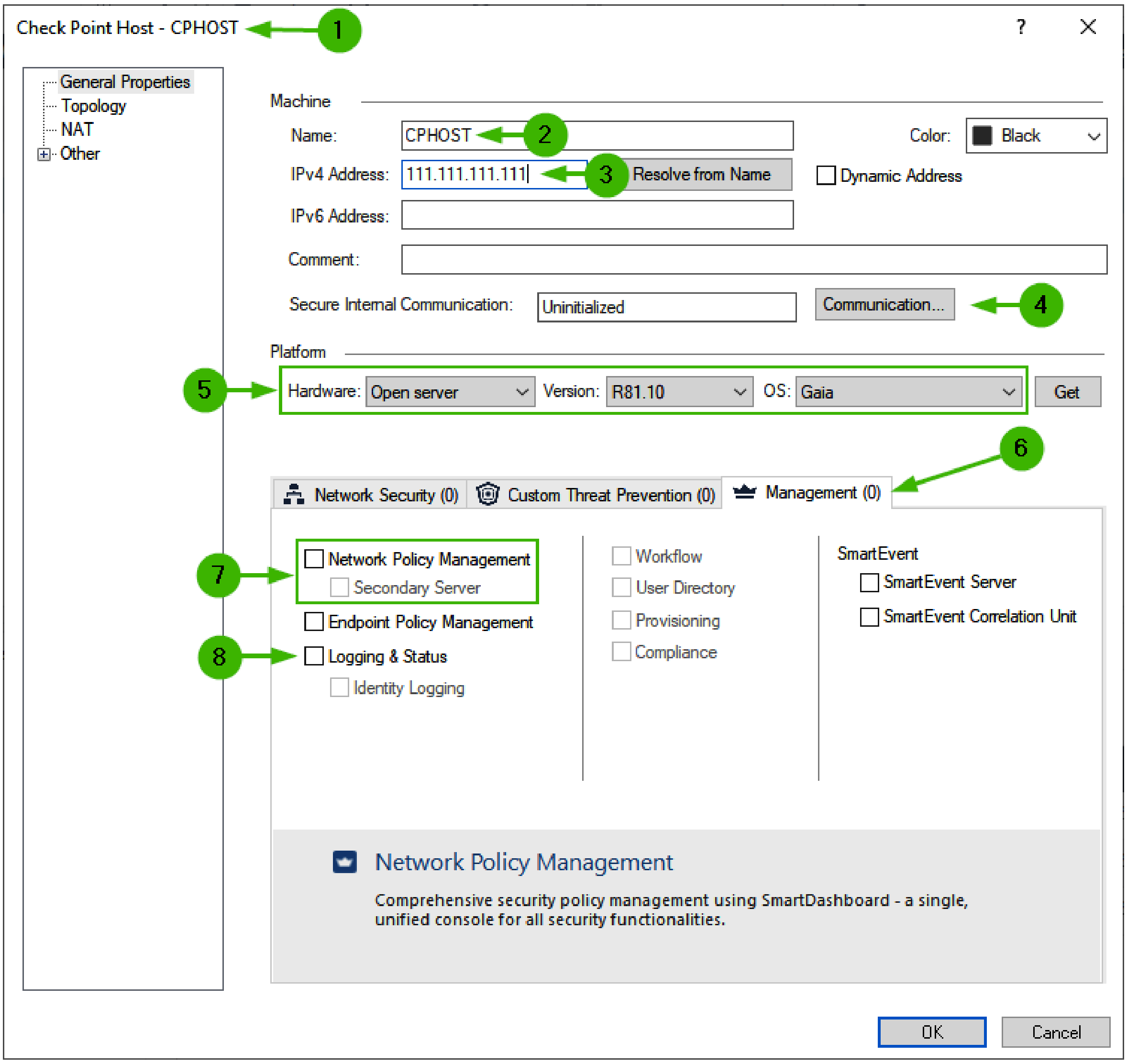
Total draft changes: 11



Columns: General

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage
✓	CPCXL	200.100.0.1	R81.10		Open server	
✓	CPCM1	10.0.0.2	R81.10		Open server	12%
✓	CPCM2	10.0.0.3	R81.10		Open server	13%
✓	CPSMS	10.0.0.10	R81.10		Open server	7%




Check Point Host - CPHOST

General Properties
Topology
NAT
Other

Machine

Name: CPHOST

IPv4 Address: 111.111.111.111

IPv6 Address:

Comment:

Color: Black

☐ Dynamic Address

Secure Internal Communication: Uninitialized

Platform

Hardware: Open server Version: R81.10 OS: Gaia

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

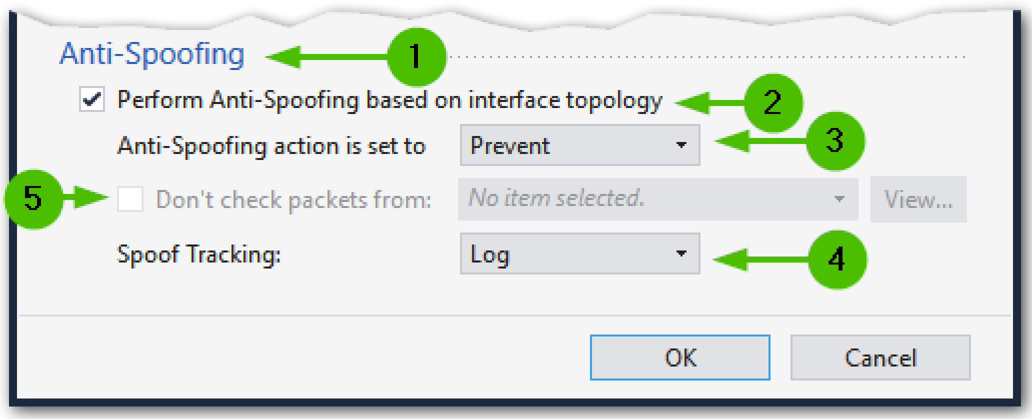
☐ Network Policy Management
☐ Secondary Server
☐ Endpoint Policy Management
☐ Logging & Status
☐ Identity Logging

☐ Workflow
☐ User Directory
☐ Provisioning
☐ Compliance

SmartEvent
☐ SmartEvent Server
☐ SmartEvent Correlation Unit

Network Policy Management

Comprehensive security policy management using SmartDashboard - a single, unified console for all security functionalities.



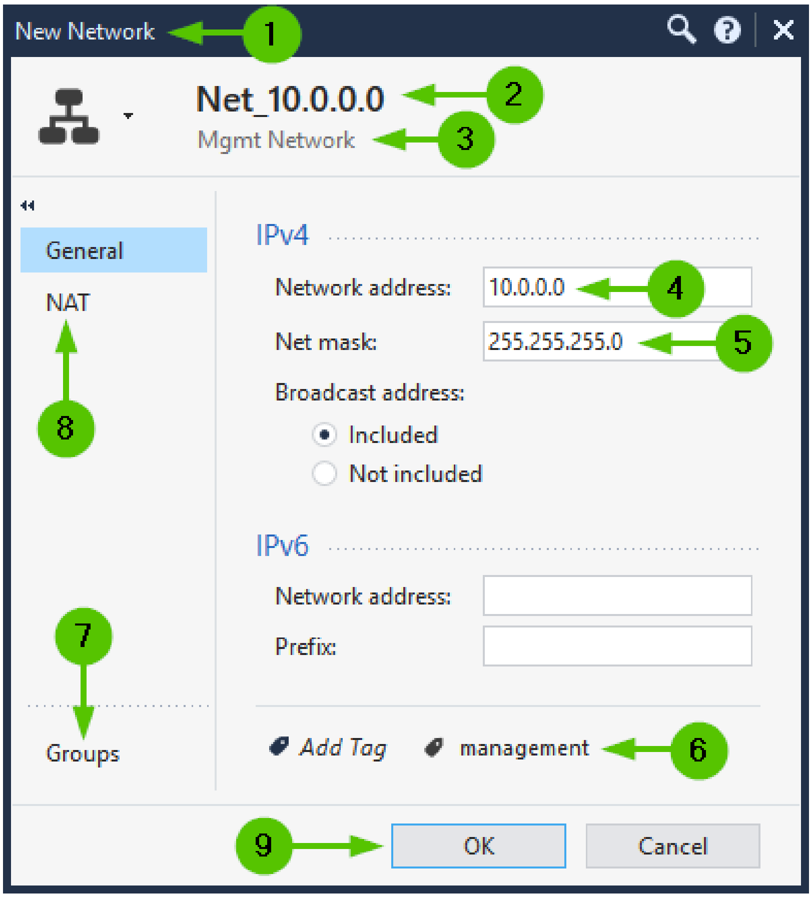
Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to: Prevent

□ Don't check packets from: *No item selected.*

Spoof Tracking: Log



New Network

Net_10.0.0.0

Mgmt Network

IPv4

Network address: 10.0.0.0

Net mask: 255.255.255.0

Broadcast address:

● Included

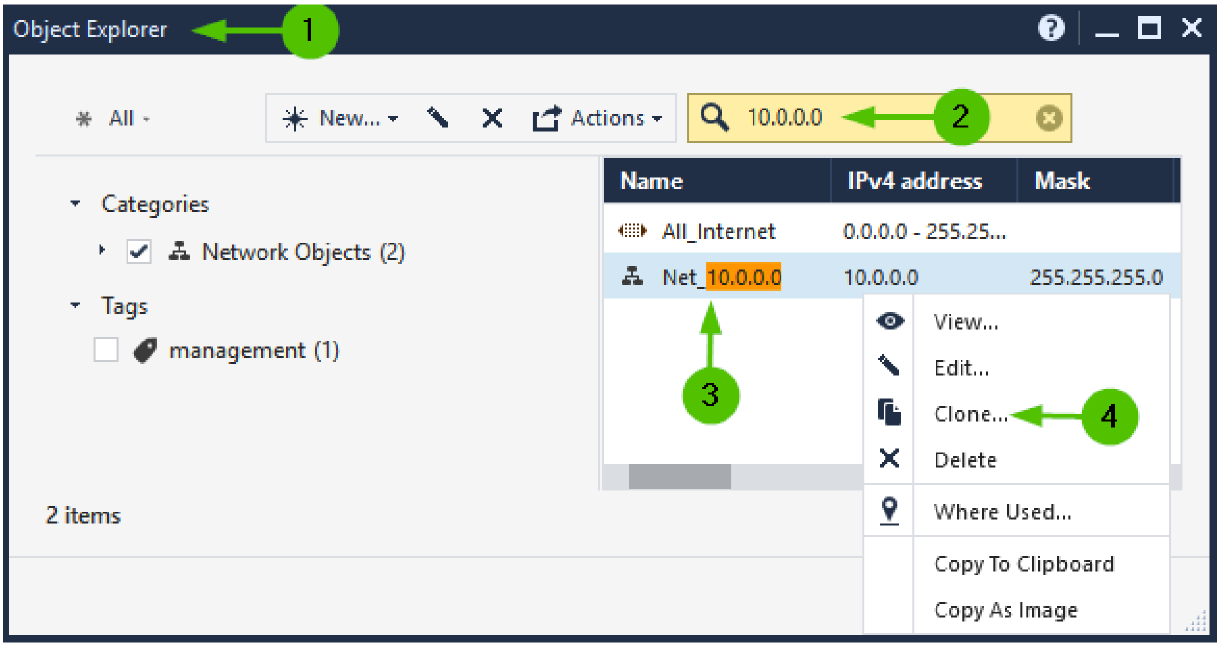
○ Not included

IPv6

Network address:

Prefix:

Add Tag | management

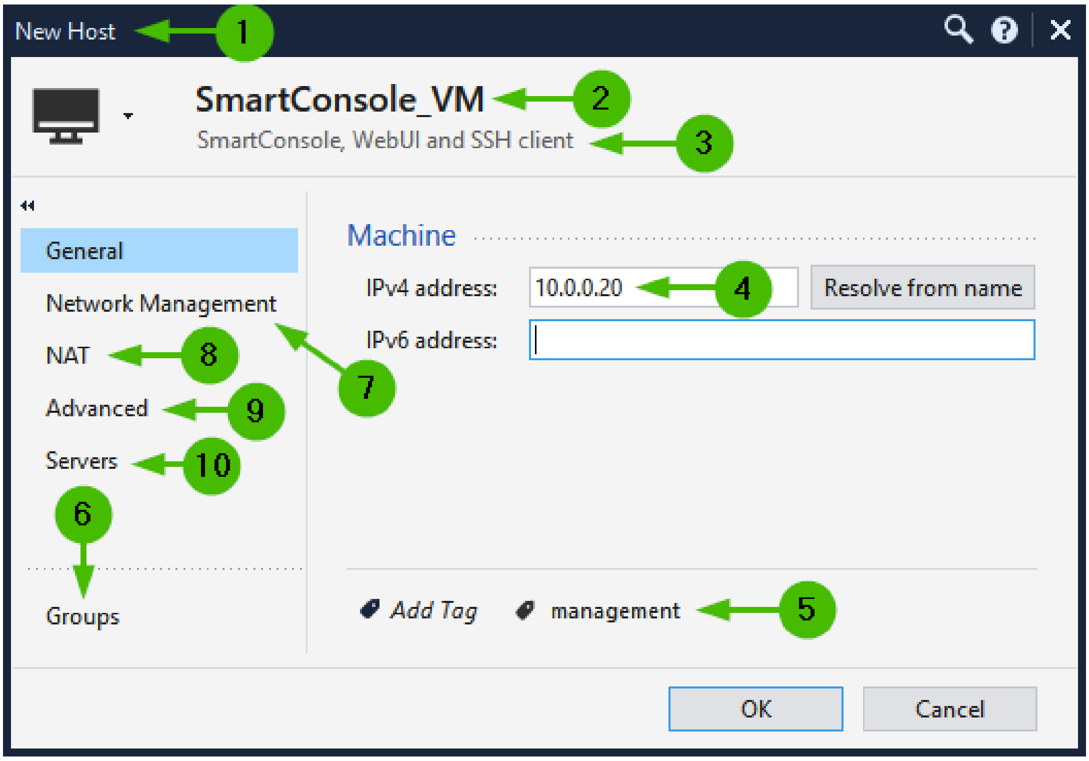


Object Explorer

Search: 10.0.0.0

Name	IPv4 address	Mask
All_Internet	0.0.0.0 - 255.25...	
Net_10.0.0.0	10.0.0.0	255.255.255.0

2 items



New Host

SmartConsole_VM

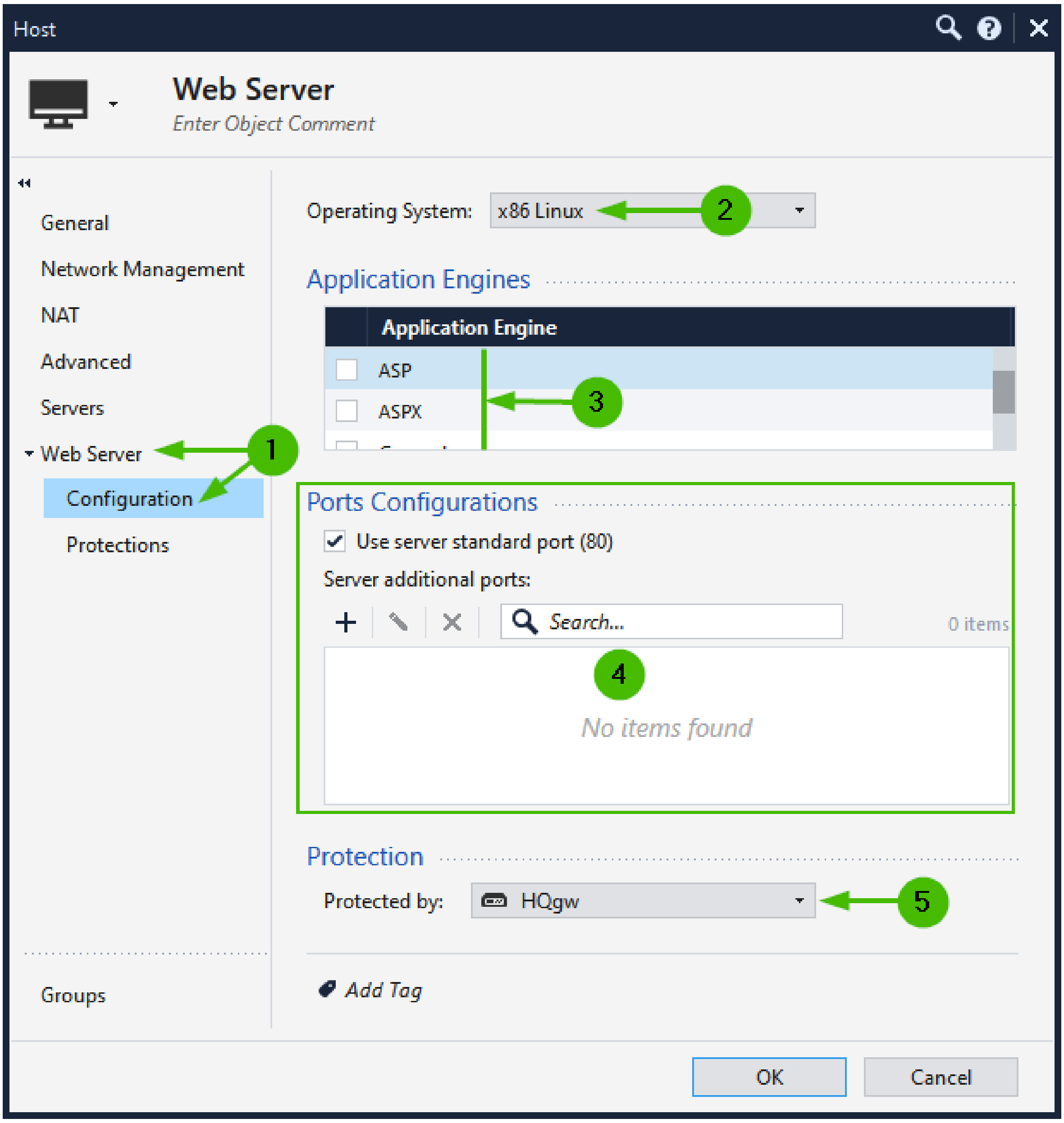
SmartConsole, WebUI and SSH client

Machine

IPv4 address: 10.0.0.20

IPv6 address:

management



Web Server

Enter Object Comment

Operating System: x86 Linux

Application Engines

	Application Engine
□	ASP
□	ASPX

Ports Configurations

☑ Use server standard port (80)

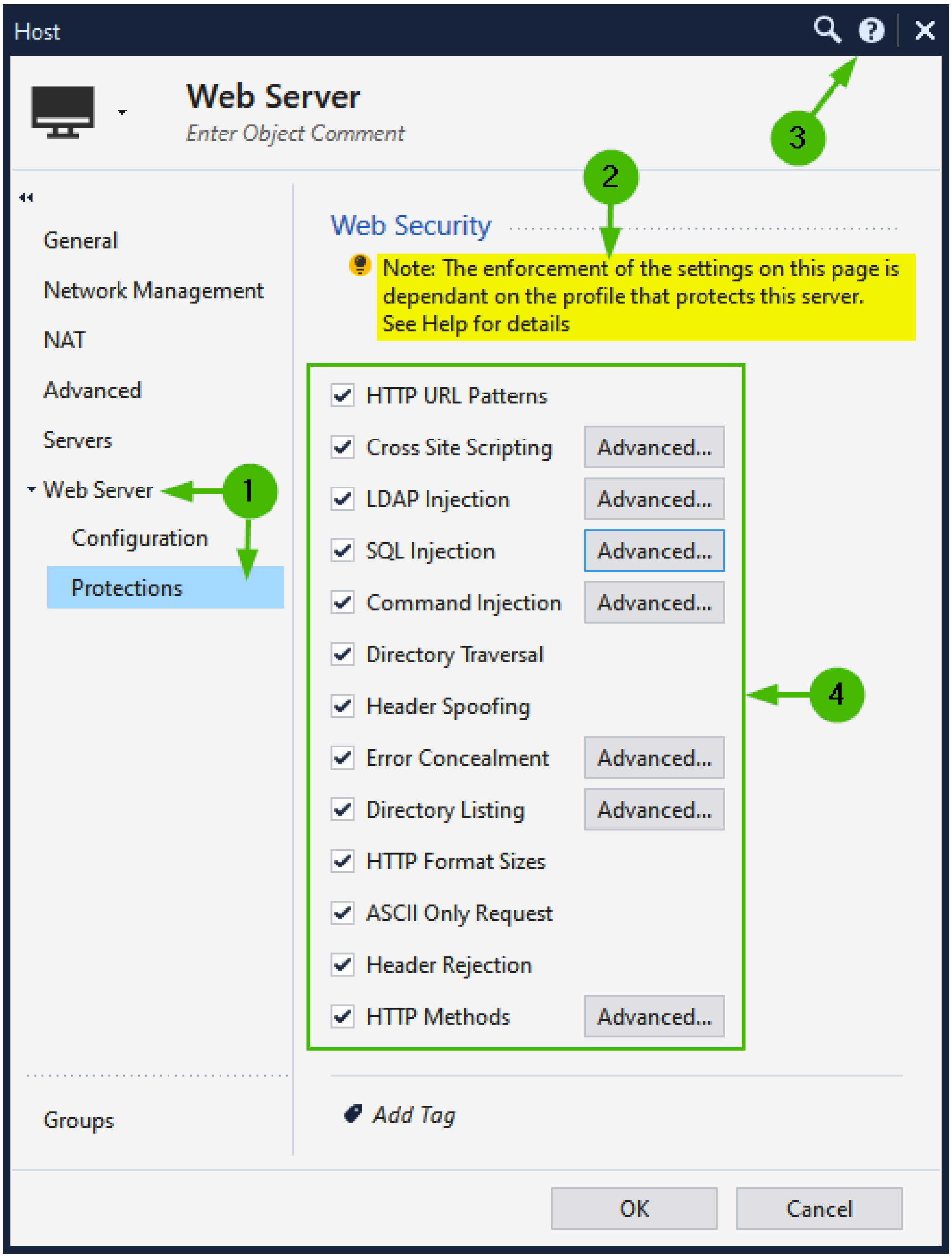
Server additional ports:

Search... 0 items

No items found

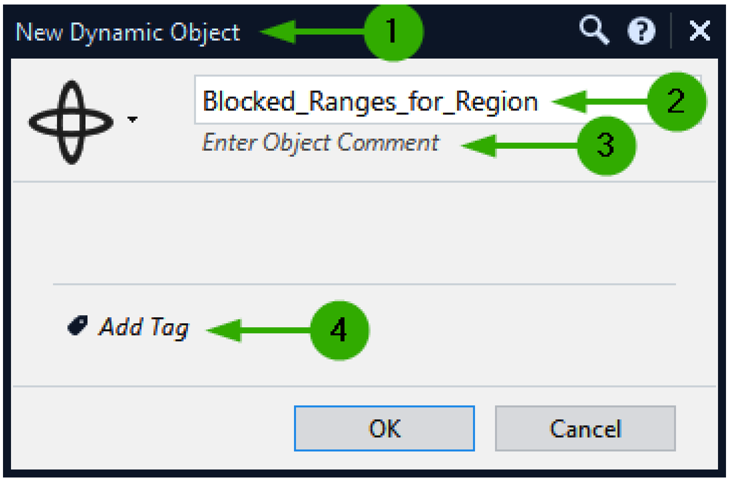
Protection

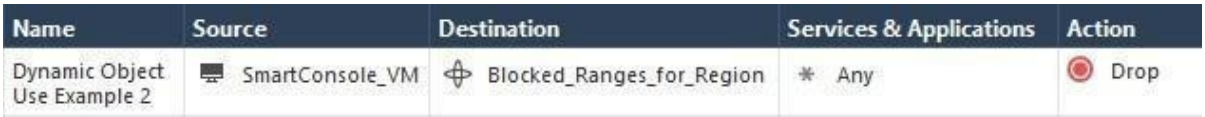
Protected by: HQgw



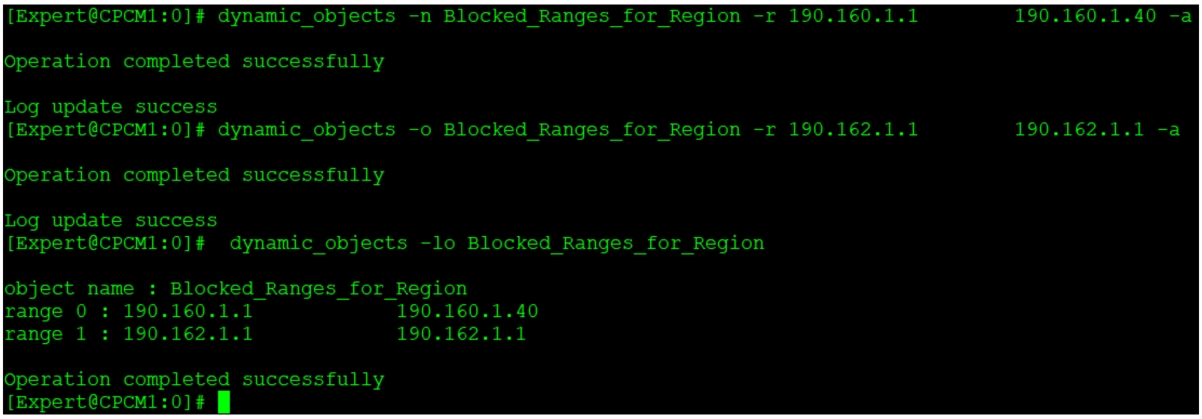
Note: The enforcement of the settings on this page is dependant on the profile that protects this server. See Help for details

- ☑ HTTP URL Patterns
- ☑ Cross Site Scripting — Advanced...
- ☑ LDAP Injection — Advanced...
- ☑ SQL Injection — Advanced...
- ☑ Command Injection — Advanced...
- ☑ Directory Traversal
- ☑ Header Spoofing
- ☑ Error Concealment — Advanced...
- ☑ Directory Listing — Advanced...
- ☑ HTTP Format Sizes
- ☑ ASCII Only Request
- ☑ Header Rejection
- ☑ HTTP Methods — Advanced...

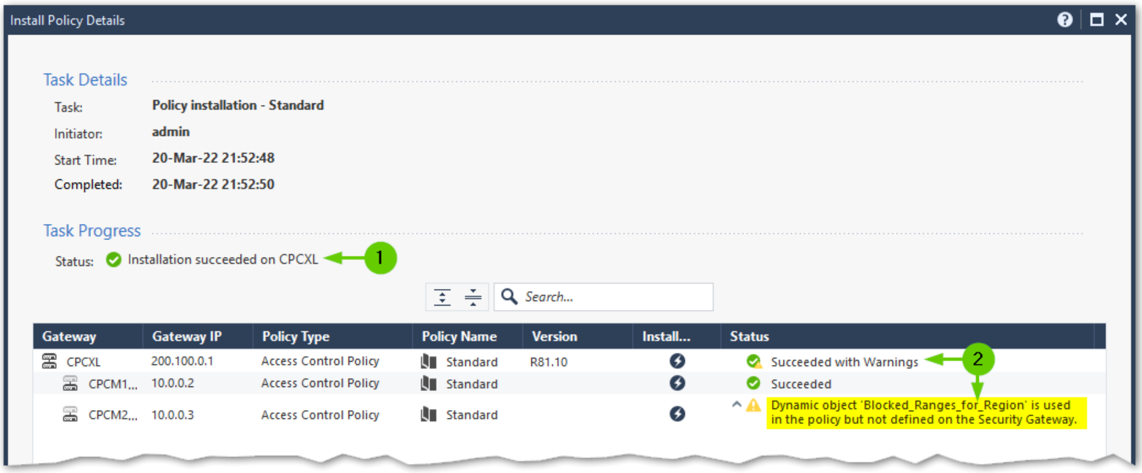




Name	Source	Destination	Services & Applications	Action
Dynamic Object Use Example 2	SmartConsole_VM	Blocked_Ranges_for_Region	Any	Drop



```
[Expert@CPCM1:0]# dynamic_objects -n Blocked_Ranges_for_Region -r 190.160.1.1        190.160.1.40 -a

Operation completed successfully

Log update success
[Expert@CPCM1:0]# dynamic_objects -o Blocked_Ranges_for_Region -r 190.162.1.1        190.162.1.1 -a

Operation completed successfully

Log update success
[Expert@CPCM1:0]#  dynamic_objects -lo Blocked_Ranges_for_Region

object name : Blocked_Ranges_for_Region
range 0 : 190.160.1.1            190.160.1.40
range 1 : 190.162.1.1            190.162.1.1

Operation completed successfully
[Expert@CPCM1:0]# █
```



Install Policy Details

Task Details

Task: **Policy installation - Standard**

Initiator: **admin**

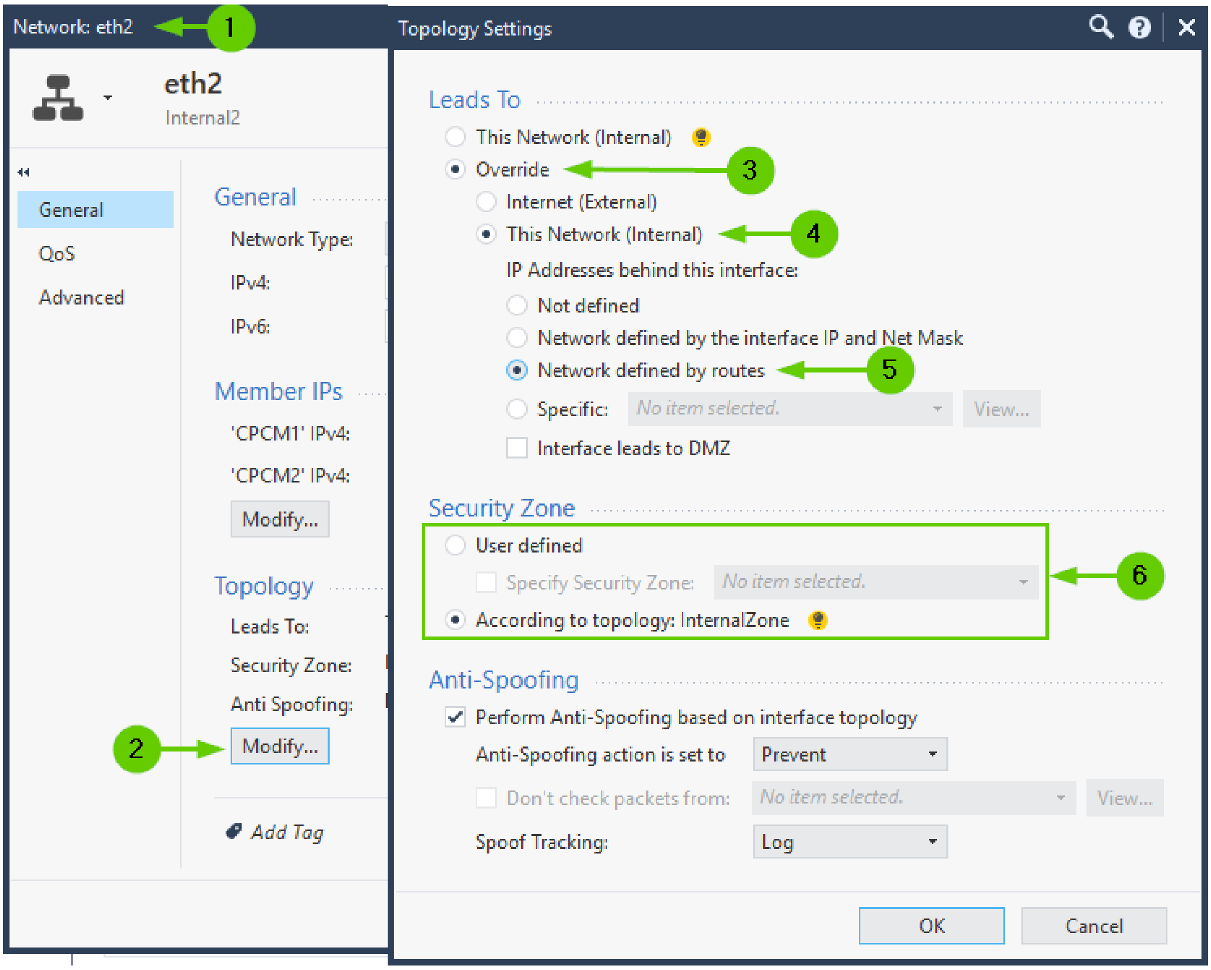
Start Time: **20-Mar-22 21:52:48**

Completed: **20-Mar-22 21:52:50**

Task Progress

Status: ✓ Installation succeeded on CPCXL

Gateway	Gateway IP	Policy Type	Policy Name	Version	Install...	Status
CPCXL	200.100.0.1	Access Control Policy	Standard	R81.10	⚡	✓ Succeeded with Warnings
CPCM1...	10.0.0.2	Access Control Policy	Standard		⚡	✓ Succeeded
CPCM2...	10.0.0.3	Access Control Policy	Standard		⚡	⚠ Dynamic object 'Blocked_Ranges_for_Region' is used in the policy but not defined on the Security Gateway.



Network: eth2

eth2
Internal2

General
QoS
Advanced

General
Network Type:
IPv4:
IPv6:

Member IPs
'CPCM1' IPv4:
'CPCM2' IPv4:
Modify...

Topology
Leads To:
Security Zone:
Anti Spoofing:
Modify...

Add Tag

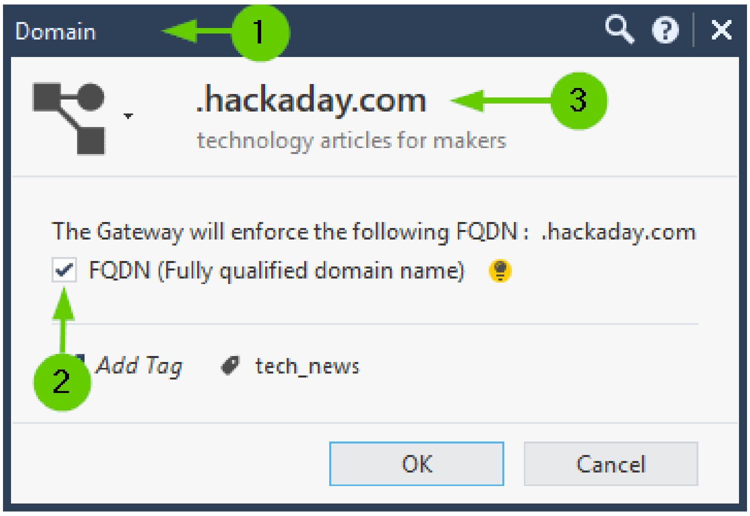
Topology Settings

Leads To
- ○ This Network (Internal)
- ● Override
  - ○ Internet (External)
  - ● This Network (Internal)
    - IP Addresses behind this interface:
    - ○ Not defined
    - ○ Network defined by the interface IP and Net Mask
    - ● Network defined by routes
    - ○ Specific: *No item selected.* View...
    - □ Interface leads to DMZ

Security Zone
- ○ User defined
  - □ Specify Security Zone: *No item selected.*
- ● According to topology: InternalZone

Anti-Spoofing
- ☑ Perform Anti-Spoofing based on interface topology
  - Anti-Spoofing action is set to: Prevent
  - □ Don't check packets from: *No item selected.* View...
  - Spoof Tracking: Log

OK Cancel



Domain

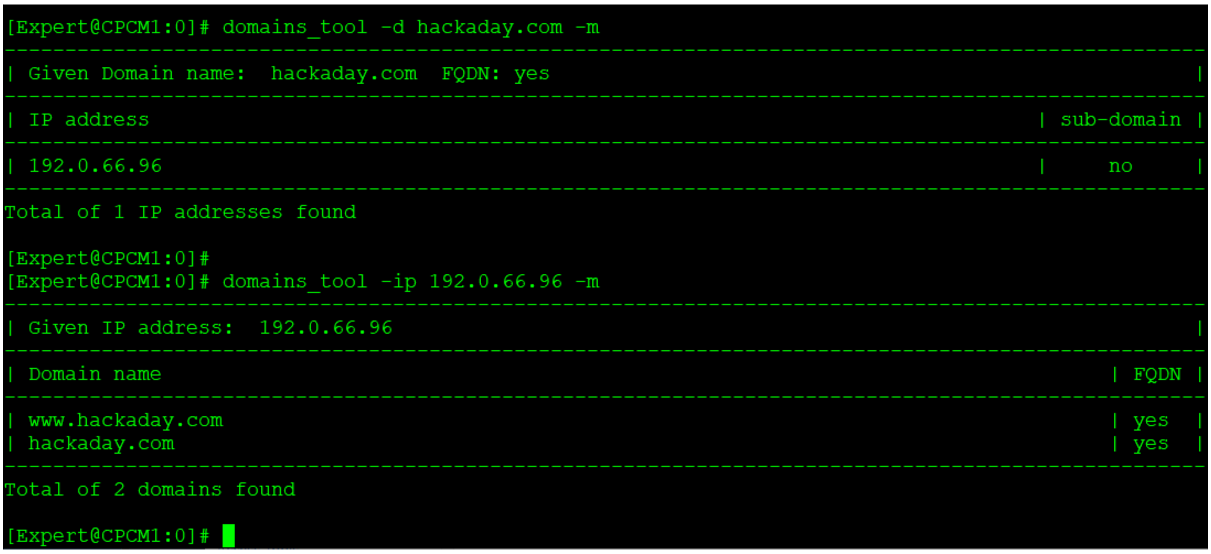
.hackaday.com
technology articles for makers

The Gateway will enforce the following FQDN : .hackaday.com

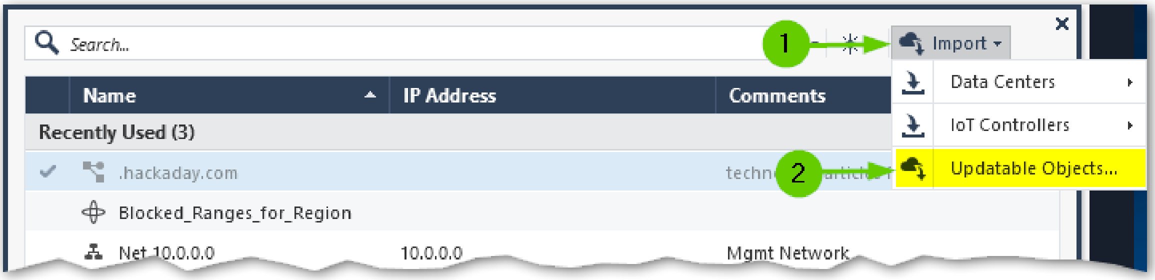
☑ FQDN (Fully qualified domain name)

Add Tag tech_news

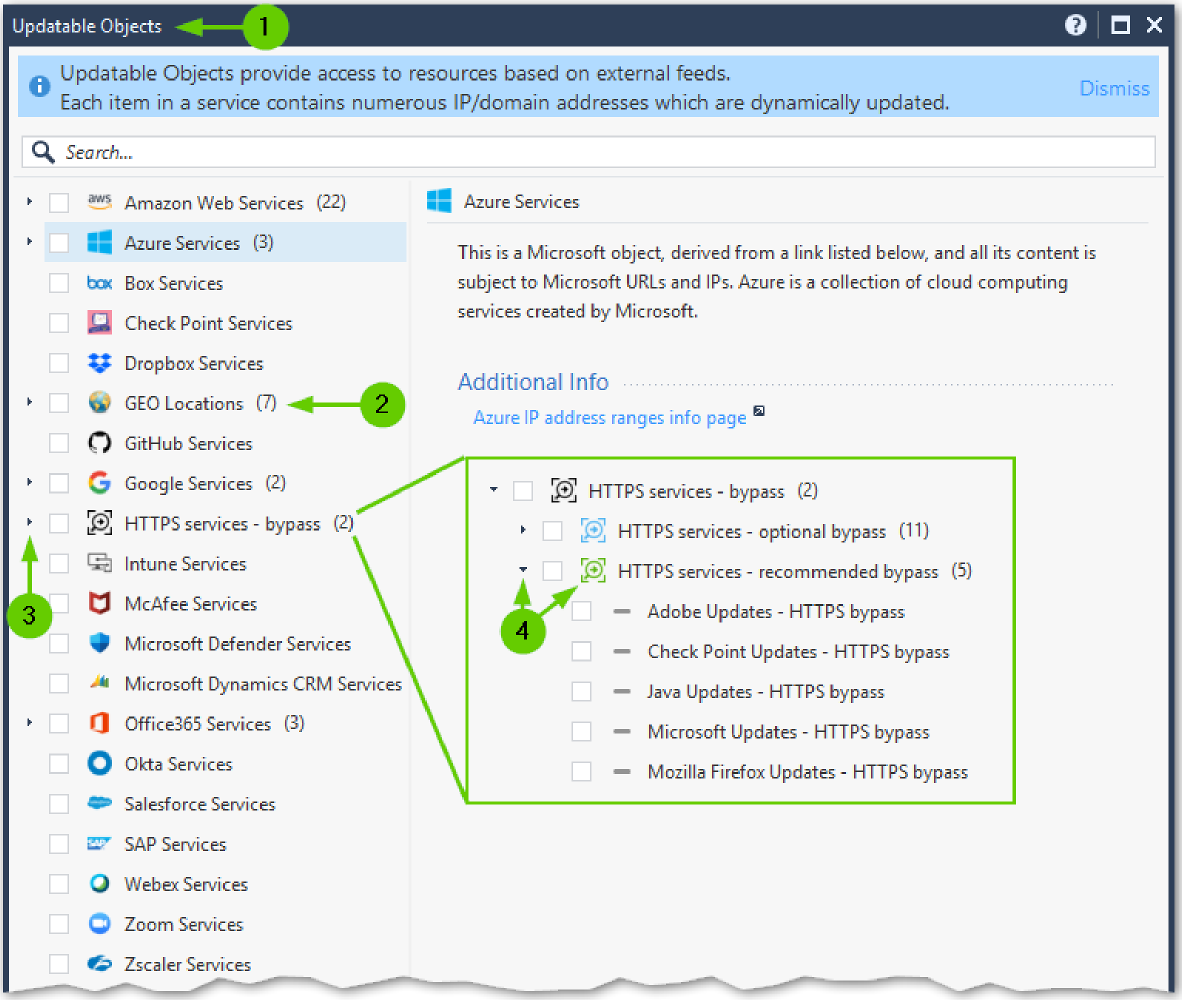
OK Cancel



```
[Expert@CPCM1:0]# domains_tool -d hackaday.com -m
---------------------------------------------------------------------------------------------------
| Given Domain name:  hackaday.com  FQDN: yes                                                      |
---------------------------------------------------------------------------------------------------
| IP address                                                                         | sub-domain |
---------------------------------------------------------------------------------------------------
| 192.0.66.96                                                                        |     no     |
---------------------------------------------------------------------------------------------------
Total of 1 IP addresses found

[Expert@CPCM1:0]#
[Expert@CPCM1:0]# domains_tool -ip 192.0.66.96 -m
---------------------------------------------------------------------------------------------------
| Given IP address:  192.0.66.96                                                                   |
---------------------------------------------------------------------------------------------------
| Domain name                                                                              | FQDN |
---------------------------------------------------------------------------------------------------
| www.hackaday.com                                                                         | yes  |
| hackaday.com                                                                             | yes  |
---------------------------------------------------------------------------------------------------
Total of 2 domains found

[Expert@CPCM1:0]#
```

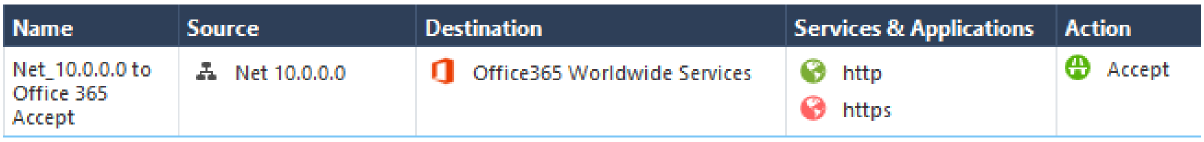


	Name	IP Address	Comments
	Recently Used (3)		
✓	.hackaday.com		techn... artic...
	Blocked_Ranges_for_Region		
	Net 10.0.0.0	10.0.0.0	Mgmt Network

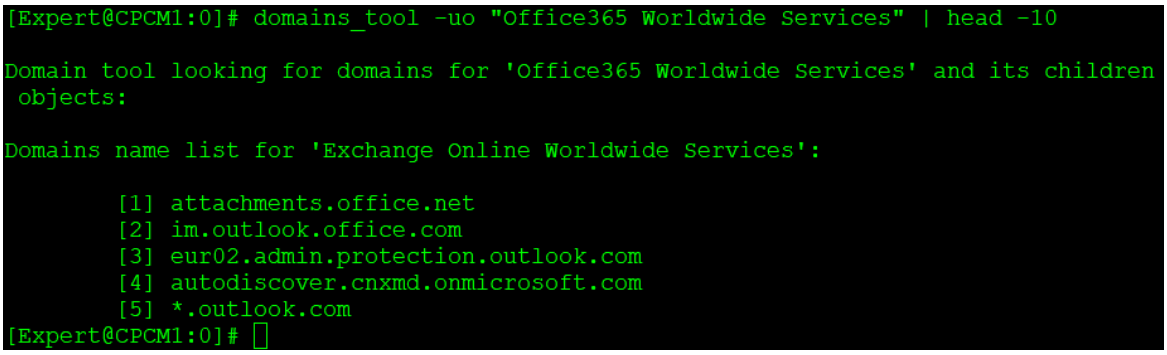

Updatable Objects
1
Dismiss
Search...
Amazon Web Services (22)
Azure Services (3)
Box Services
Check Point Services
Dropbox Services
GEO Locations (7)
2
GitHub Services
Google Services (2)
HTTPS services - bypass (2)
Intune Services
3
McAfee Services
Microsoft Defender Services
Microsoft Dynamics CRM Services
Office365 Services (3)
Okta Services
Salesforce Services
SAP Services
Webex Services
Zoom Services
Zscaler Services
Azure Services
Additional Info
Azure IP address ranges info page
HTTPS services - bypass (2)
HTTPS services - optional bypass (11)
HTTPS services - recommended bypass (5)
4
Adobe Updates - HTTPS bypass
Check Point Updates - HTTPS bypass
Java Updates - HTTPS bypass
Microsoft Updates - HTTPS bypass
Mozilla Firefox Updates - HTTPS bypass

Updatable Objects provide access to resources based on external feeds.
Each item in a service contains numerous IP/domain addresses which are dynamically updated.

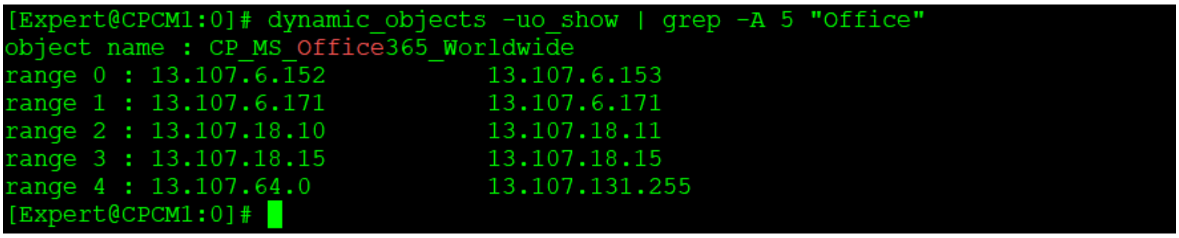
This is a Microsoft object, derived from a link listed below, and all its content is subject to Microsoft URLs and IPs. Azure is a collection of cloud computing services created by Microsoft.



Name	Source	Destination	Services & Applications	Action
Net_10.0.0.0 to Office 365 Accept	Net 10.0.0.0	Office365 Worldwide Services	http https	Accept

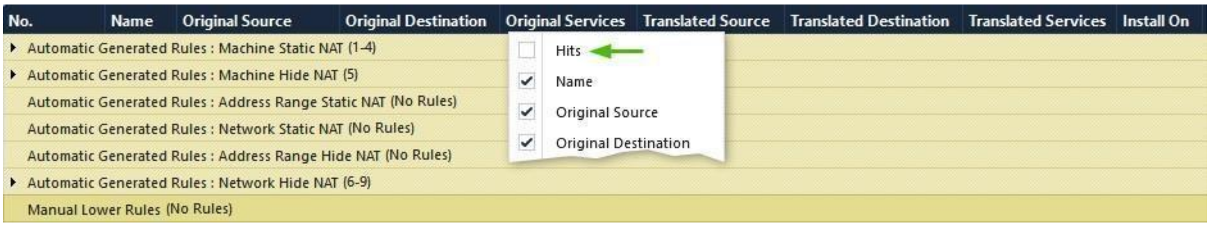


```
[Expert@CPCM1:0]# domains_tool -uo "Office365 Worldwide Services" | head -10

Domain tool looking for domains for 'Office365 Worldwide Services' and its children
 objects:

Domains name list for 'Exchange Online Worldwide Services':

        [1] attachments.office.net
        [2] im.outlook.office.com
        [3] eur02.admin.protection.outlook.com
        [4] autodiscover.cnxmd.onmicrosoft.com
        [5] *.outlook.com
[Expert@CPCM1:0]# 
```



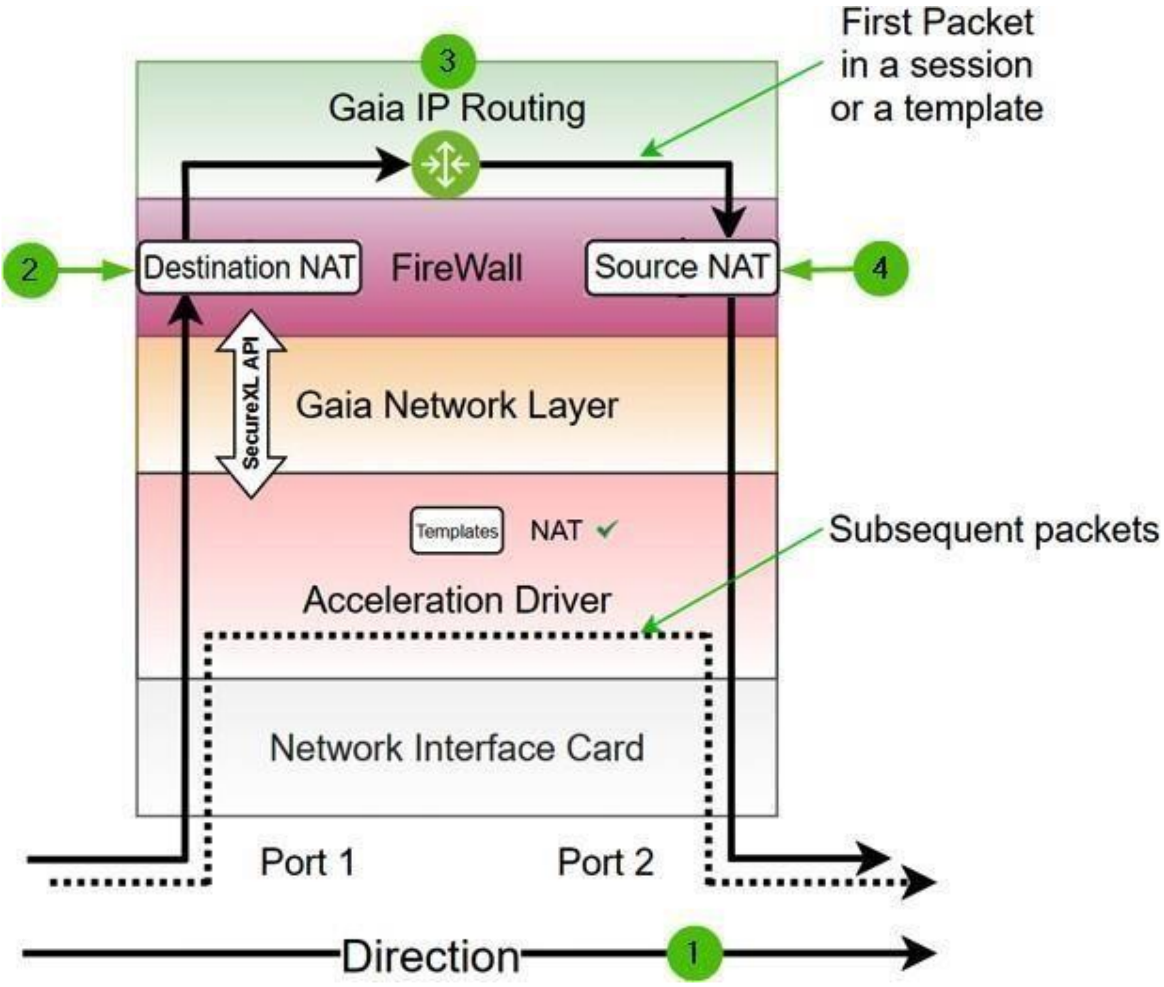
```
[Expert@CPCM1:0]# dynamic_objects -uo_show | grep -A 5 "Office"
object name : CP_MS_Office365_Worldwide
range 0 : 13.107.6.152          13.107.6.153
range 1 : 13.107.6.171          13.107.6.171
range 2 : 13.107.18.10          13.107.18.11
range 3 : 13.107.18.15          13.107.18.15
range 4 : 13.107.64.0           13.107.131.255
[Expert@CPCM1:0]#
```

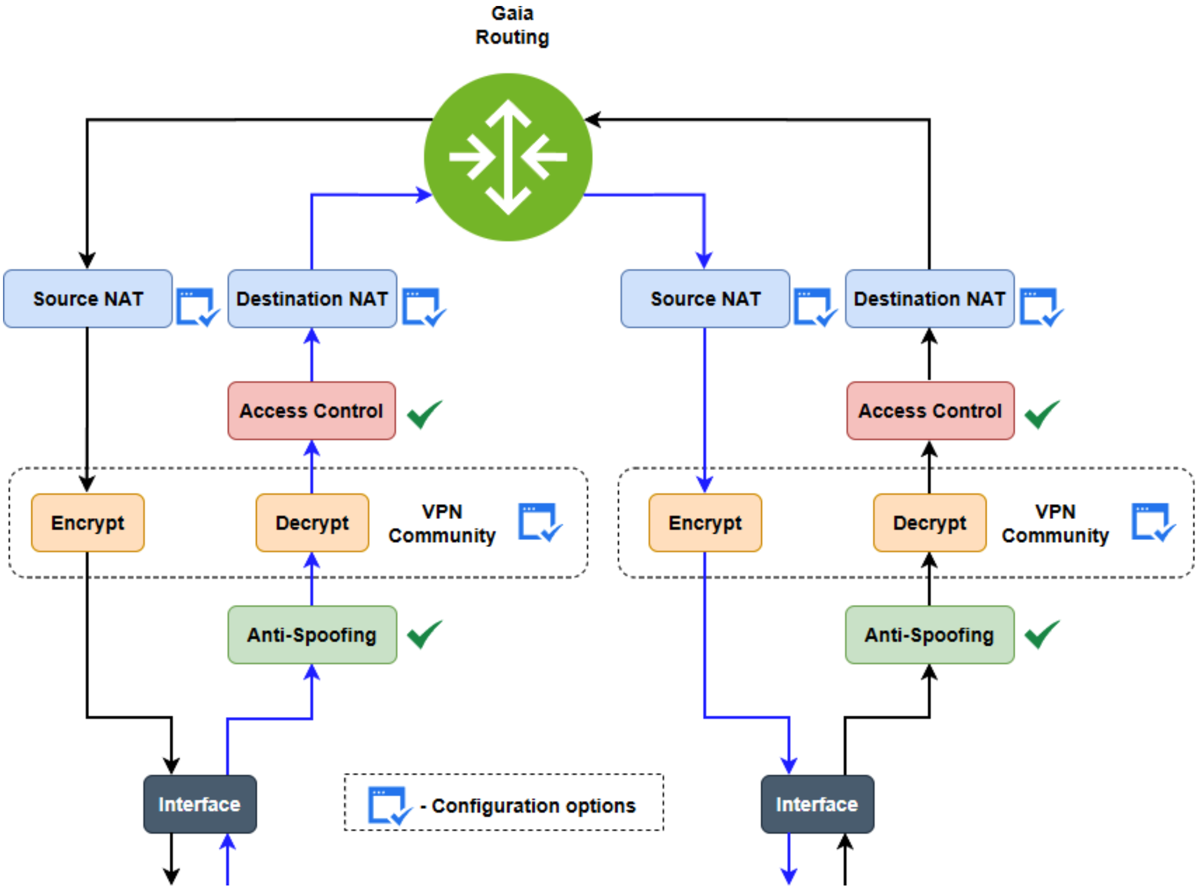
Chapter 10: Working with Network Address Translation

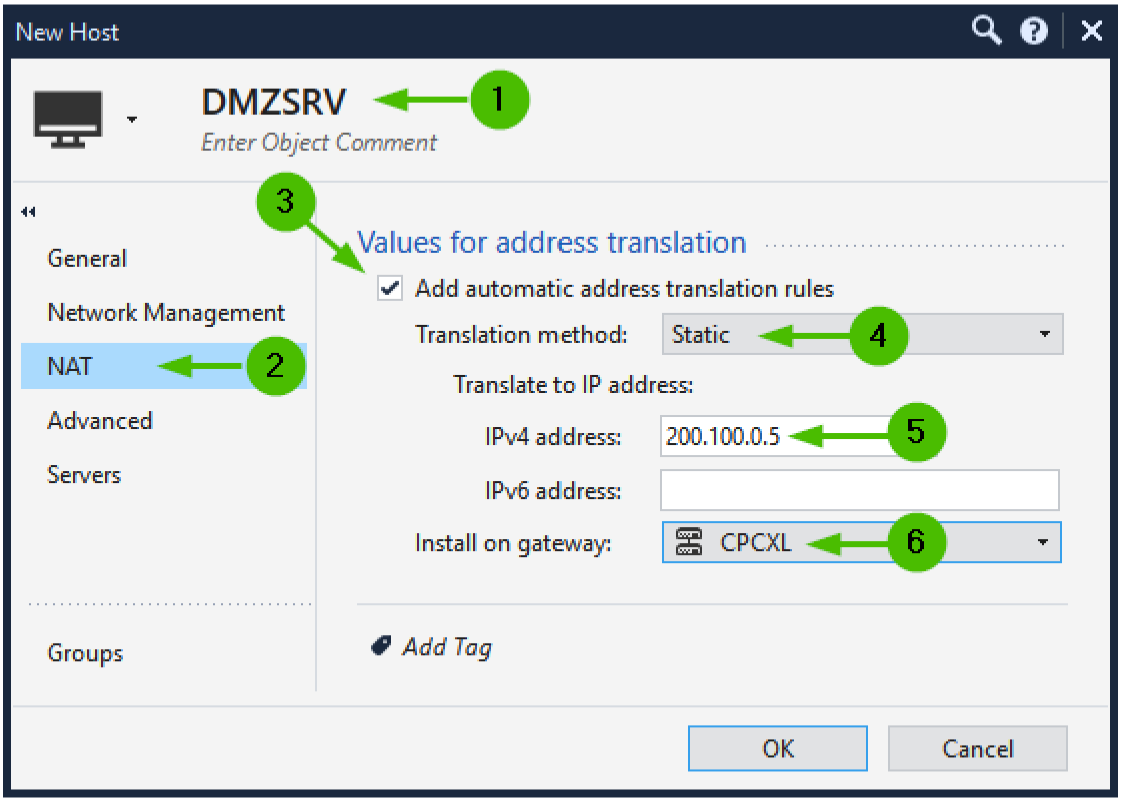


No.	Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On
▸ Automatic Generated Rules : Machine Static NAT (1-4)								
▸ Automatic Generated Rules : Machine Hide NAT (5)								
Automatic Generated Rules : Address Range Static NAT (No Rules)								
Automatic Generated Rules : Network Static NAT (No Rules)								
Automatic Generated Rules : Address Range Hide NAT (No Rules)								
▸ Automatic Generated Rules : Network Hide NAT (6-9)								
Manual Lower Rules (No Rules)								

- ☐ Hits
- ☑ Name
- ☑ Original Source
- ☑ Original Destination







DMZSRV

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

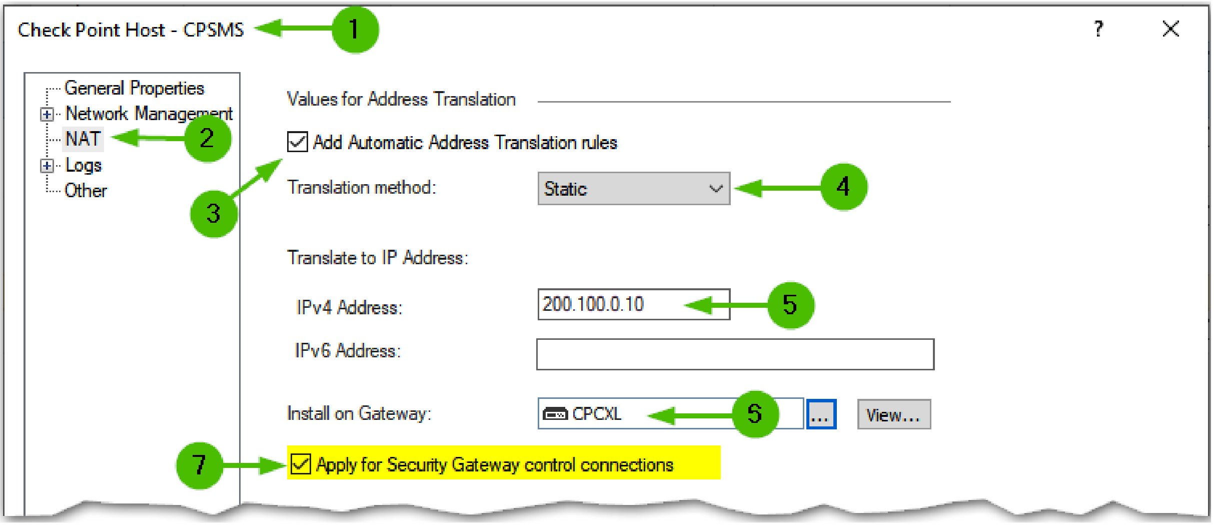
Translation method: Static

Translate to IP address:

IPv4 address: 200.100.0.5

IPv6 address:

Install on gateway: CPCXL



Check Point Host - CPSMS

Values for Address Translation

☑ Add Automatic Address Translation rules

Translation method: Static

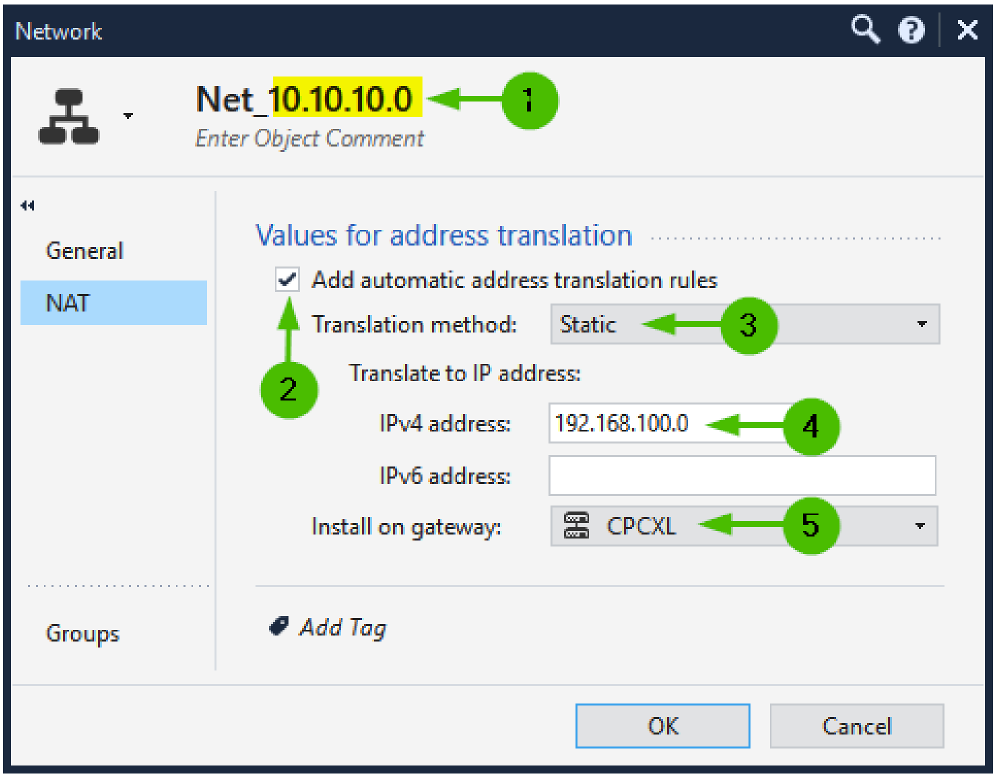
Translate to IP Address:

IPv4 Address: 200.100.0.10

IPv6 Address:

Install on Gateway: CPCXL

☑ Apply for Security Gateway control connections



Network

Net_10.10.10.0

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

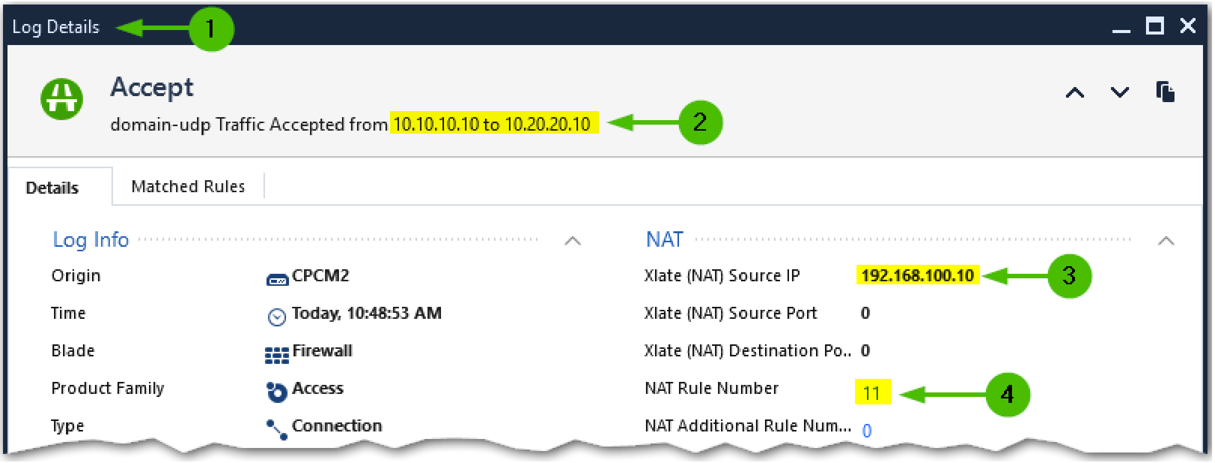
Translation method: Static

Translate to IP address:

IPv4 address: 192.168.100.0

IPv6 address:

Install on gateway: CPCXL



Log Details

Accept

domain-udp Traffic Accepted from 10.10.10.10 to 10.20.20.10

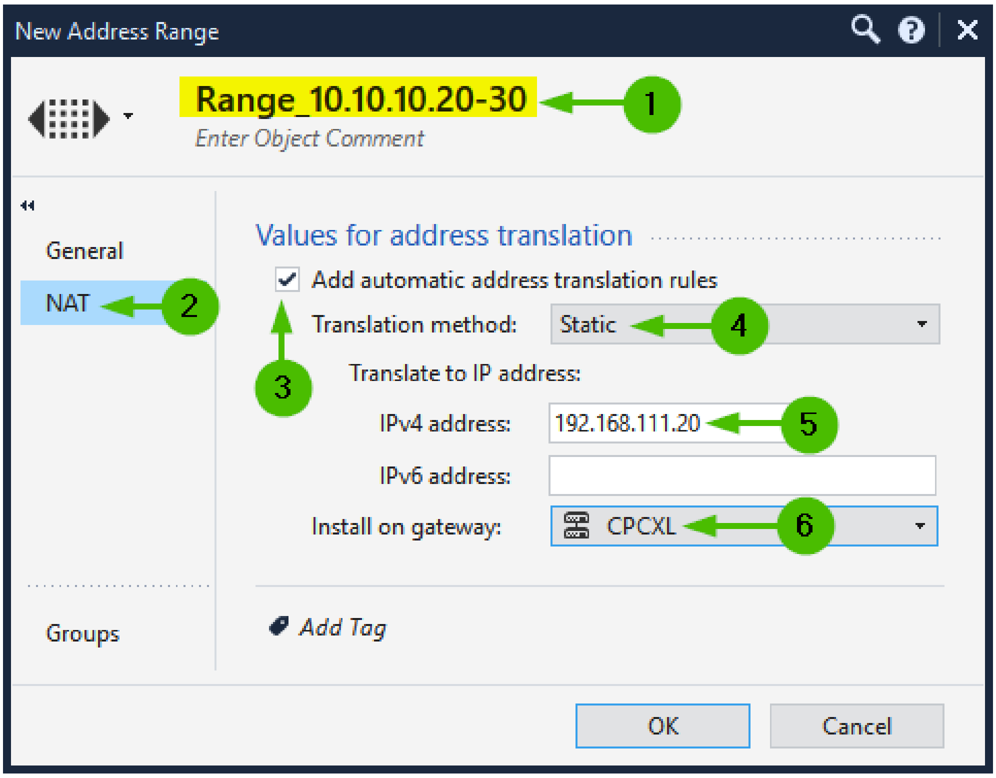
Details | Matched Rules

Log Info

Origin	CPCM2
Time	Today, 10:48:53 AM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Source IP	192.168.100.10
Xlate (NAT) Source Port	0
Xlate (NAT) Destination Po..	0
NAT Rule Number	11
NAT Additional Rule Num...	0



New Address Range

Range_10.10.10.20-30

Enter Object Comment

General

NAT

Groups

Values for address translation

☑ Add automatic address translation rules

Translation method: Static

Translate to IP address:

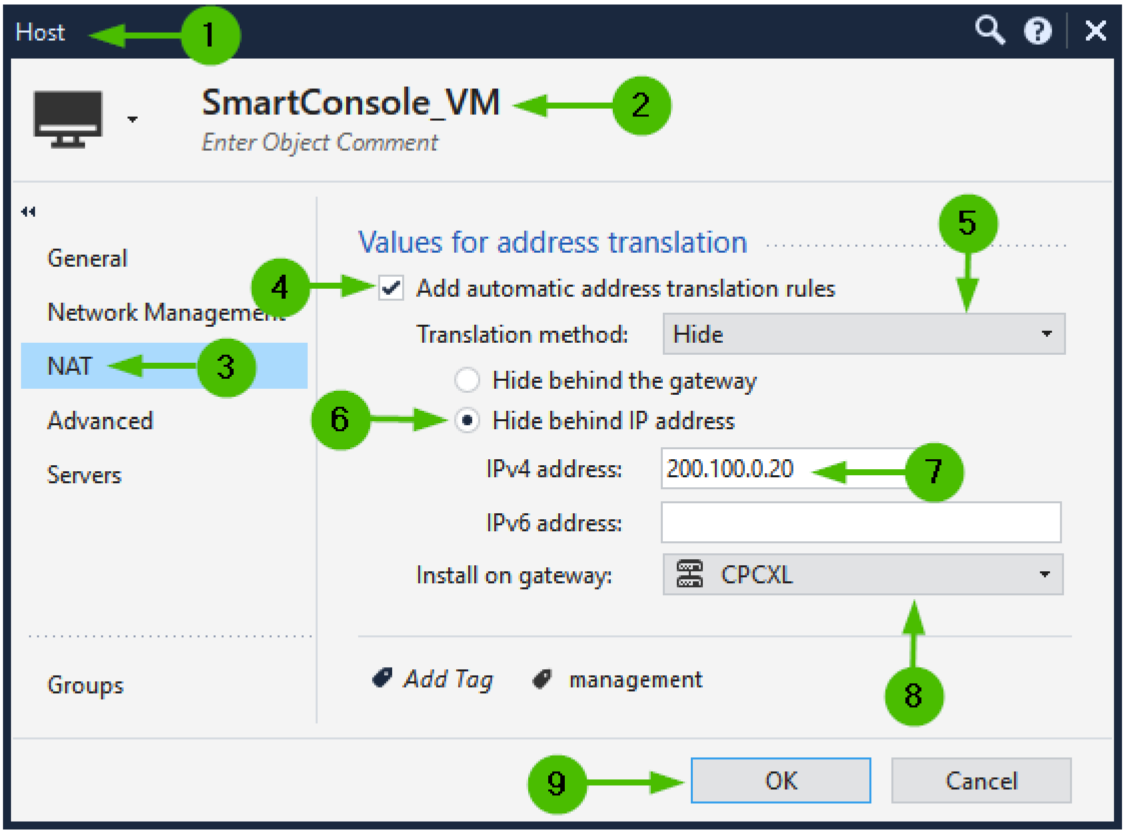
IPv4 address: 192.168.111.20

IPv6 address:

Install on gateway: CPCXL

Add Tag

OK | Cancel



Host

SmartConsole_VM

Enter Object Comment

General

Network Management

NAT

Advanced

Servers

Groups

Values for address translation

☑ Add automatic address translation rules

Translation method: Hide

○ Hide behind the gateway

● Hide behind IP address

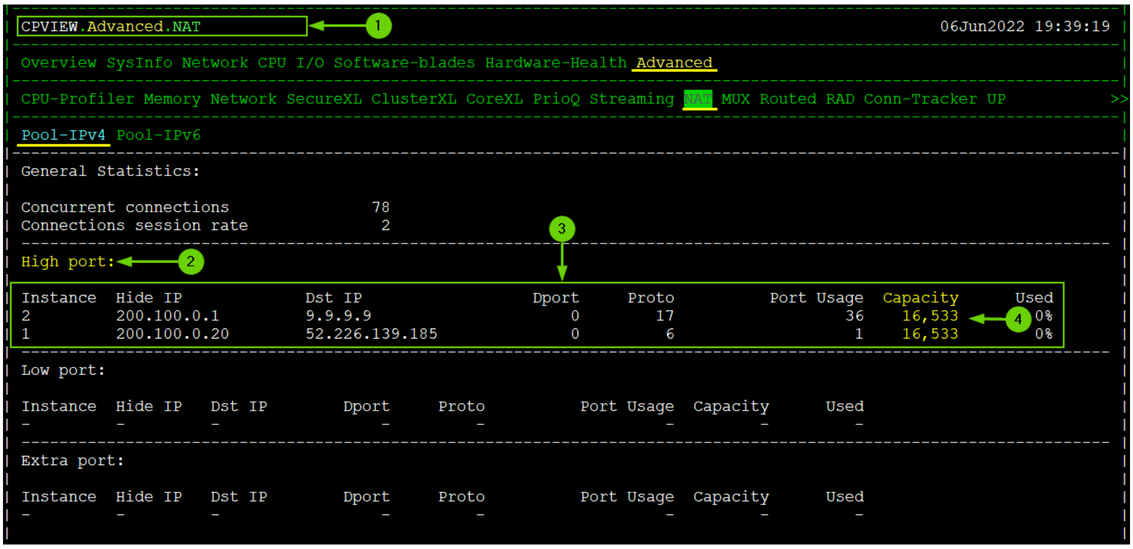
IPv4 address: 200.100.0.20

IPv6 address:

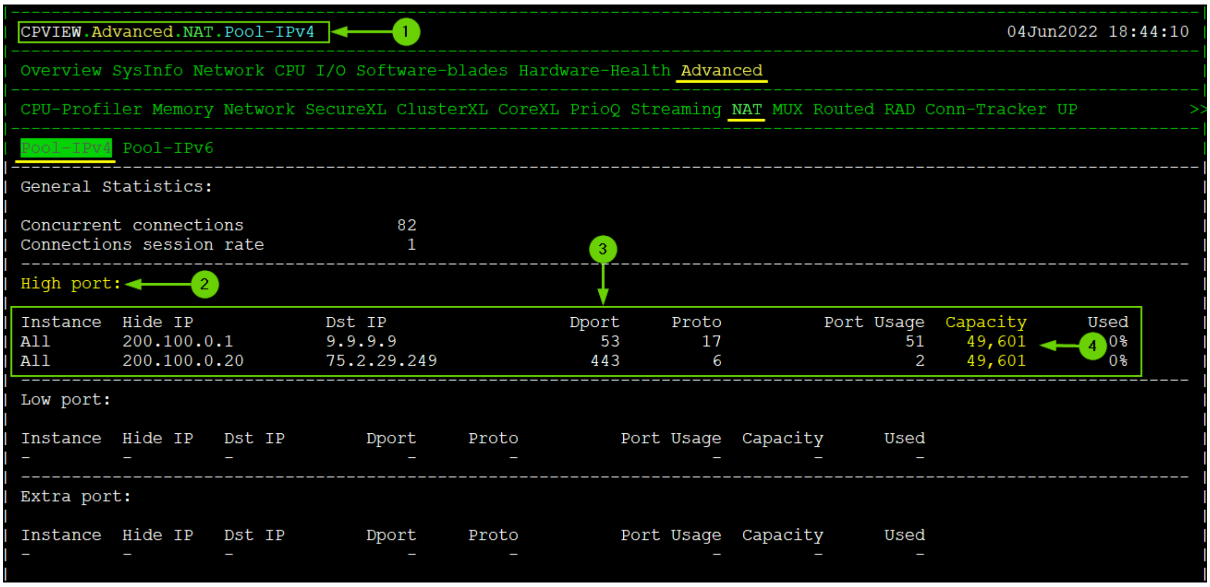
Install on gateway: CPCXL

Add Tag management

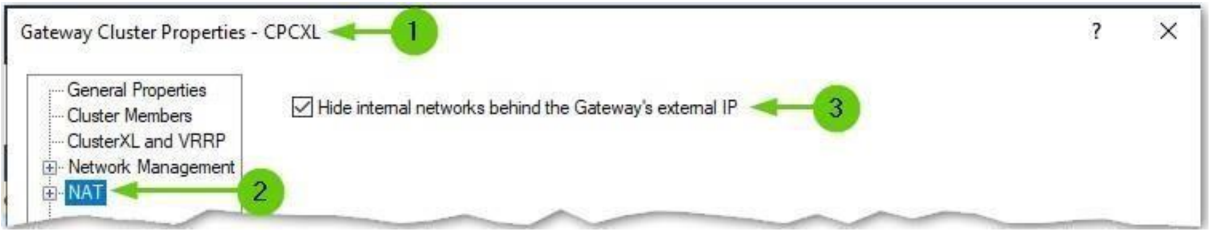
OK Cancel



```
CPVIEW.Advanced.NAT                                                   06Jun2022 19:39:19

Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced

CPU-Profiler Memory Network SecureXL ClusterXL CoreXL PrioQ Streaming NAT MUX Routed RAD Conn-Tracker UP  >>

Pool-IPv4 Pool-IPv6

General Statistics:

Concurrent connections                78
Connections session rate               2

High port:

Instance  Hide IP             Dst IP                 Dport     Proto          Port Usage  Capacity      Used
2         200.100.0.1         9.9.9.9                    0        17                  36    16,533        0%
1         200.100.0.20        52.226.139.185             0         6                   1    16,533        0%

Low port:

Instance  Hide IP  Dst IP         Dport     Proto          Port Usage  Capacity      Used
-         -        -                  -         -                   -         -         -

Extra port:

Instance  Hide IP  Dst IP         Dport     Proto          Port Usage  Capacity      Used
-         -        -                  -         -                   -         -         -
```

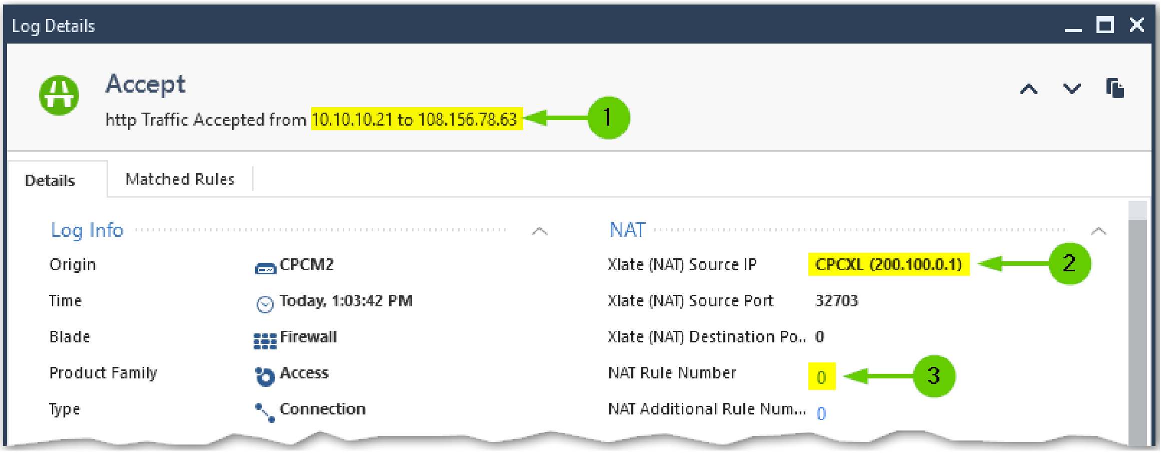


```
CPVIEW.Advanced.NAT.Pool-IPv4                                                         04Jun2022 18:44:10
Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced
CPU-Profiler Memory Network SecureXL ClusterXL CoreXL PrioQ Streaming NAT MUX Routed RAD Conn-Tracker UP     >>
Pool-IPv4 Pool-IPv6
General Statistics:

Concurrent connections                82
Connections session rate               1

High port:

Instance  Hide IP             Dst IP                  Dport     Proto          Port Usage  Capacity      Used
All       200.100.0.1         9.9.9.9                    53        17                  51    49,601        0%
All       200.100.0.20        75.2.29.249               443         6                   2    49,601        0%

Low port:

Instance  Hide IP   Dst IP        Dport     Proto          Port Usage  Capacity      Used
-         -         -                 -         -                   -         -         -

Extra port:

Instance  Hide IP   Dst IP        Dport     Proto          Port Usage  Capacity      Used
-         -         -                 -         -                   -         -         -
```



Gateway Cluster Properties - CPCXL

☑ Hide internal networks behind the Gateway's external IP



Log Details

Accept

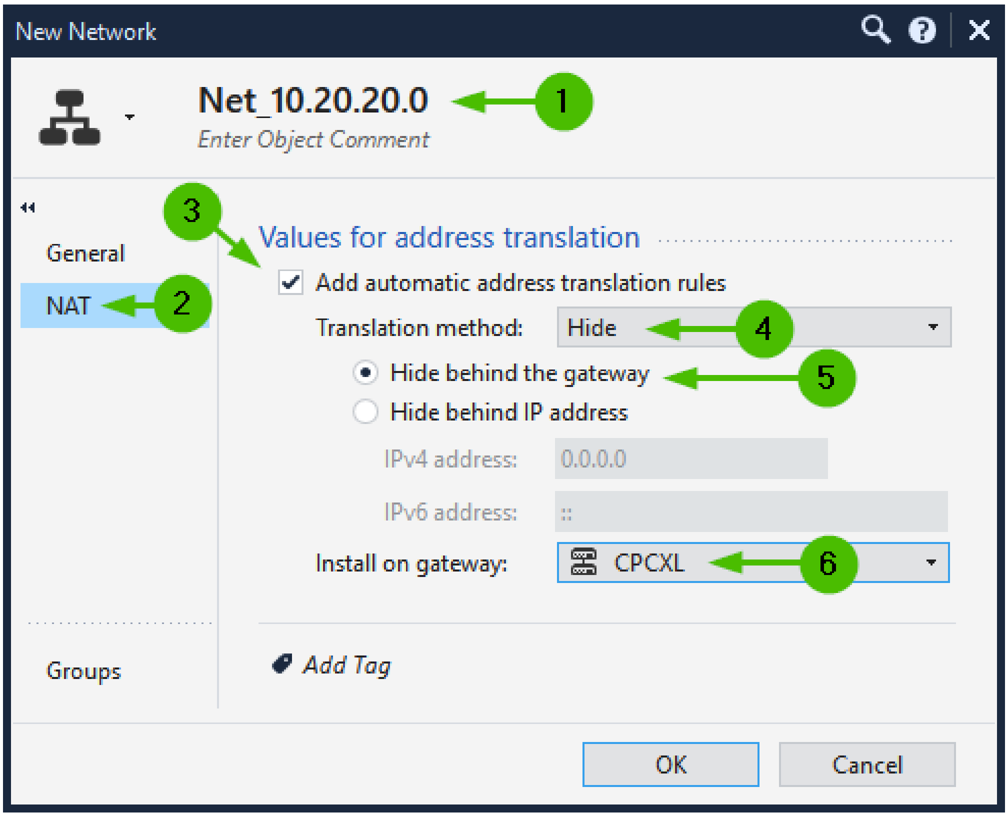
http Traffic Accepted from 10.10.10.21 to 108.156.78.63

Log Info

Origin	CPCM2
Time	Today, 1:03:42 PM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Source IP	CPCXL (200.100.0.1)
Xlate (NAT) Source Port	32703
Xlate (NAT) Destination Po...	0
NAT Rule Number	0
NAT Additional Rule Num...	0



New Network

Net_10.20.20.0

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Hide

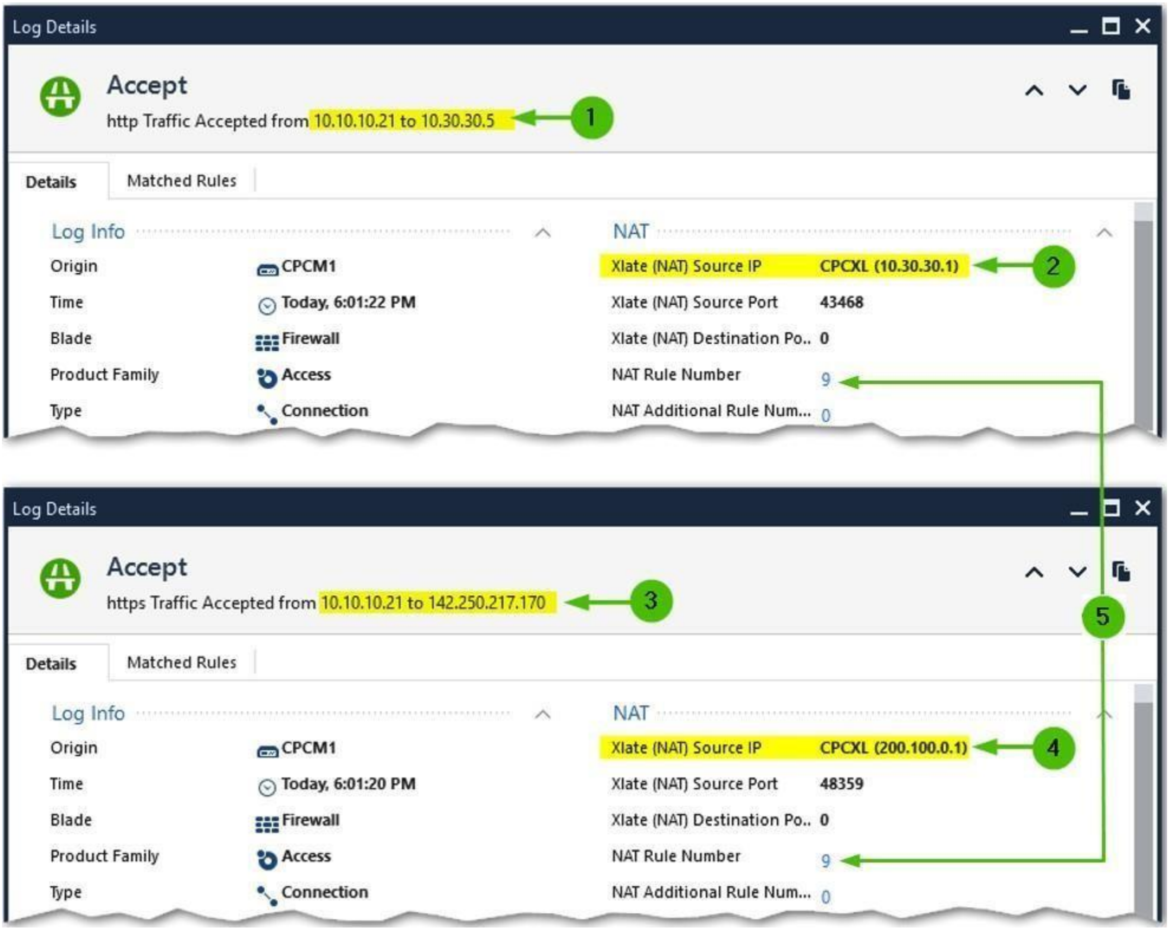
● Hide behind the gateway

○ Hide behind IP address

IPv4 address: 0.0.0.0

IPv6 address: ::

Install on gateway: CPCXL


Log Details

Accept

http Traffic Accepted from 10.10.10.21 to 10.30.30.5

Details | Matched Rules

Log Info

Origin	CPCM1
Time	Today, 6:01:22 PM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Source IP	CPCXL (10.30.30.1)
Xlate (NAT) Source Port	43468
Xlate (NAT) Destination Po..	0
NAT Rule Number	9
NAT Additional Rule Num...	0

Log Details

Accept

https Traffic Accepted from 10.10.10.21 to 142.250.217.170

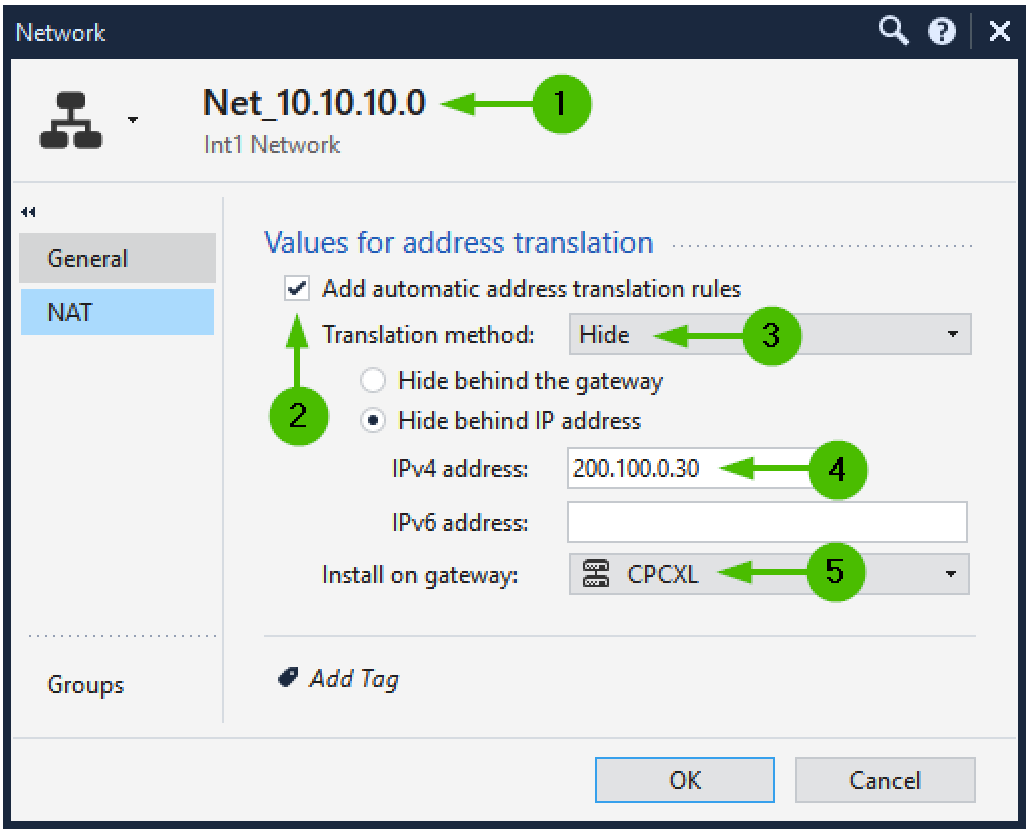
Details | Matched Rules

Log Info

Origin	CPCM1
Time	Today, 6:01:20 PM
Blade	Firewall
Product Family	Access
Type	Connection

NAT

Xlate (NAT) Source IP	CPCXL (200.100.0.1)
Xlate (NAT) Source Port	48359
Xlate (NAT) Destination Po..	0
NAT Rule Number	9
NAT Additional Rule Num...	0



Net_10.10.10.0

Int1 Network

Values for address translation

☑ Add automatic address translation rules

Translation method: Hide

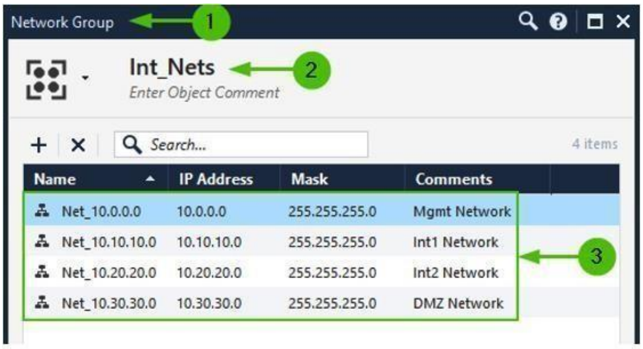
○ Hide behind the gateway

● Hide behind IP address

IPv4 address: 200.100.0.30

IPv6 address:

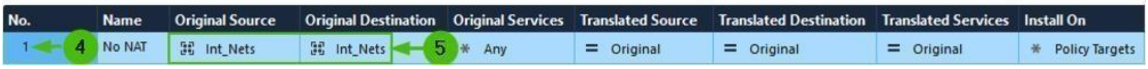
Install on gateway: CPCXL



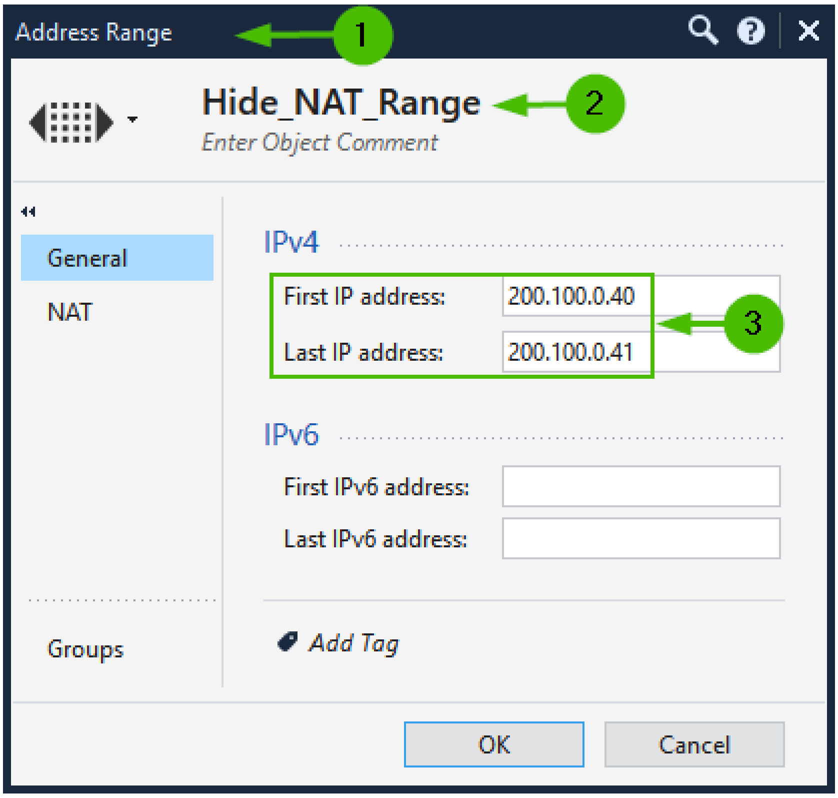
Int_Nets

Enter Object Comment

Name	IP Address	Mask	Comments
Net_10.0.0.0	10.0.0.0	255.255.255.0	Mgmt Network
Net_10.10.10.0	10.10.10.0	255.255.255.0	Int1 Network
Net_10.20.20.0	10.20.20.0	255.255.255.0	Int2 Network
Net_10.30.30.0	10.30.30.0	255.255.255.0	DMZ Network



No.	Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On
1	No NAT	Int_Nets	Int_Nets	Any	= Original	= Original	= Original	Policy Targets



Hide_NAT_Range

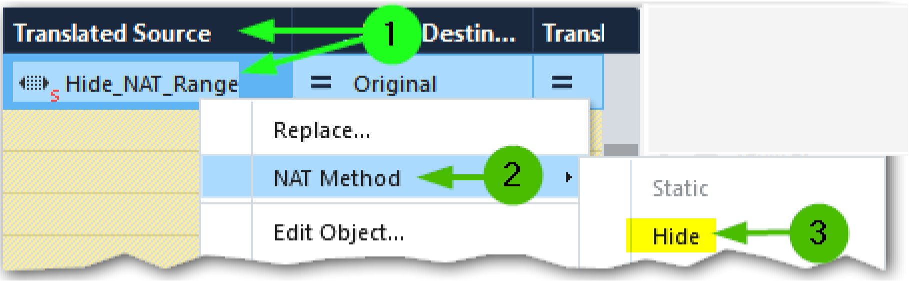
Enter Object Comment

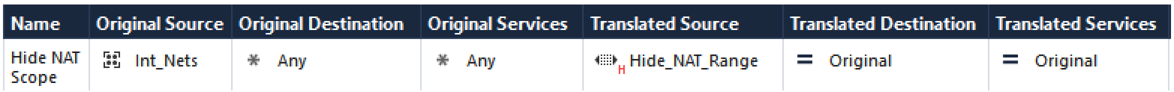
First IP address: 200.100.0.40

Last IP address: 200.100.0.41

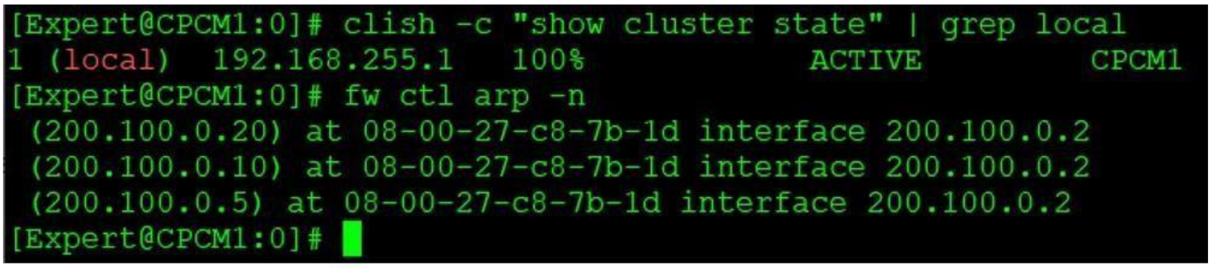
First IPv6 address:

Last IPv6 address:

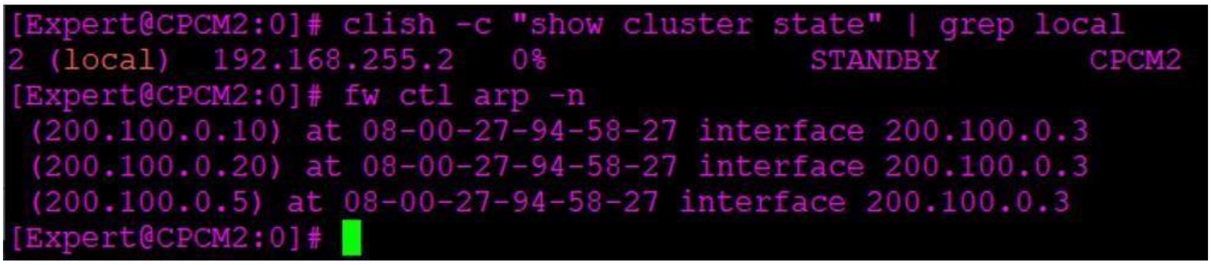




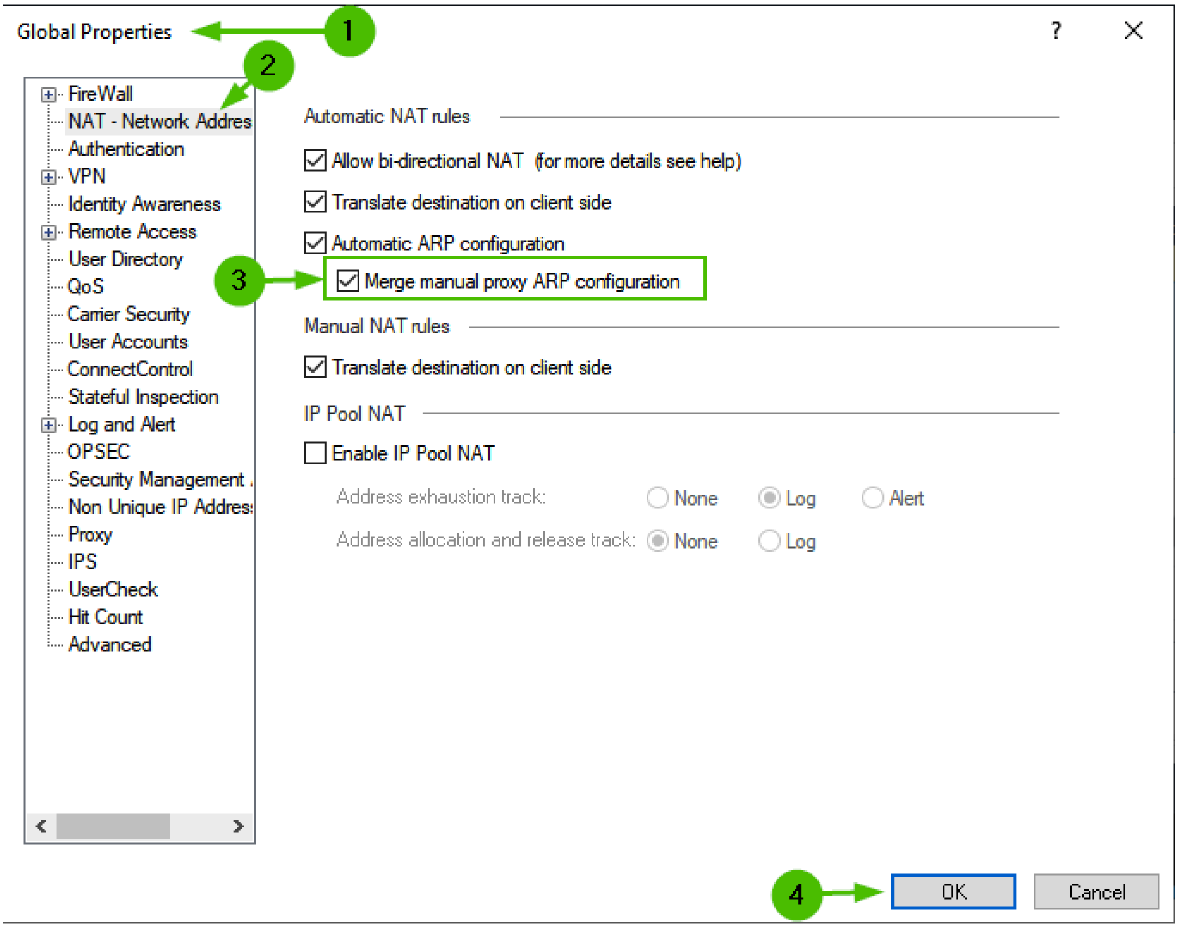
Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
Hide NAT Scope	Int_Nets	* Any	* Any	Hide_NAT_Range	= Original	= Original



```
[Expert@CPCM1:0]# clish -c "show cluster state" | grep local
1 (local)  192.168.255.1   100%              ACTIVE        CPCM1
[Expert@CPCM1:0]# fw ctl arp -n
 (200.100.0.20) at 08-00-27-c8-7b-1d interface 200.100.0.2
 (200.100.0.10) at 08-00-27-c8-7b-1d interface 200.100.0.2
 (200.100.0.5) at 08-00-27-c8-7b-1d interface 200.100.0.2
[Expert@CPCM1:0]#
```



```
[Expert@CPCM2:0]# clish -c "show cluster state" | grep local
2 (local)  192.168.255.2   0%                STANDBY       CPCM2
[Expert@CPCM2:0]# fw ctl arp -n
 (200.100.0.10) at 08-00-27-94-58-27 interface 200.100.0.3
 (200.100.0.20) at 08-00-27-94-58-27 interface 200.100.0.3
 (200.100.0.5) at 08-00-27-94-58-27 interface 200.100.0.3
[Expert@CPCM2:0]#
```



Global Properties

Automatic NAT rules

☑ Allow bi-directional NAT (for more details see help)

☑ Translate destination on client side

☑ Automatic ARP configuration

☑ Merge manual proxy ARP configuration

Manual NAT rules

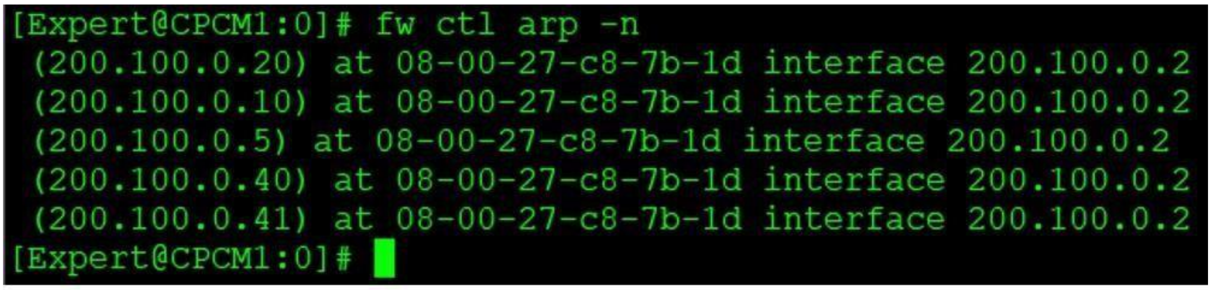
☑ Translate destination on client side

IP Pool NAT

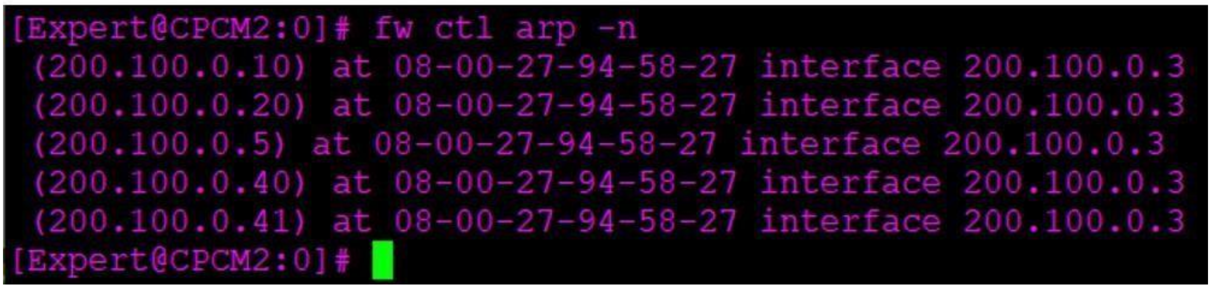
□ Enable IP Pool NAT

Address exhaustion track: ○ None ● Log ○ Alert

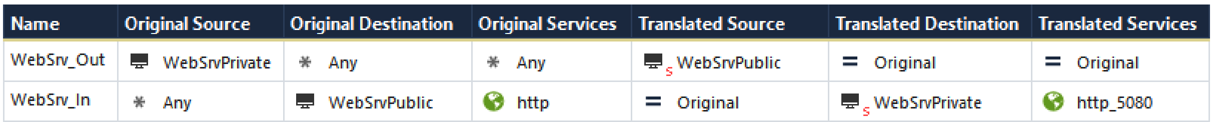
Address allocation and release track: ● None ○ Log



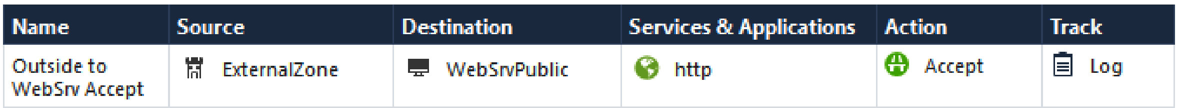
```
[Expert@CPCM1:0]# fw ctl arp -n
 (200.100.0.20) at 08-00-27-c8-7b-1d interface 200.100.0.2
 (200.100.0.10) at 08-00-27-c8-7b-1d interface 200.100.0.2
 (200.100.0.5) at 08-00-27-c8-7b-1d interface 200.100.0.2
 (200.100.0.40) at 08-00-27-c8-7b-1d interface 200.100.0.2
 (200.100.0.41) at 08-00-27-c8-7b-1d interface 200.100.0.2
[Expert@CPCM1:0]#
```



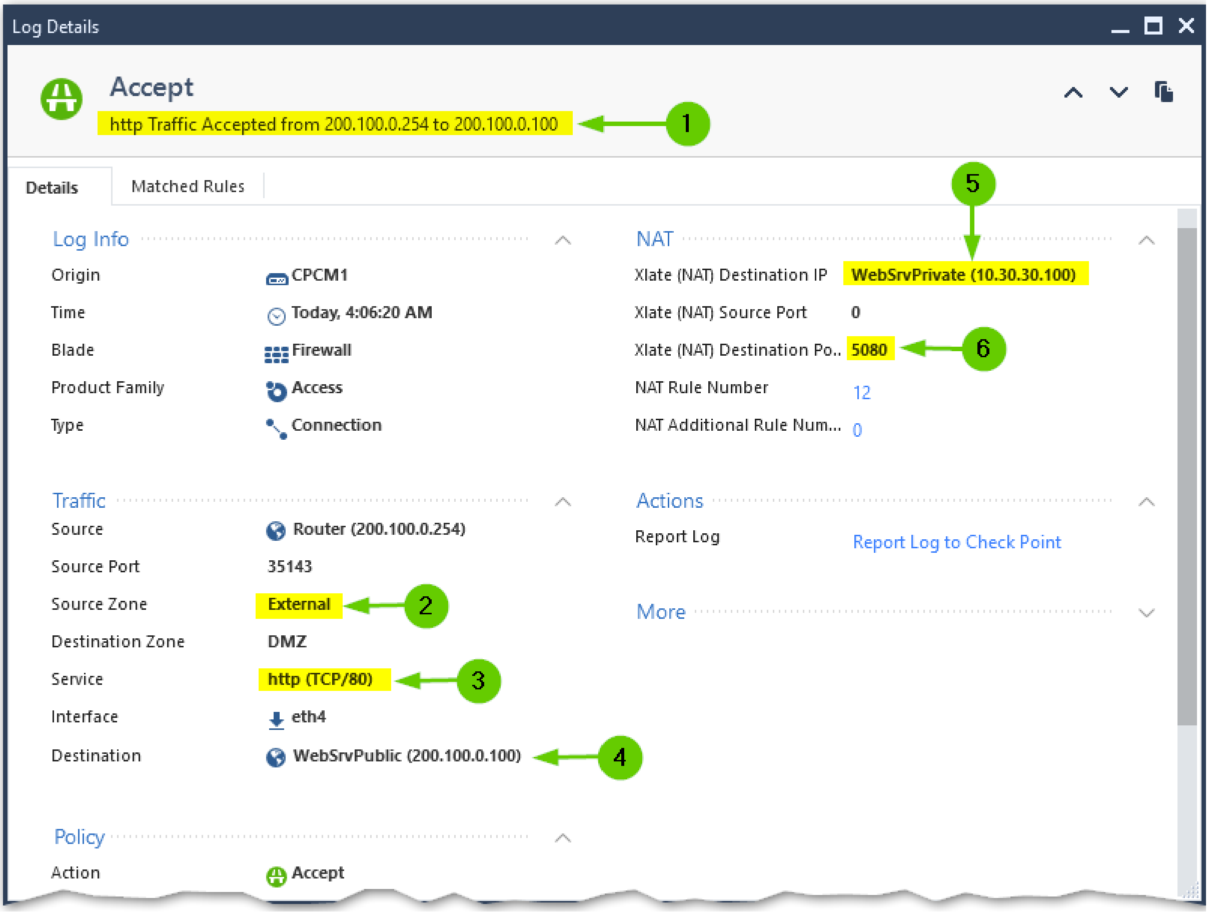
```
[Expert@CPCM2:0]# fw ctl arp -n
 (200.100.0.10) at 08-00-27-94-58-27 interface 200.100.0.3
 (200.100.0.20) at 08-00-27-94-58-27 interface 200.100.0.3
 (200.100.0.5) at 08-00-27-94-58-27 interface 200.100.0.3
 (200.100.0.40) at 08-00-27-94-58-27 interface 200.100.0.3
 (200.100.0.41) at 08-00-27-94-58-27 interface 200.100.0.3
[Expert@CPCM2:0]#
```



Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
WebSrv_Out	WebSrvPrivate	Any	Any	WebSrvPublic	Original	Original
WebSrv_In	Any	WebSrvPublic	http	Original	WebSrvPrivate	http_5080



Name	Source	Destination	Services & Applications	Action	Track
Outside to WebSrv Accept	ExternalZone	WebSrvPublic	http	Accept	Log



Log Details

Accept

http Traffic Accepted from 200.100.0.254 to 200.100.0.100

Details | Matched Rules

Log Info

Origin CPCM1

Time Today, 4:06:20 AM

Blade Firewall

Product Family Access

Type Connection

NAT

Xlate (NAT) Destination IP WebSrvPrivate (10.30.30.100)

Xlate (NAT) Source Port 0

Xlate (NAT) Destination Po.. 5080

NAT Rule Number 12

NAT Additional Rule Num... 0

Traffic

Source Router (200.100.0.254)

Source Port 35143

Source Zone External

Destination Zone DMZ

Service http (TCP/80)

Interface eth4

Destination WebSrvPublic (200.100.0.100)

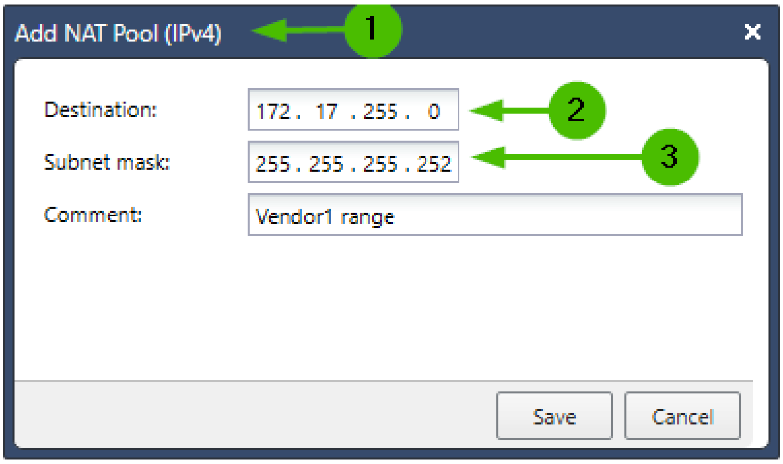
Actions

Report Log Report Log to Check Point

More

Policy

Action Accept

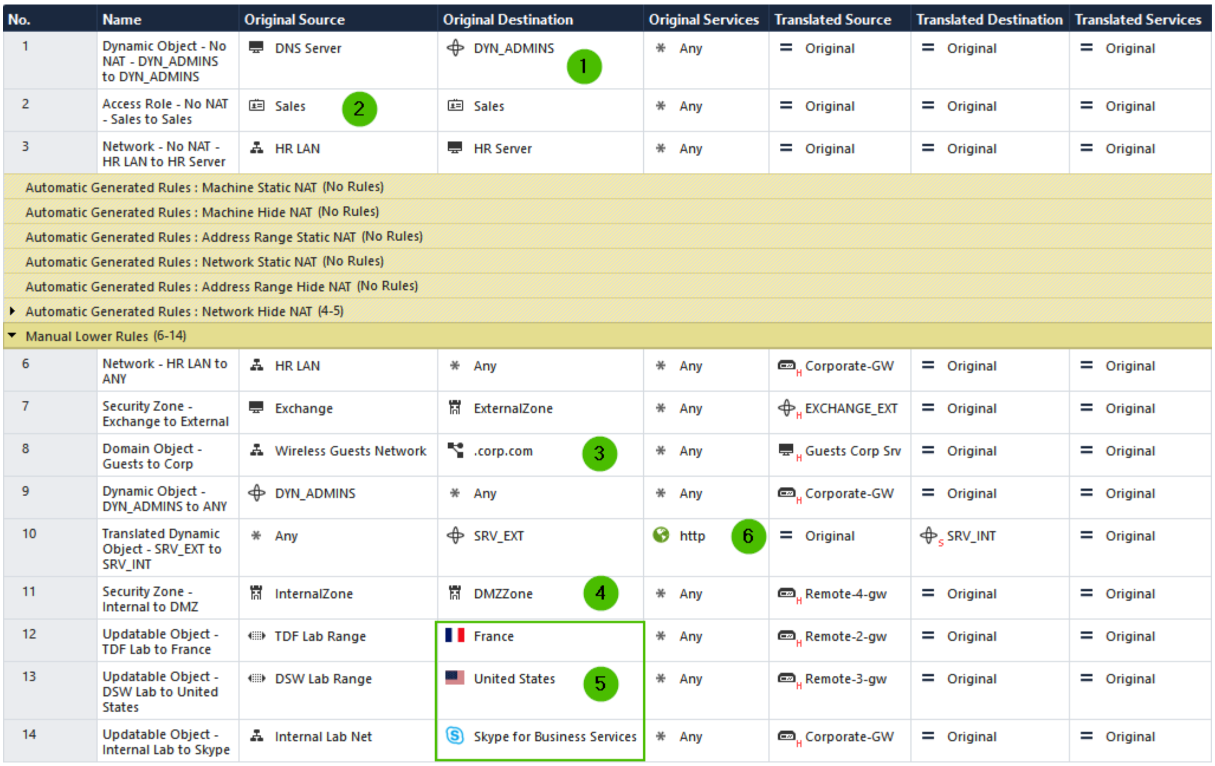


Add NAT Pool (IPv4)

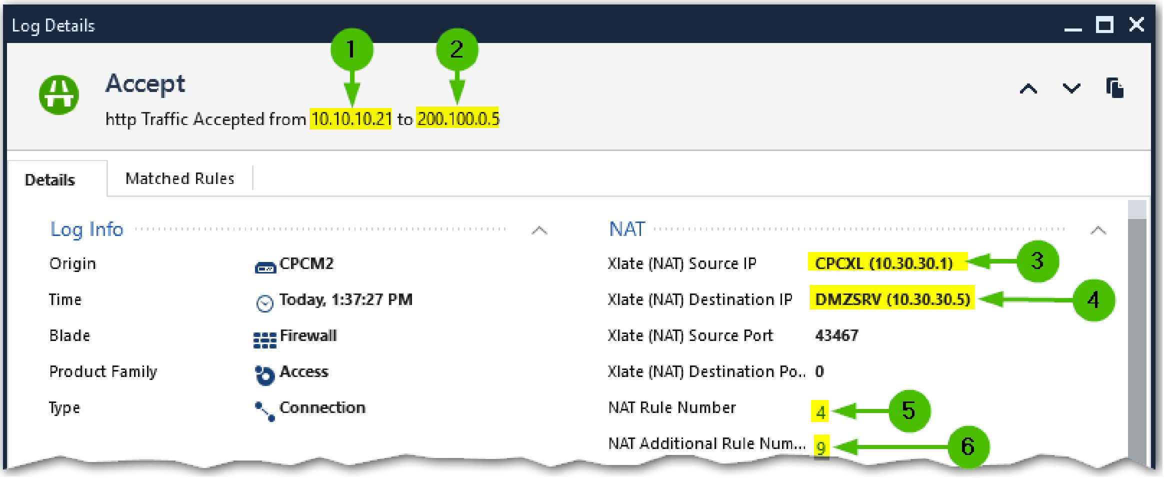
Destination: 172 . 17 . 255 . 0

Subnet mask: 255 . 255 . 255 . 252

Comment: Vendor1 range



No.	Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
1	Dynamic Object - No NAT - DYN_ADMINS to DYN_ADMINS	DNS Server	DYN_ADMINS	Any	= Original	= Original	= Original
2	Access Role - No NAT - Sales to Sales	Sales	Sales	Any	= Original	= Original	= Original
3	Network - No NAT - HR LAN to HR Server	HR LAN	HR Server	Any	= Original	= Original	= Original
Automatic Generated Rules : Machine Static NAT (No Rules)							
Automatic Generated Rules : Machine Hide NAT (No Rules)							
Automatic Generated Rules : Address Range Static NAT (No Rules)							
Automatic Generated Rules : Network Static NAT (No Rules)							
Automatic Generated Rules : Address Range Hide NAT (No Rules)							
Automatic Generated Rules : Network Hide NAT (4-5)							
Manual Lower Rules (6-14)							
6	Network - HR LAN to ANY	HR LAN	Any	Any	Corporate-GW	= Original	= Original
7	Security Zone - Exchange to External	Exchange	ExternalZone	Any	EXCHANGE_EXT	= Original	= Original
8	Domain Object - Guests to Corp	Wireless Guests Network	.corp.com	Any	Guests Corp Srv	= Original	= Original
9	Dynamic Object - DYN_ADMINS to ANY	DYN_ADMINS	Any	Any	Corporate-GW	= Original	= Original
10	Translated Dynamic Object - SRV_EXT to SRV_INT	Any	SRV_EXT	http	= Original	SRV_INT	= Original
11	Security Zone - Internal to DMZ	InternalZone	DMZZone	Any	Remote-4-gw	= Original	= Original
12	Updatable Object - TDF Lab to France	TDF Lab Range	France	Any	Remote-2-gw	= Original	= Original
13	Updatable Object - DSW Lab to United States	DSW Lab Range	United States	Any	Remote-3-gw	= Original	= Original
14	Updatable Object - Internal Lab to Skype	Internal Lab Net	Skype for Business Services	Any	Corporate-GW	= Original	= Original



Log Details

Accept

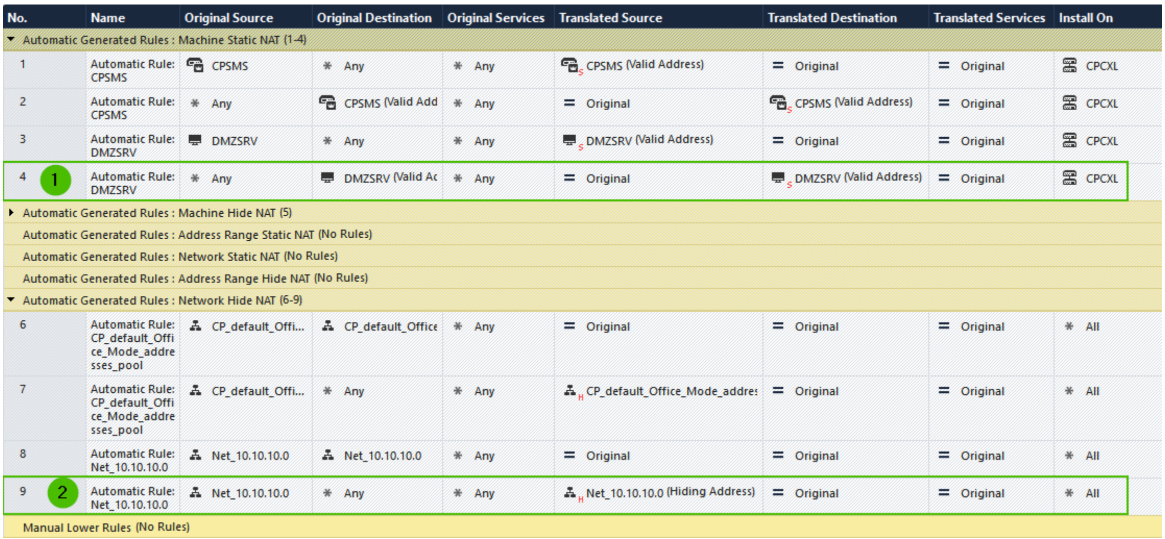
http Traffic Accepted from 10.10.10.21 to 200.100.0.5

Log Info

Origin	CPCM2
Time	Today, 1:37:27 PM
Blade	Firewall
Product Family	Access
Type	Connection

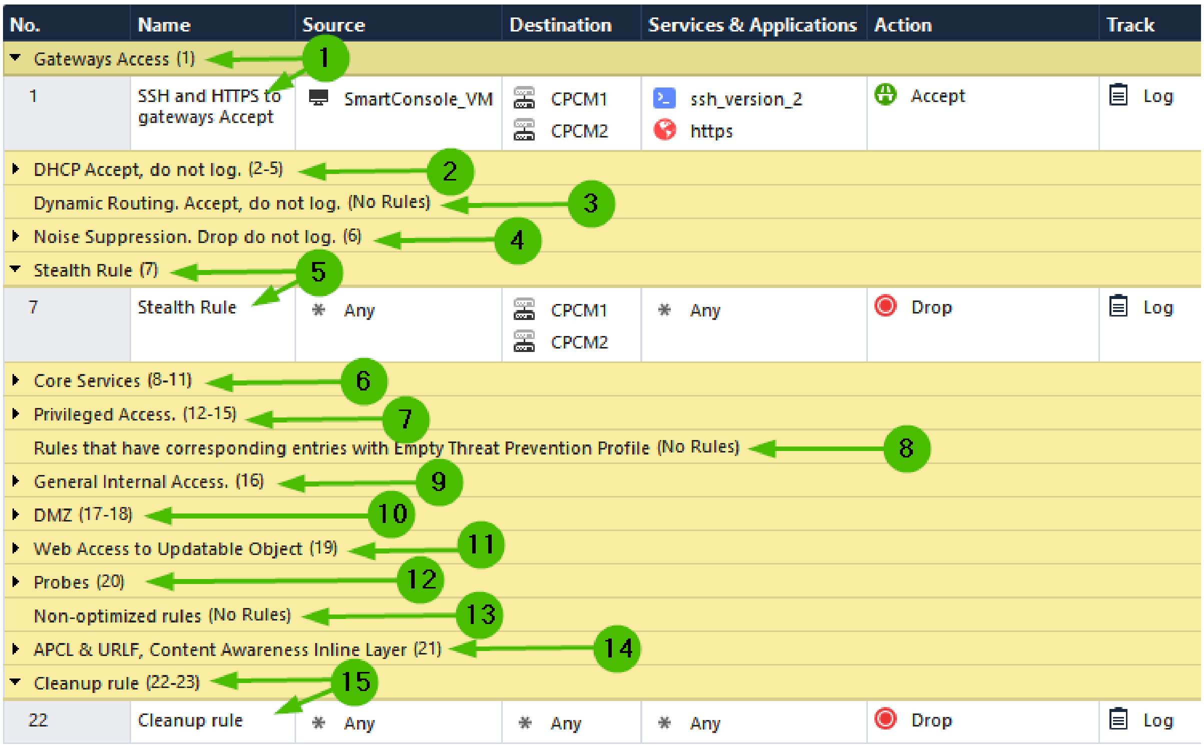
NAT

Xlate (NAT) Source IP	CPCXL (10.30.30.1)
Xlate (NAT) Destination IP	DMZSRV (10.30.30.5)
Xlate (NAT) Source Port	43467
Xlate (NAT) Destination Po..	0
NAT Rule Number	4
NAT Additional Rule Num...	9

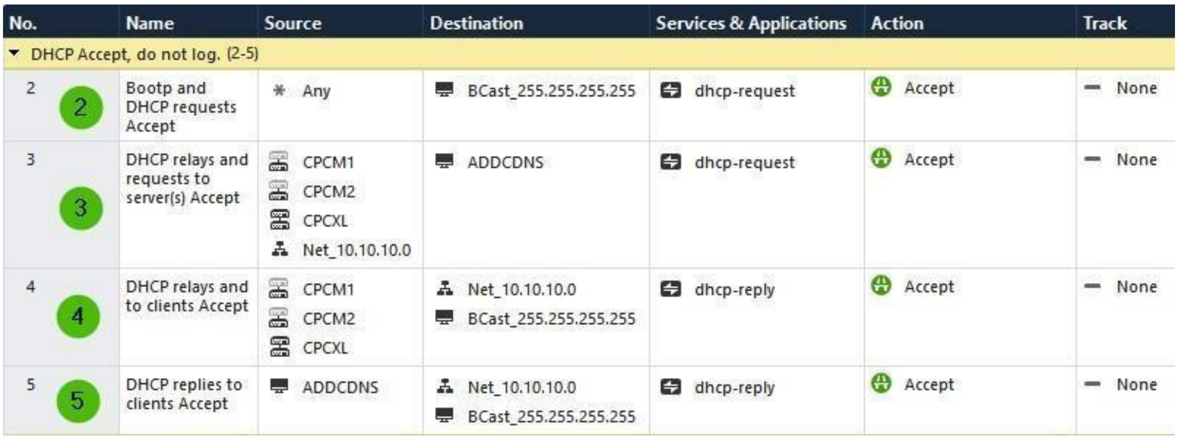


No.	Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On
Automatic Generated Rules : Machine Static NAT (1-4)								
1	Automatic Rule: CPSMS	CPSMS	Any	Any	CPSMS (Valid Address)	= Original	= Original	CPCXL
2	Automatic Rule: CPSMS	Any	CPSMS (Valid Add	Any	= Original	CPSMS (Valid Address)	= Original	CPCXL
3	Automatic Rule: DMZSRV	DMZSRV	Any	Any	DMZSRV (Valid Address)	= Original	= Original	CPCXL
4	Automatic Rule: DMZSRV	Any	DMZSRV (Valid Ac	Any	= Original	DMZSRV (Valid Address)	= Original	CPCXL
Automatic Generated Rules : Machine Hide NAT (5)								
Automatic Generated Rules : Address Range Static NAT (No Rules)								
Automatic Generated Rules : Network Static NAT (No Rules)								
Automatic Generated Rules : Address Range Hide NAT (No Rules)								
Automatic Generated Rules : Network Hide NAT (6-9)								
6	Automatic Rule: CP_default_Office_Mode_addresses_pool	CP_default_Offi...	CP_default_Office	Any	= Original	= Original	= Original	All
7	Automatic Rule: CP_default_Office_Mode_addresses_pool	CP_default_Offi...	Any	Any	CP_default_Office_Mode_addres	= Original	= Original	All
8	Automatic Rule: Net_10.10.10.0	Net_10.10.10.0	Net_10.10.10.0	Any	= Original	= Original	= Original	All
9	Automatic Rule: Net_10.10.10.0	Net_10.10.10.0	Any	Any	Net_10.10.10.0 (Hiding Address)	= Original	= Original	All
Manual Lower Rules (No Rules)								

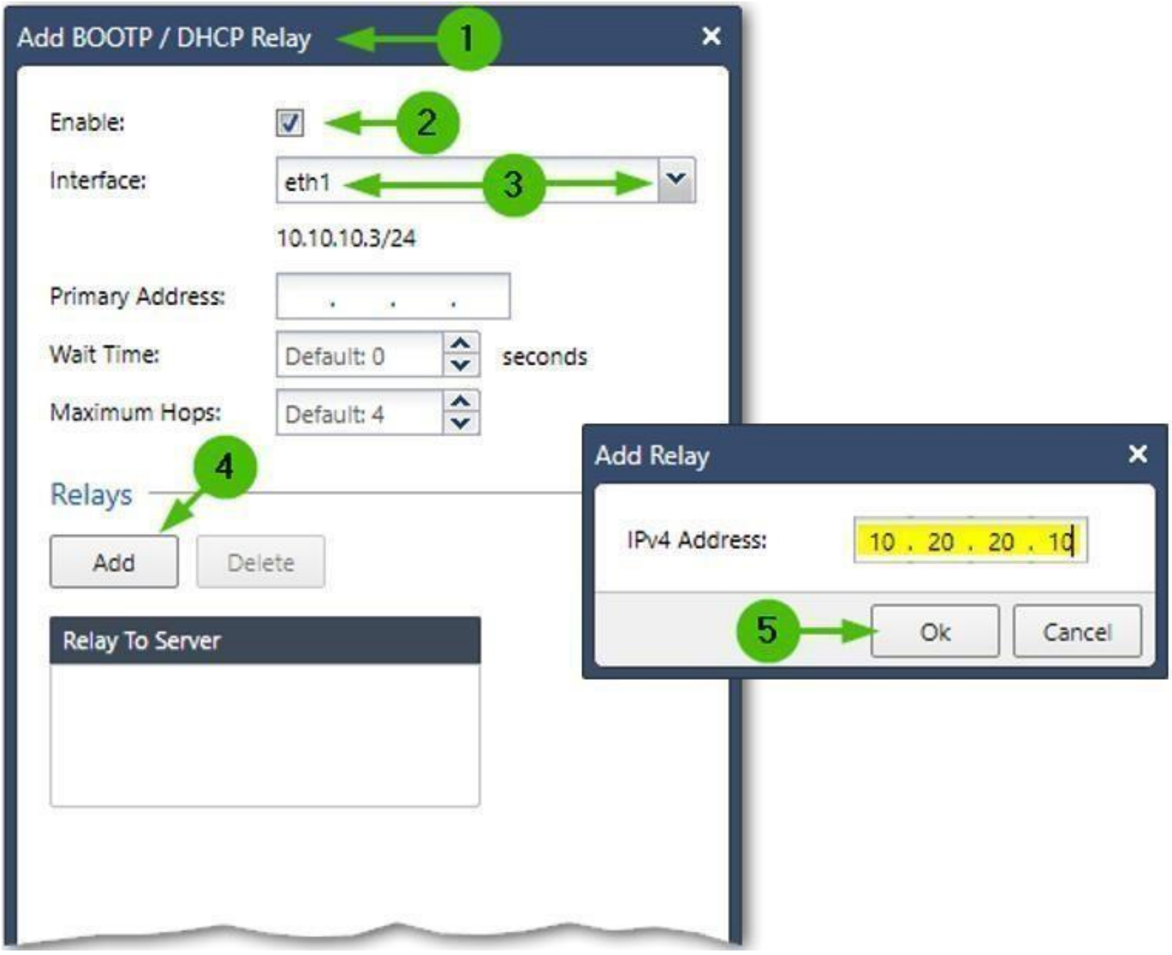
Chapter 11: Building Your First Policy



No.	Name	Source	Destination	Services & Applications	Action	Track
Gateways Access (1)						
1	SSH and HTTPS to gateways Accept	SmartConsole_VM	CPCM1 CPCM2	ssh_version_2 https	Accept	Log
DHCP Accept, do not log. (2-5)						
Dynamic Routing. Accept, do not log. (No Rules)						
Noise Suppression. Drop do not log. (6)						
Stealth Rule (7)						
7	Stealth Rule	Any	CPCM1 CPCM2	Any	Drop	Log
Core Services (8-11)						
Privileged Access. (12-15)						
Rules that have corresponding entries with Empty Threat Prevention Profile (No Rules)						
General Internal Access. (16)						
DMZ (17-18)						
Web Access to Updatable Object (19)						
Probes (20)						
Non-optimized rules (No Rules)						
APCL & URLF, Content Awareness Inline Layer (21)						
Cleanup rule (22-23)						
22	Cleanup rule	Any	Any	Any	Drop	Log



No.	Name	Source	Destination	Services & Applications	Action	Track
DHCP Accept, do not log. (2-5)						
2	Bootp and DHCP requests Accept	Any	BCast_255.255.255.255	dhcp-request	Accept	None
3	DHCP relays and requests to server(s) Accept	CPCM1 CPCM2 CPCXL Net_10.10.10.0	ADDCDNS	dhcp-request	Accept	None
4	DHCP relays and to clients Accept	CPCM1 CPCM2 CPCXL	Net_10.10.10.0 BCast_255.255.255.255	dhcp-reply	Accept	None
5	DHCP replies to clients Accept	ADDCDNS	Net_10.10.10.0 BCast_255.255.255.255	dhcp-reply	Accept	None



Add BOOTP / DHCP Relay

Enable: ☑

Interface: eth1

10.10.10.3/24

Primary Address: . . .

Wait Time: Default: 0 seconds

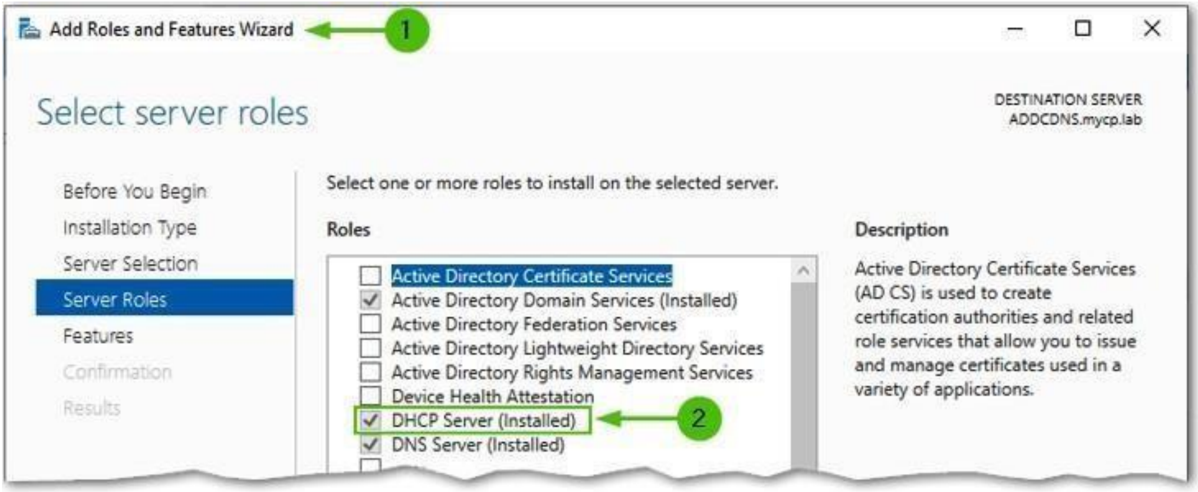
Maximum Hops: Default: 4

Relays

Relay To Server

Add Relay

IPv4 Address: 10 . 20 . 20 . 10



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
ADDCDNS.mycp.lab

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

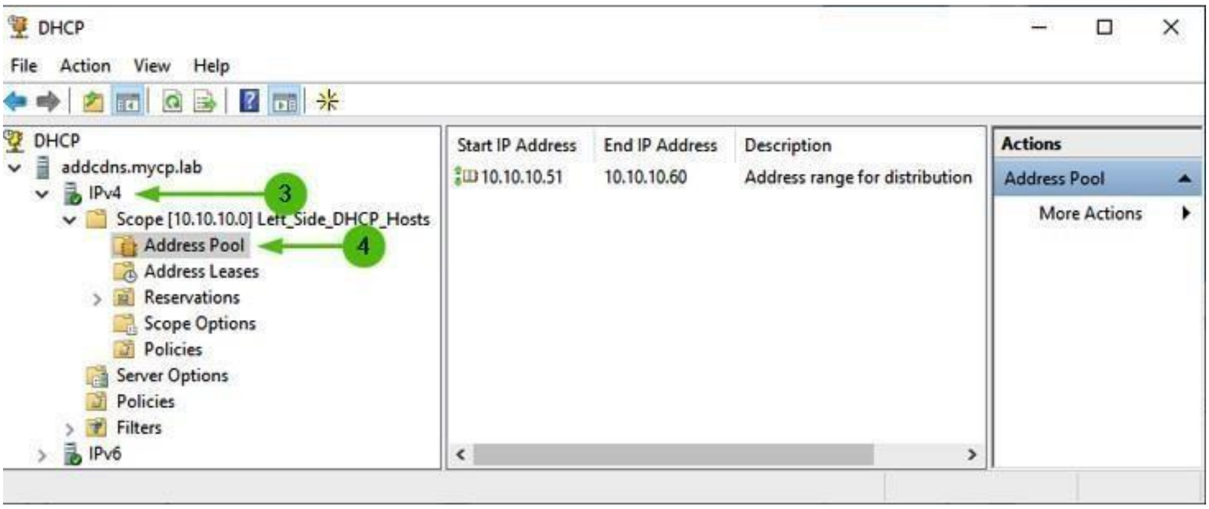
Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.



DHCP

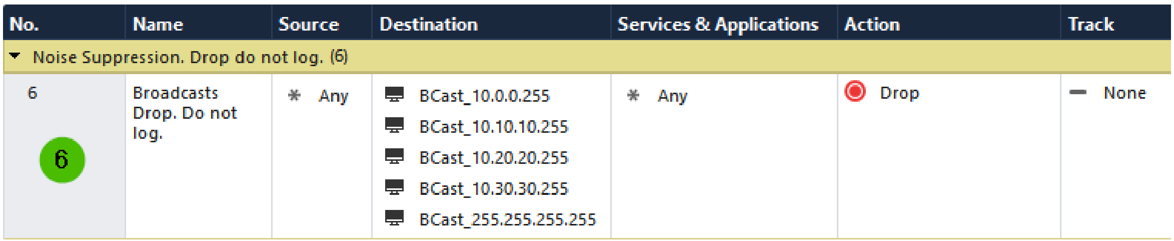
- DHCP
  - addcdns.mycp.lab
    - IPv4
      - Scope [10.10.10.0] Left_Side_DHCP_Hosts
        - Address Pool
        - Address Leases
        - Reservations
        - Scope Options
        - Policies
      - Server Options
      - Policies
      - Filters
    - IPv6

Start IP Address	End IP Address	Description
10.10.10.51	10.10.10.60	Address range for distribution

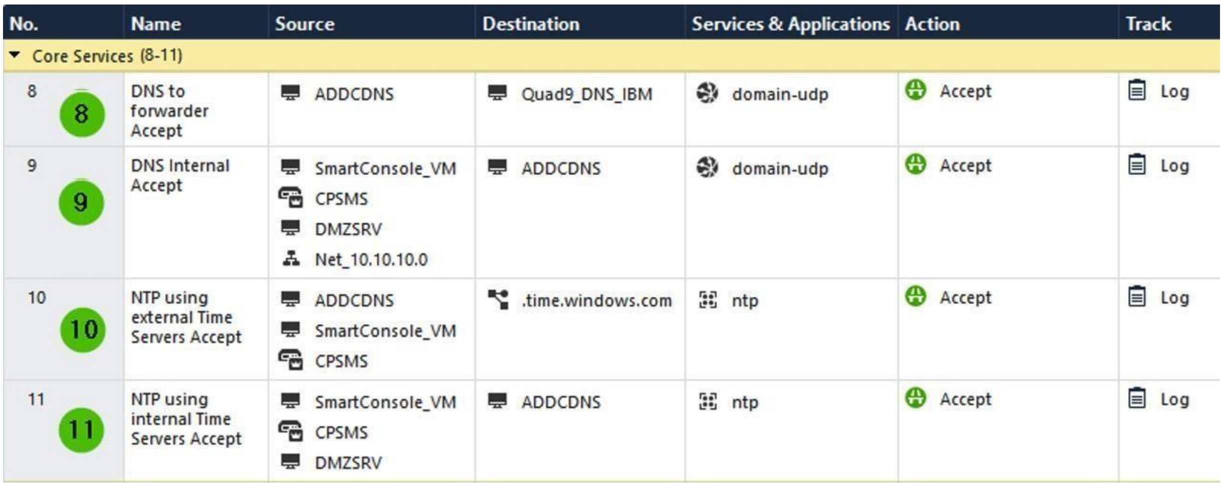
Actions

Address Pool

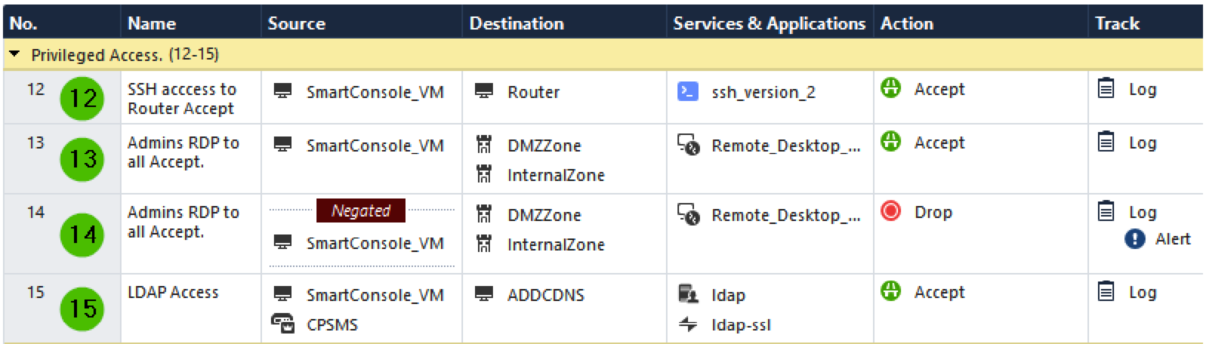
More Actions



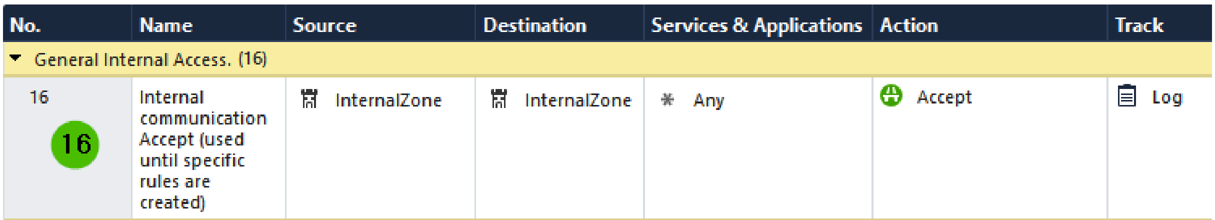
No.	Name	Source	Destination	Services & Applications	Action	Track
Noise Suppression. Drop do not log. (6)						
6	Broadcasts Drop. Do not log.	Any	BCast_10.0.0.255 BCast_10.10.10.255 BCast_10.20.20.255 BCast_10.30.30.255 BCast_255.255.255.255	Any	Drop	None



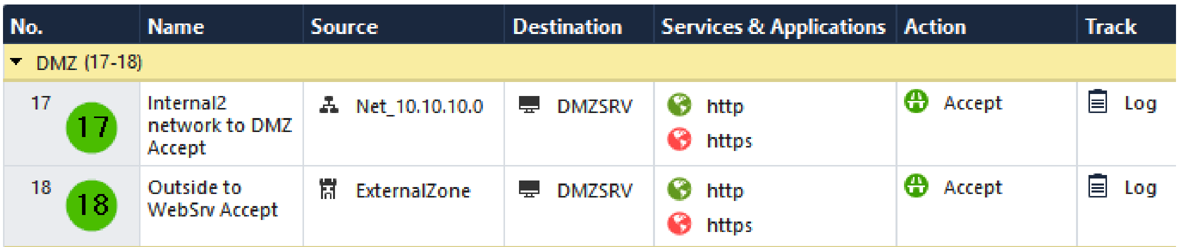
No.	Name	Source	Destination	Services & Applications	Action	Track
▾ Core Services (8-11)						
8 8	DNS to forwarder Accept	ADDCDNS	Quad9_DNS_IBM	domain-udp	Accept	Log
9 9	DNS Internal Accept	SmartConsole_VM CPSMS DMZSRV Net_10.10.10.0	ADDCDNS	domain-udp	Accept	Log
10 10	NTP using external Time Servers Accept	ADDCDNS SmartConsole_VM CPSMS	.time.windows.com	ntp	Accept	Log
11 11	NTP using internal Time Servers Accept	SmartConsole_VM CPSMS DMZSRV	ADDCDNS	ntp	Accept	Log



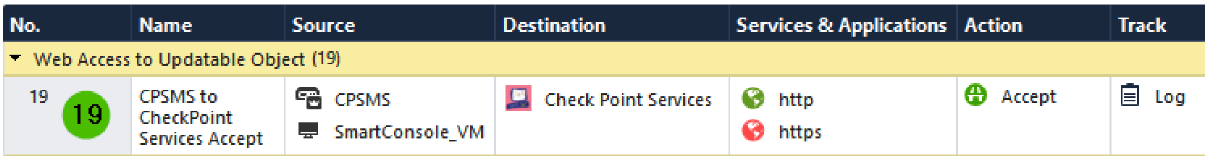
No.	Name	Source	Destination	Services & Applications	Action	Track
▾ Privileged Access. (12-15)						
12 12	SSH acccess to Router Accept	SmartConsole_VM	Router	ssh_version_2	Accept	Log
13 13	Admins RDP to all Accept.	SmartConsole_VM	DMZZone InternalZone	Remote_Desktop_...	Accept	Log
14 14	Admins RDP to all Accept.	*Negated* SmartConsole_VM	DMZZone InternalZone	Remote_Desktop_...	Drop	Log Alert
15 15	LDAP Access	SmartConsole_VM CPSMS	ADDCDNS	ldap ldap-ssl	Accept	Log



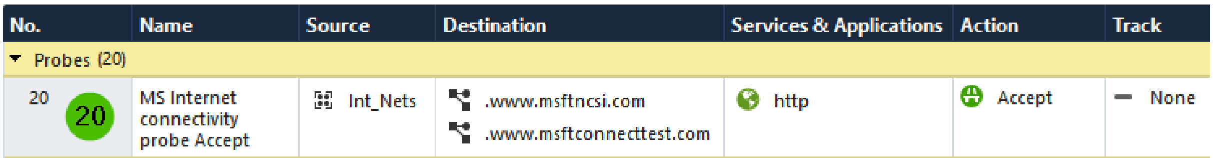
No.	Name	Source	Destination	Services & Applications	Action	Track
▾ General Internal Access. (16)						
16 16	Internal communication Accept (used until specific rules are created)	InternalZone	InternalZone	Any	Accept	Log



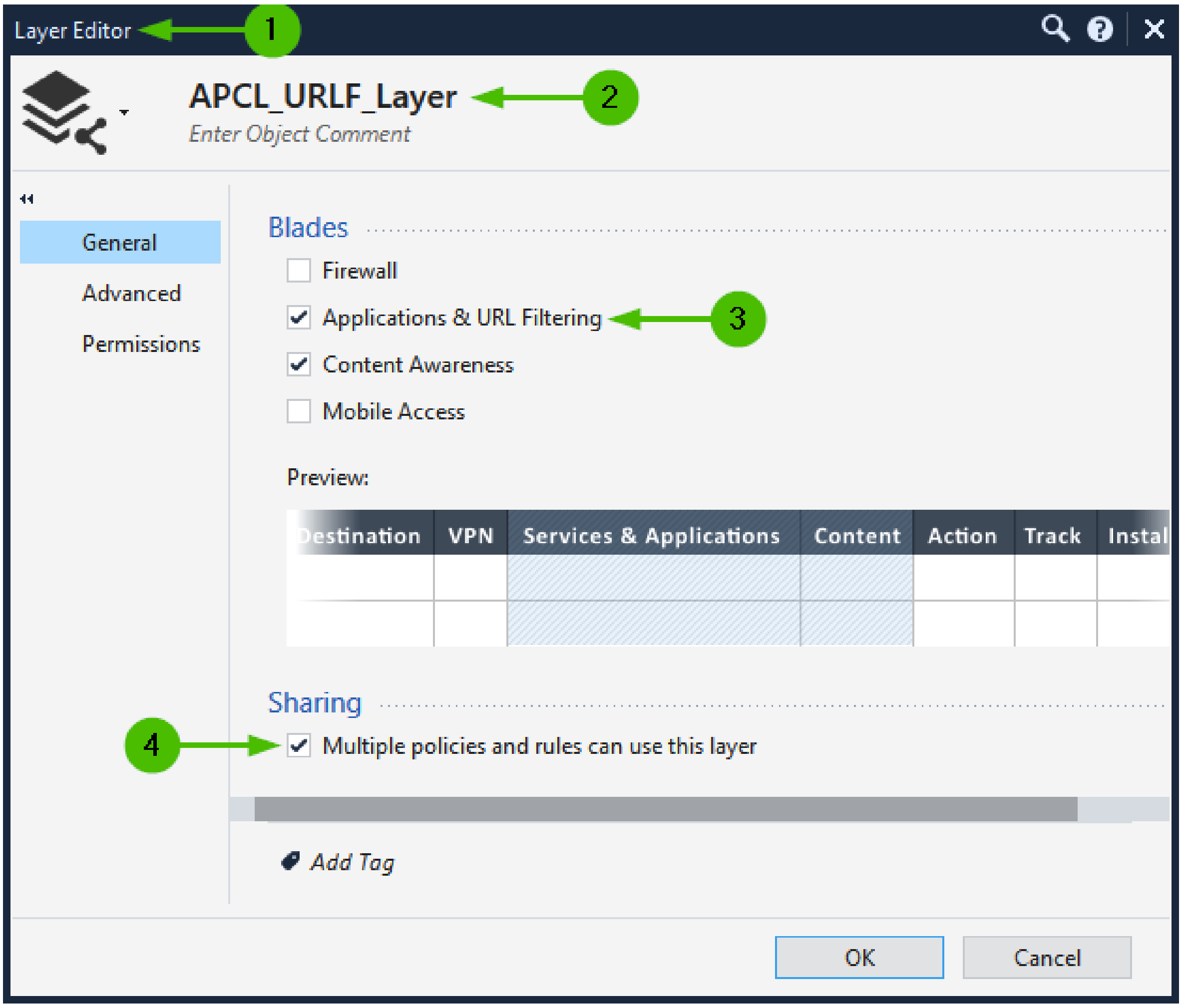
No.	Name	Source	Destination	Services & Applications	Action	Track
▾ DMZ (17-18)						
17 17	Internal2 network to DMZ Accept	Net_10.10.10.0	DMZSRV	http https	Accept	Log
18 18	Outside to WebSrv Accept	ExternalZone	DMZSRV	http https	Accept	Log



No.	Name	Source	Destination	Services & Applications	Action	Track
Web Access to Updatable Object (19)						
19	CPSMS to CheckPoint Services Accept	CPSMS SmartConsole_VM	Check Point Services	http https	Accept	Log



No.	Name	Source	Destination	Services & Applications	Action	Track
Probes (20)						
20	MS Internet connectivity probe Accept	Int_Nets	.www.msftncsi.com .www.msftconnecttest.com	http	Accept	None



Layer Editor

APCL_URLF_Layer

Enter Object Comment

Blades

□ Firewall

☑ Applications & URL Filtering

☑ Content Awareness

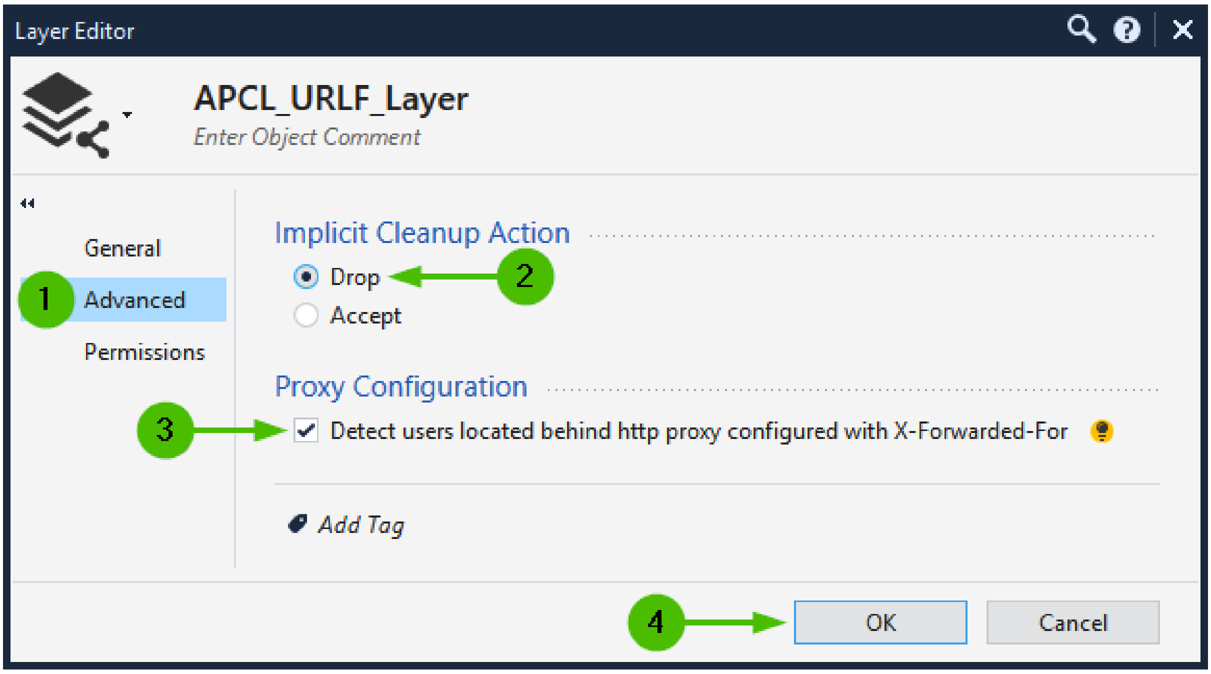
□ Mobile Access

Preview:

Destination	VPN	Services & Applications	Content	Action	Track	Instal

Sharing

☑ Multiple policies and rules can use this layer



APCL_URLF_Layer

Enter Object Comment

General

Advanced

Permissions

Implicit Cleanup Action

● Drop

○ Accept

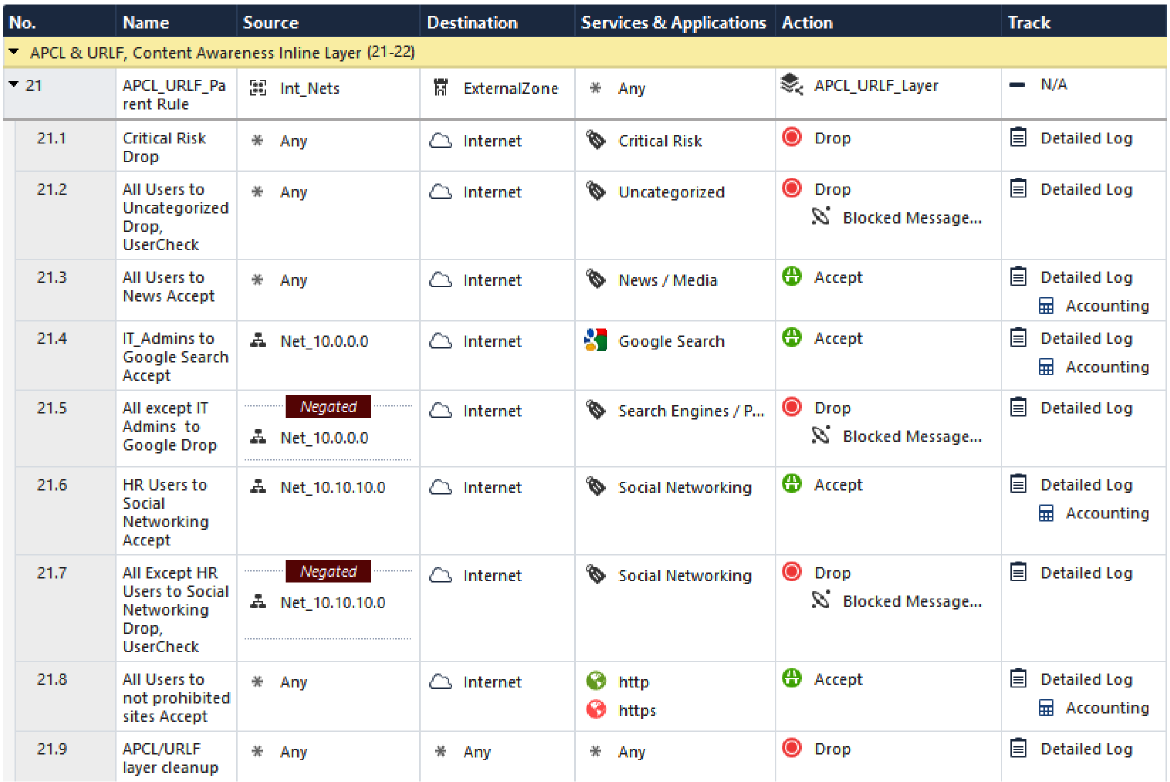
Proxy Configuration

☑ Detect users located behind http proxy configured with X-Forwarded-For

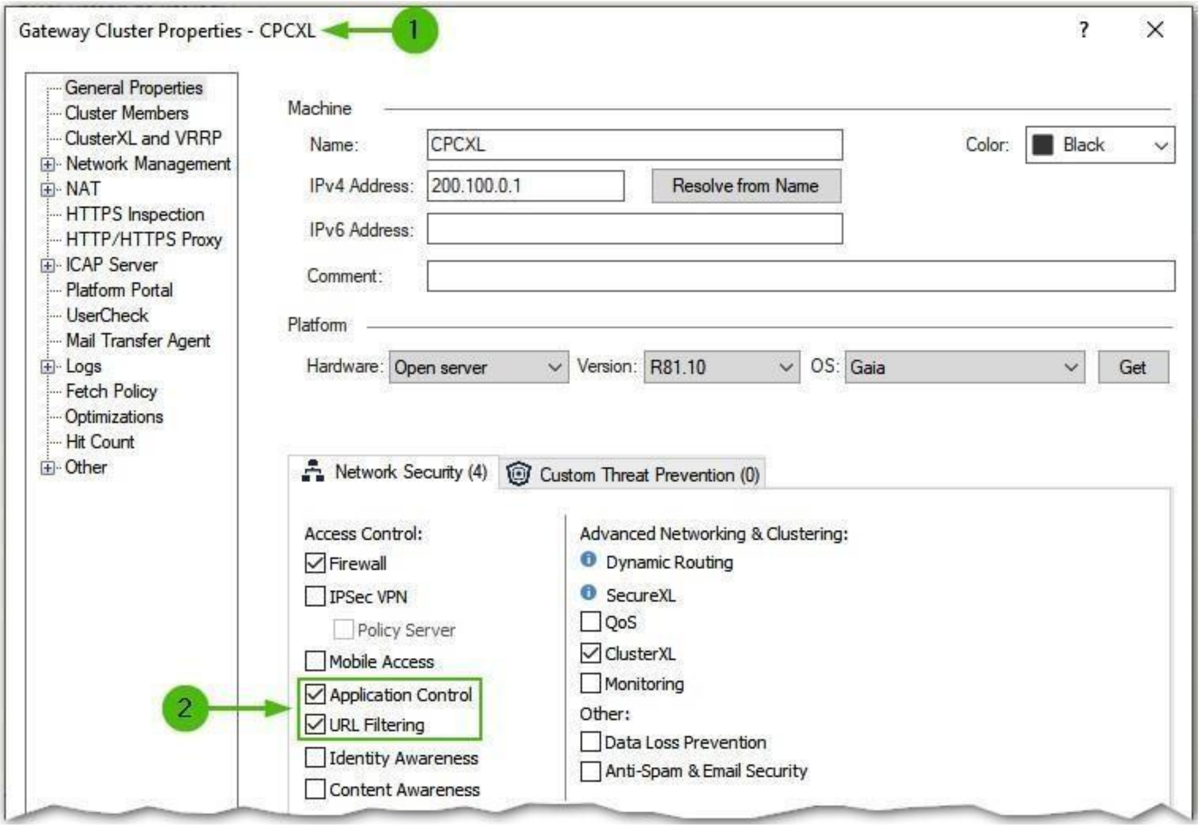
Add Tag

OK

Cancel



No.	Name	Source	Destination	Services & Applications	Action	Track
APCL & URLF, Content Awareness Inline Layer (21-22)						
21	APCL_URLF_Parent Rule	Int_Nets	ExternalZone	Any	APCL_URLF_Layer	N/A
21.1	Critical Risk Drop	Any	Internet	Critical Risk	Drop	Detailed Log
21.2	All Users to Uncategorized Drop, UserCheck	Any	Internet	Uncategorized	Drop Blocked Message...	Detailed Log
21.3	All Users to News Accept	Any	Internet	News / Media	Accept	Detailed Log Accounting
21.4	IT_Admins to Google Search Accept	Net_10.0.0.0	Internet	Google Search	Accept	Detailed Log Accounting
21.5	All except IT Admins to Google Drop	Negated Net_10.0.0.0	Internet	Search Engines / P...	Drop Blocked Message...	Detailed Log
21.6	HR Users to Social Networking Accept	Net_10.10.10.0	Internet	Social Networking	Accept	Detailed Log Accounting
21.7	All Except HR Users to Social Networking Drop, UserCheck	Negated Net_10.10.10.0	Internet	Social Networking	Drop Blocked Message...	Detailed Log
21.8	All Users to not prohibited sites Accept	Any	Internet	http https	Accept	Detailed Log Accounting
21.9	APCL/URLF layer cleanup	Any	Any	Any	Drop	Detailed Log



Gateway Cluster Properties - CPCXL

Machine

Name: CPCXL

Color: Black

IPv4 Address: 200.100.0.1

IPv6 Address:

Comment:

Platform

Hardware: Open server Version: R81.10 OS: Gaia

Access Control:

☑ Firewall

□ IPSec VPN

□ Policy Server

□ Mobile Access

☑ Application Control

☑ URL Filtering

□ Identity Awareness

□ Content Awareness

Advanced Networking & Clustering:

Dynamic Routing

SecureXL

□ QoS

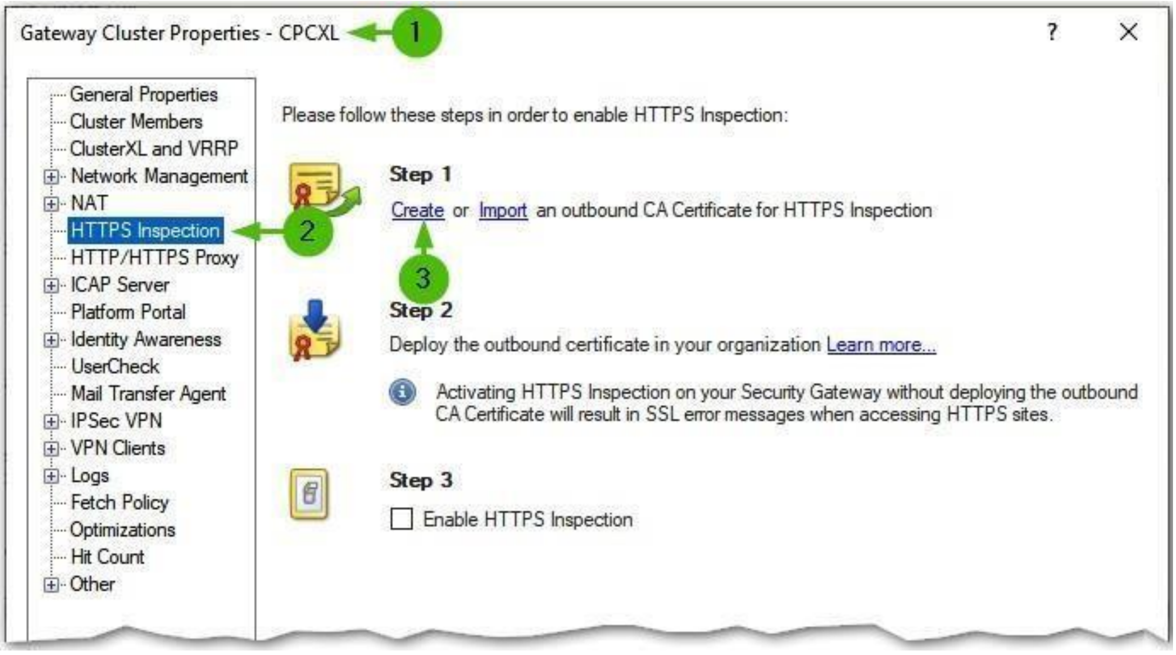
☑ ClusterXL

□ Monitoring

Other:

□ Data Loss Prevention

□ Anti-Spam & Email Security



Gateway Cluster Properties - CPCXL

Please follow these steps in order to enable HTTPS Inspection:

Step 1

Create or Import an outbound CA Certificate for HTTPS Inspection

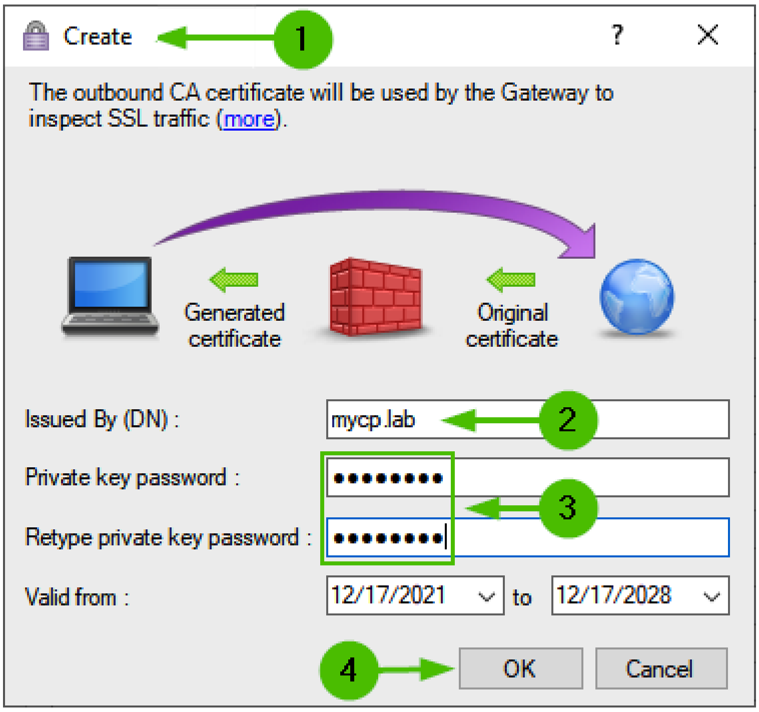
Step 2

Deploy the outbound certificate in your organization Learn more...

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3

□ Enable HTTPS Inspection



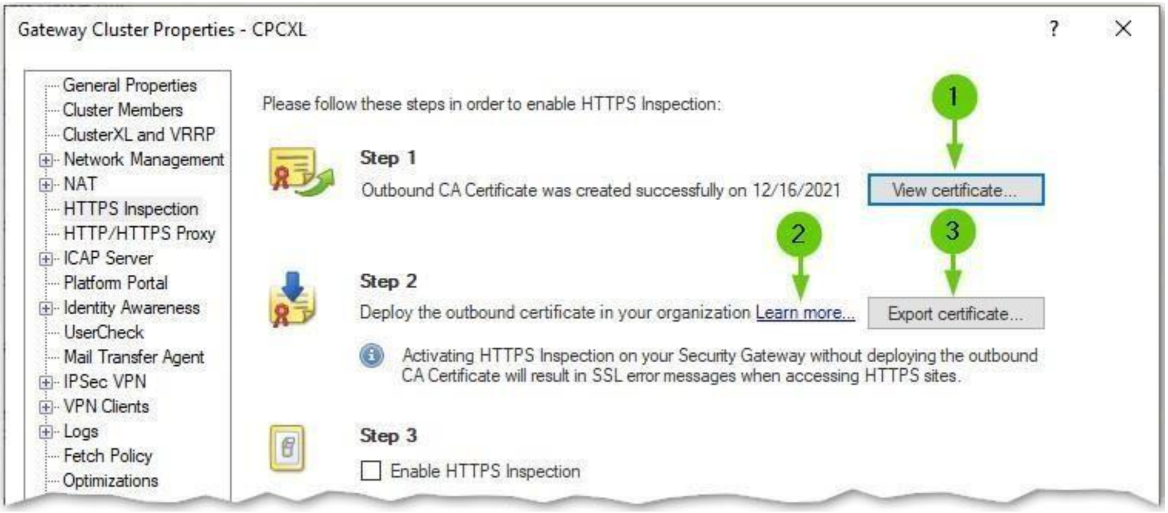
The outbound CA certificate will be used by the Gateway to inspect SSL traffic (more).

Issued By (DN) : mycp.lab

Private key password : ••••••••

Retype private key password : ••••••••

Valid from : 12/17/2021 to 12/17/2028



Please follow these steps in order to enable HTTPS Inspection:

Step 1

Outbound CA Certificate was created successfully on 12/16/2021

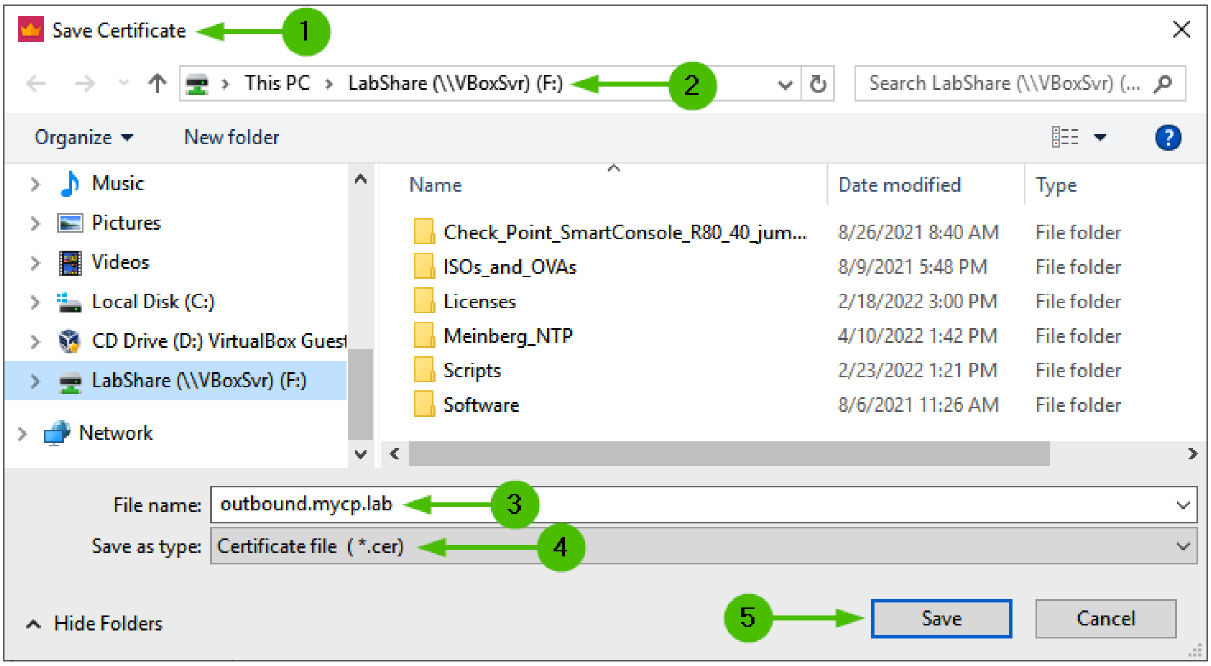
Step 2

Deploy the outbound certificate in your organization Learn more...

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3

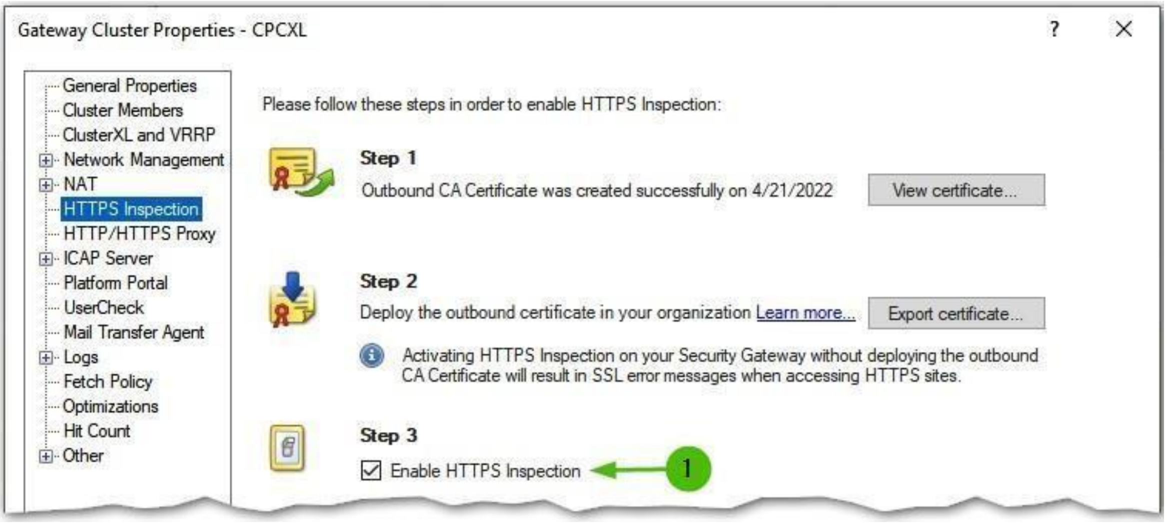
□ Enable HTTPS Inspection


Save Certificate
1
This PC › LabShare (\\VBoxSvr) (F:)
2
Search LabShare (\\VBoxSvr) (...
Organize
New folder
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) VirtualBox Guest
LabShare (\\VBoxSvr) (F:)
Network
3
4
5
Hide Folders
Save
Cancel

Name	Date modified	Type
Check_Point_SmartConsole_R80_40_jum...	8/26/2021 8:40 AM	File folder
ISOs_and_OVAs	8/9/2021 5:48 PM	File folder
Licenses	2/18/2022 3:00 PM	File folder
Meinberg_NTP	4/10/2022 1:42 PM	File folder
Scripts	2/23/2022 1:21 PM	File folder
Software	8/6/2021 11:26 AM	File folder

File name: outbound.mycp.lab

Save as type: Certificate file (*.cer)



Please follow these steps in order to enable HTTPS Inspection:

Step 1

Outbound CA Certificate was created successfully on 4/21/2022

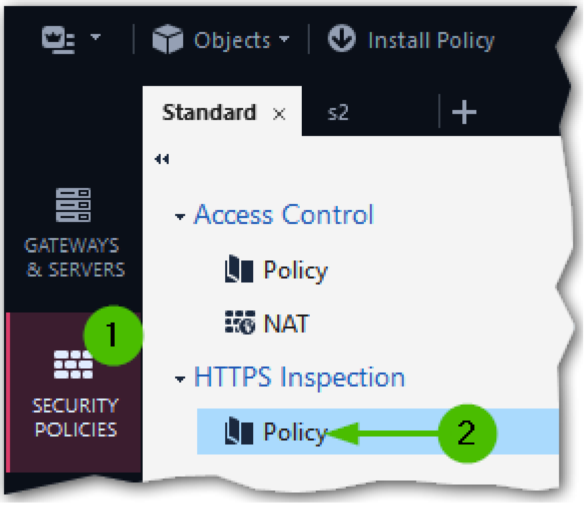
Step 2

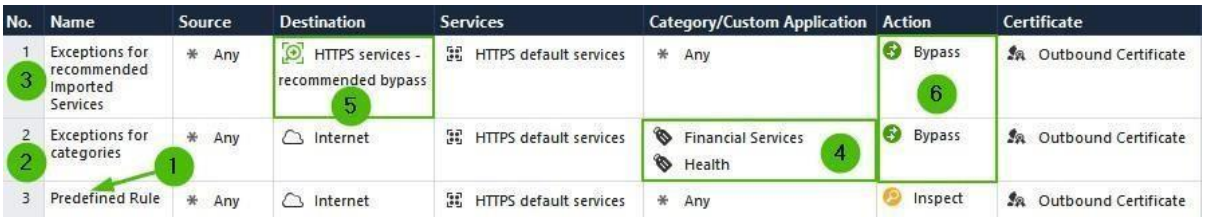
Deploy the outbound certificate in your organization Learn more...

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

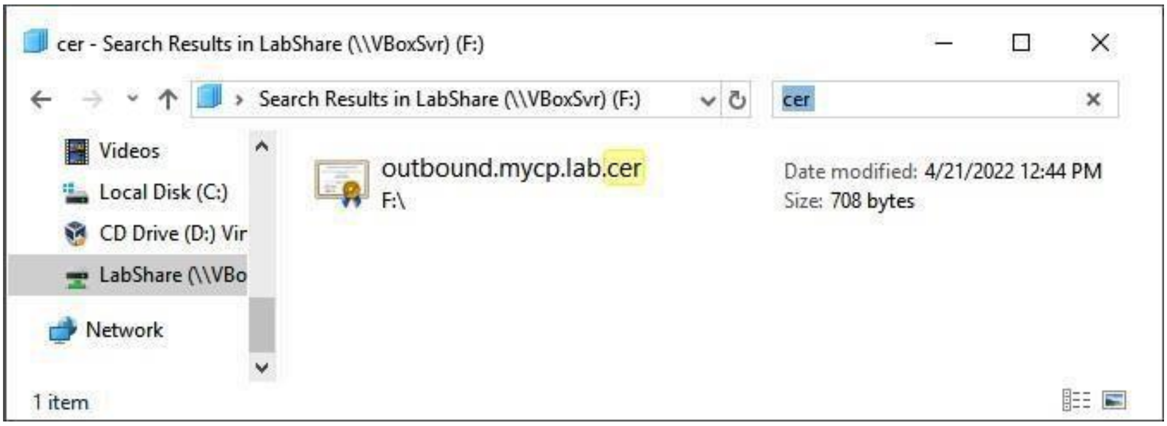
Step 3

☑ Enable HTTPS Inspection





No.	Name	Source	Destination	Services	Category/Custom Application	Action	Certificate
1	Exceptions for recommended Imported Services	Any	HTTPS services - recommended bypass	HTTPS default services	Any	Bypass	Outbound Certificate
2	Exceptions for categories	Any	Internet	HTTPS default services	Financial Services Health	Bypass	Outbound Certificate
3	Predefined Rule	Any	Internet	HTTPS default services	Any	Inspect	Outbound Certificate



cer - Search Results in LabShare (\\VBoxSvr) (F:)

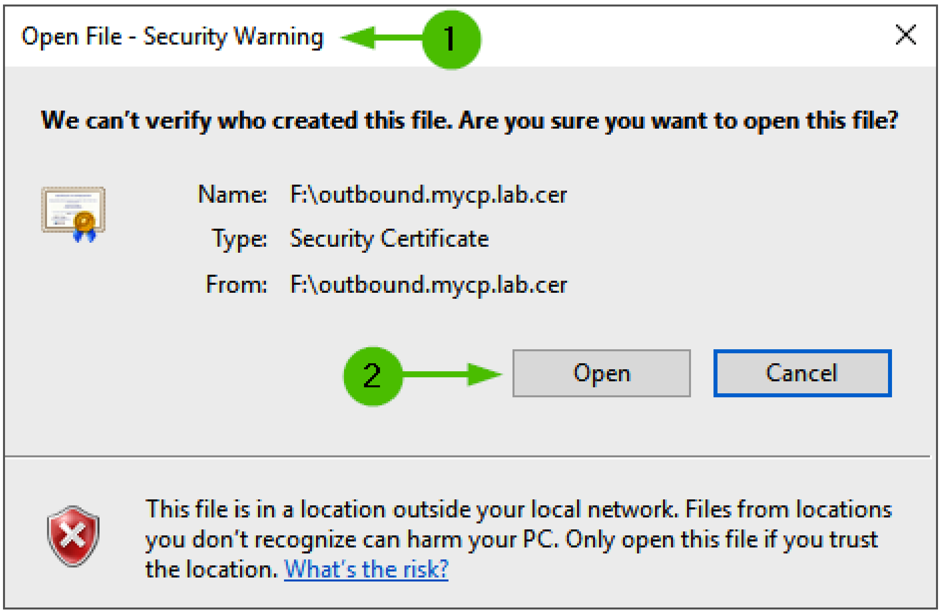
Search Results in LabShare (\\VBoxSvr) (F:)

cer

outbound.mycp.lab.cer
F:\

Date modified: 4/21/2022 12:44 PM
Size: 708 bytes

1 item

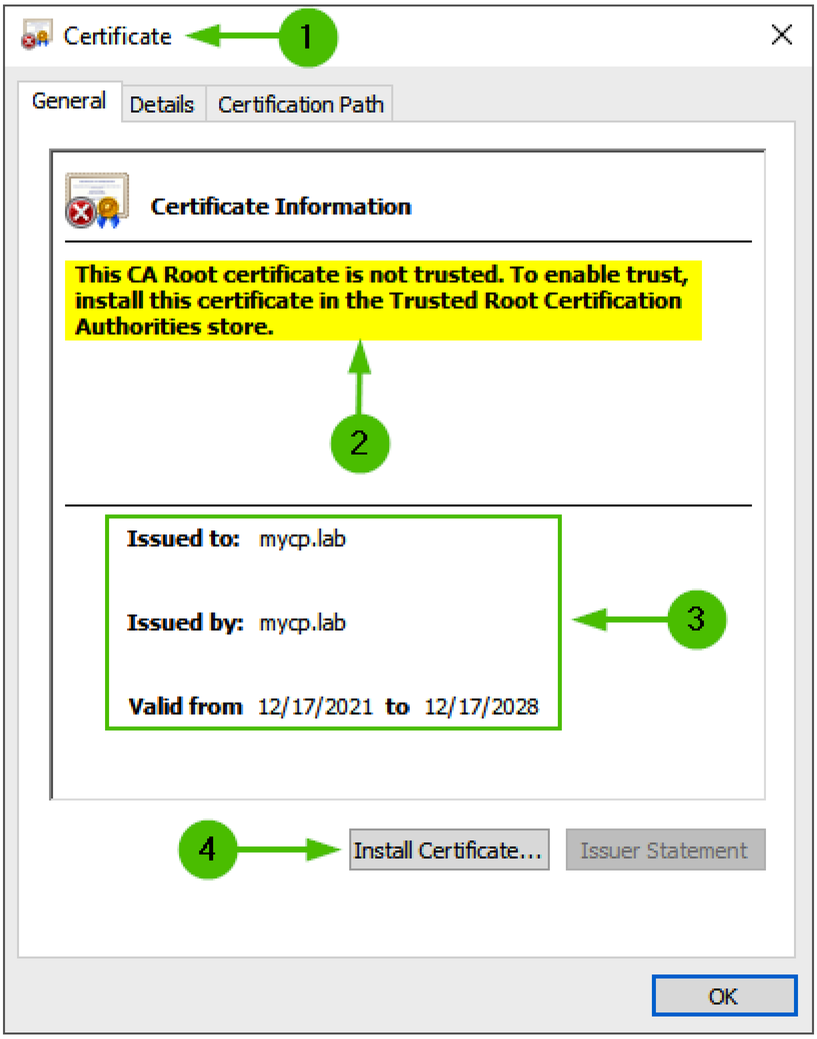


Open File - Security Warning

We can't verify who created this file. Are you sure you want to open this file?

Name: F:\outbound.mycp.lab.cer
Type: Security Certificate
From: F:\outbound.mycp.lab.cer

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only open this file if you trust the location. What's the risk?



Certificate

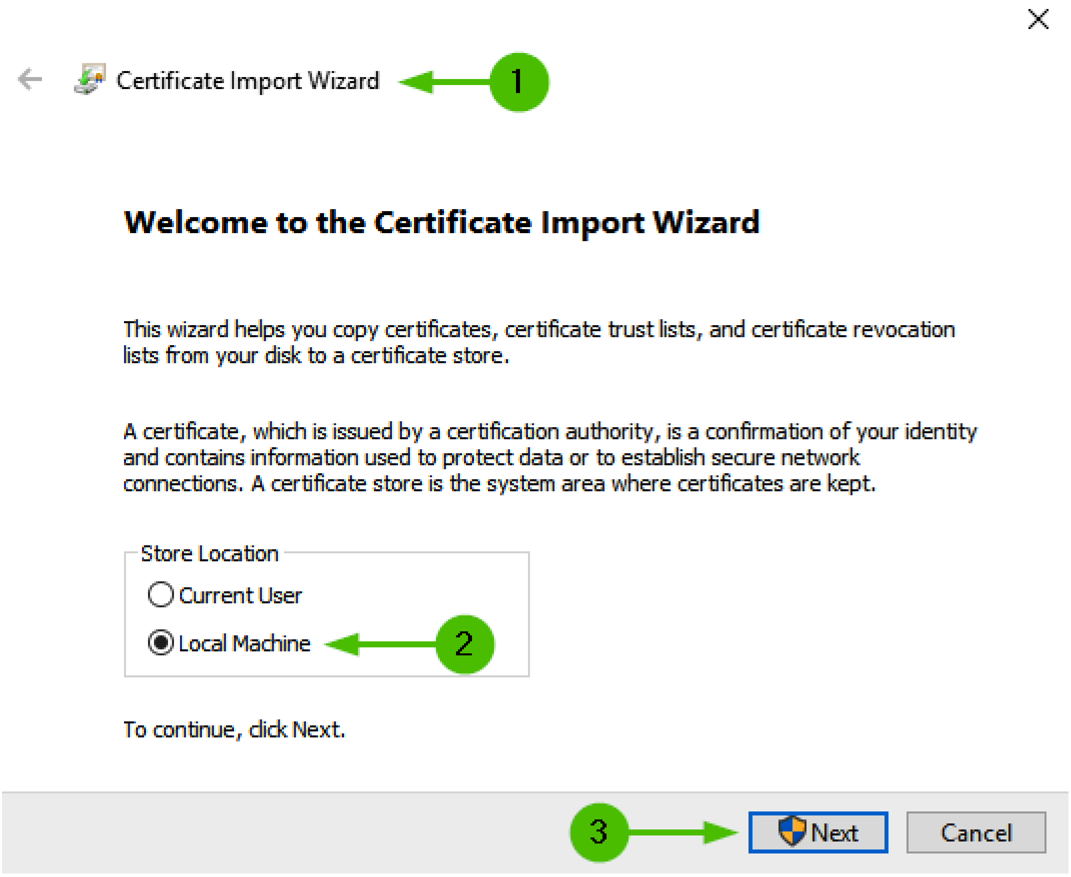
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: mycp.lab

Issued by: mycp.lab

Valid from 12/17/2021 **to** 12/17/2028



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

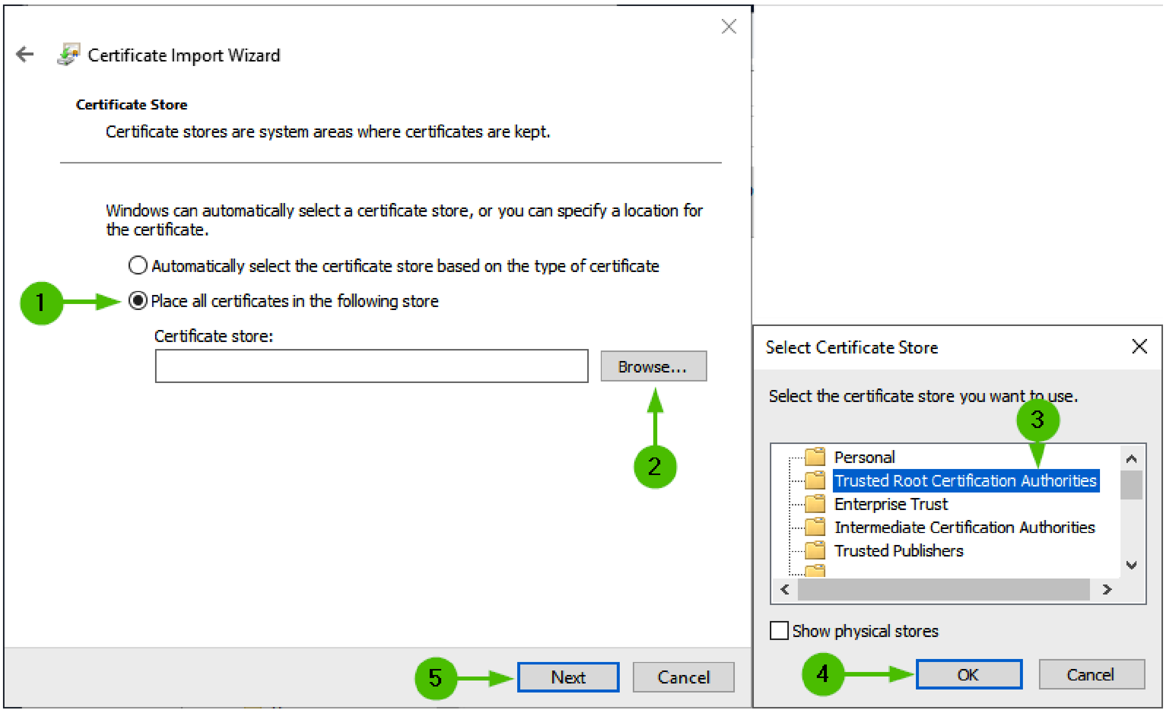
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

● Local Machine

To continue, click Next.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

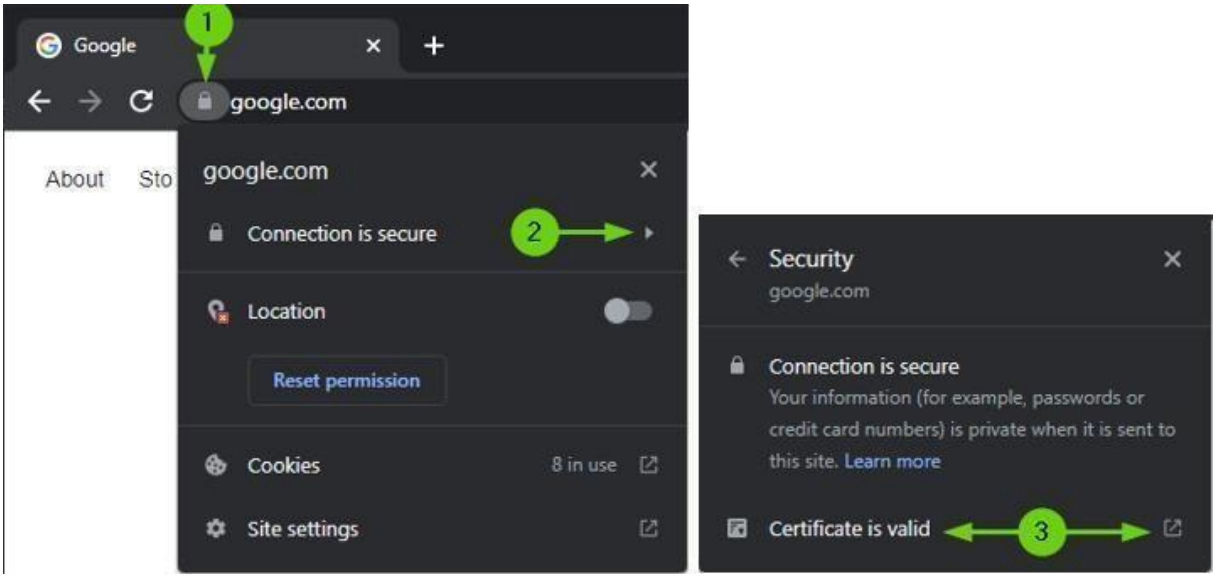
● Place all certificates in the following store

Certificate store:

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers

□ Show physical stores

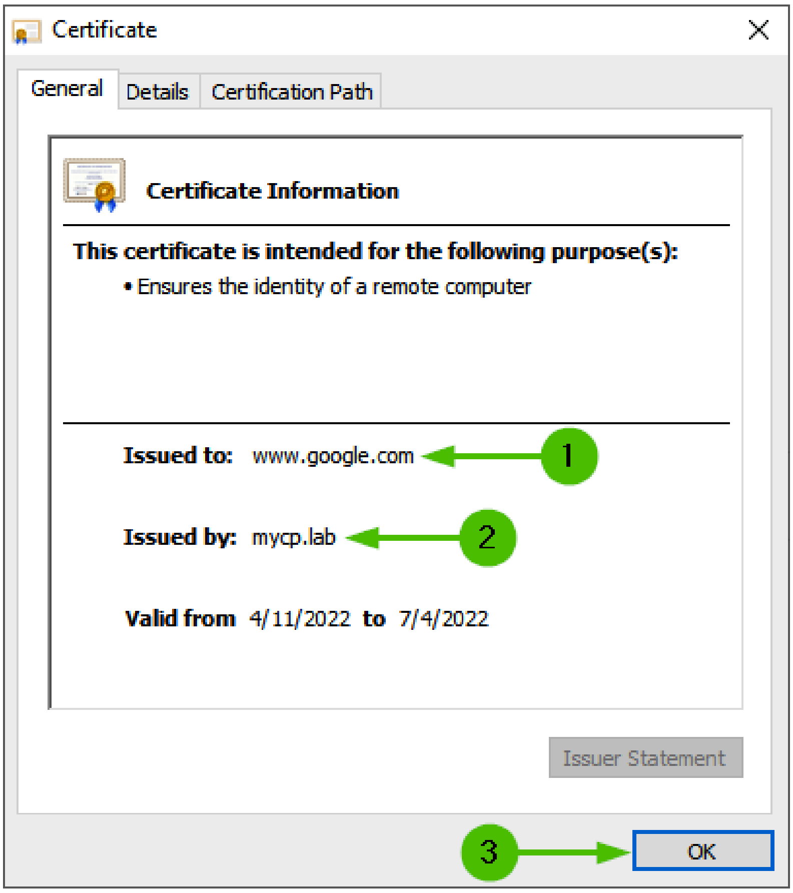


Connection is secure

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid



Certificate Information

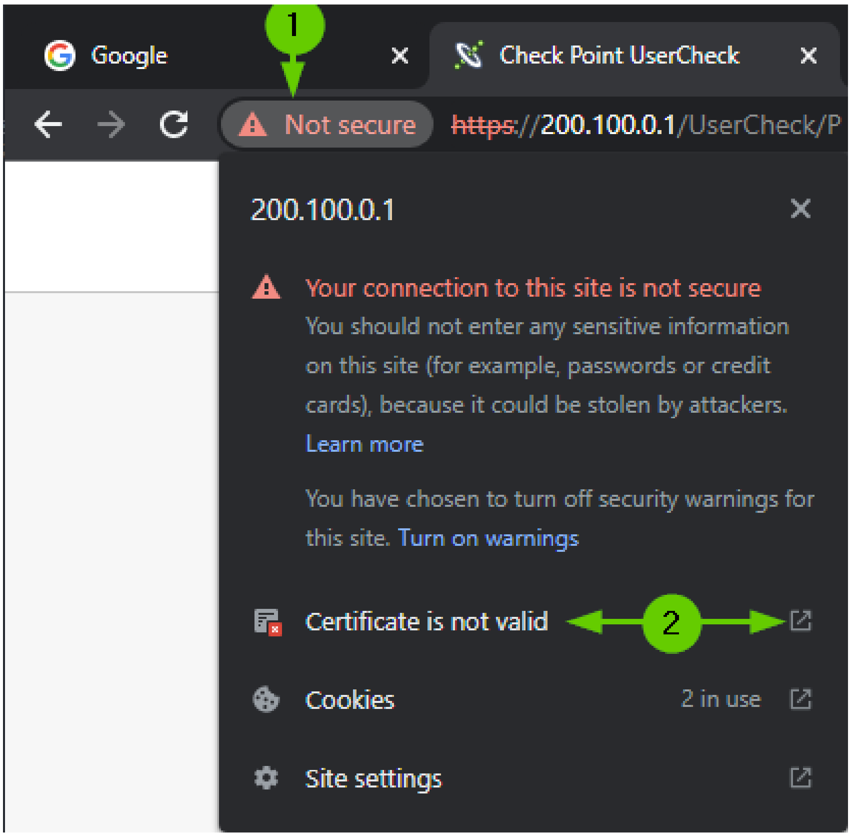
This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: www.google.com

Issued by: mycp.lab

Valid from 4/11/2022 to 7/4/2022



200.100.0.1

Your connection to this site is not secure

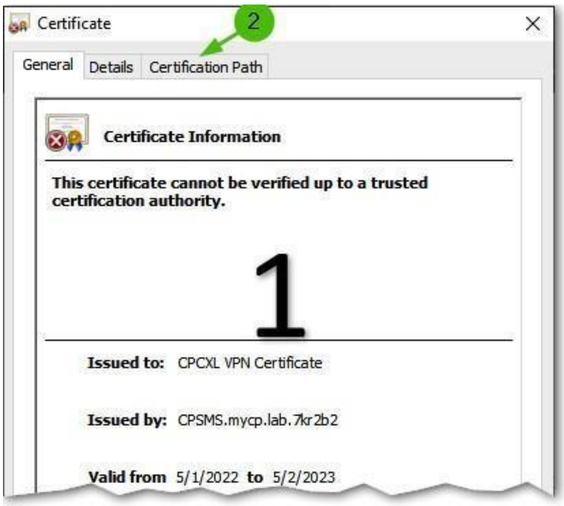
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to turn off security warnings for this site. Turn on warnings

Certificate is not valid

Cookies 2 in use

Site settings



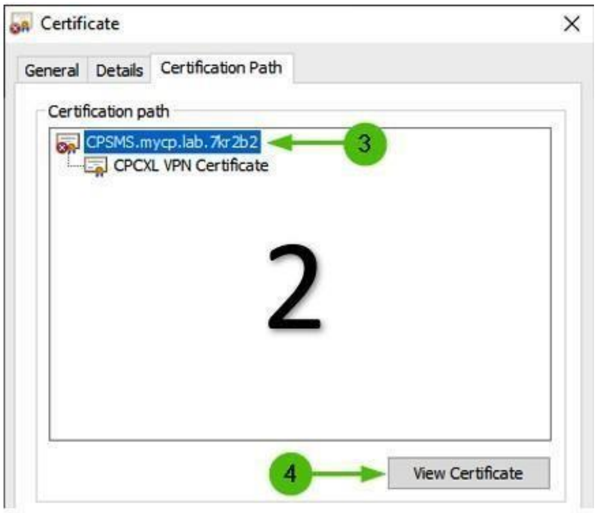
Certificate Information

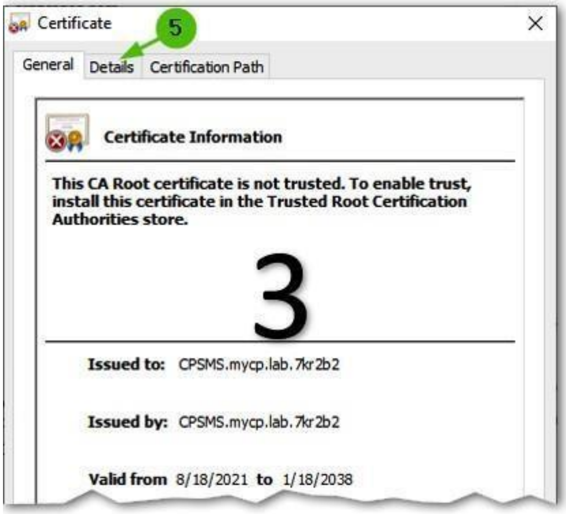
This certificate cannot be verified up to a trusted certification authority.

Issued to: CPCXL VPN Certificate

Issued by: CPSMS.mycp.lab.7kr2b2

Valid from 5/1/2022 **to** 5/2/2023





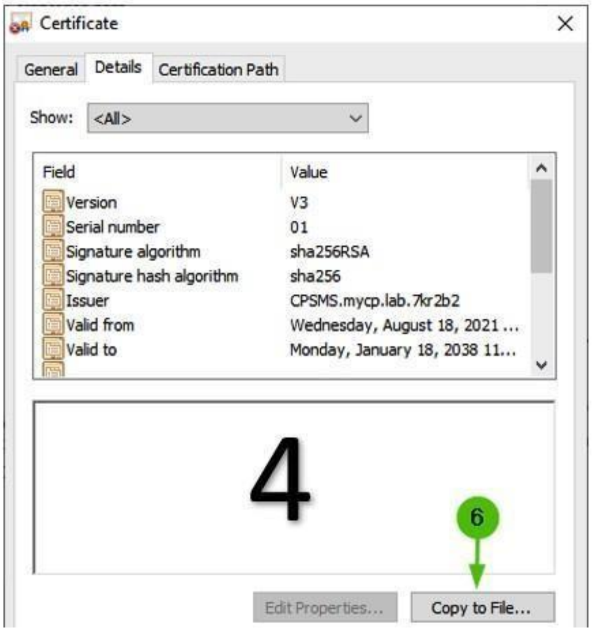
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: CPSMS.mycp.lab.7kr2b2

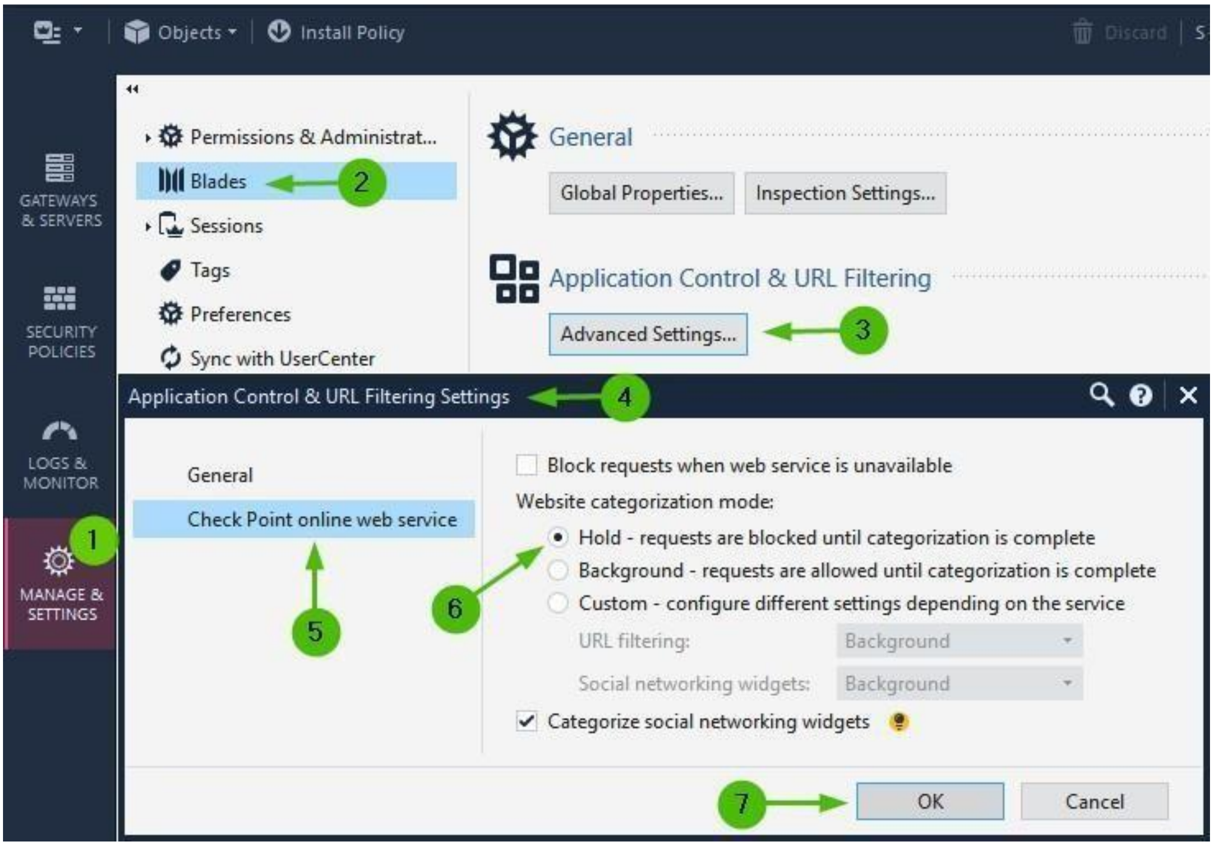
Issued by: CPSMS.mycp.lab.7kr2b2

Valid from 8/18/2021 **to** 1/18/2038



Show: <All>

Field	Value
Version	V3
Serial number	01
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CPSMS.mycp.lab.7kr2b2
Valid from	Wednesday, August 18, 2021 ...
Valid to	Monday, January 18, 2038 11...



Application Control & URL Filtering Settings

□ Block requests when web service is unavailable

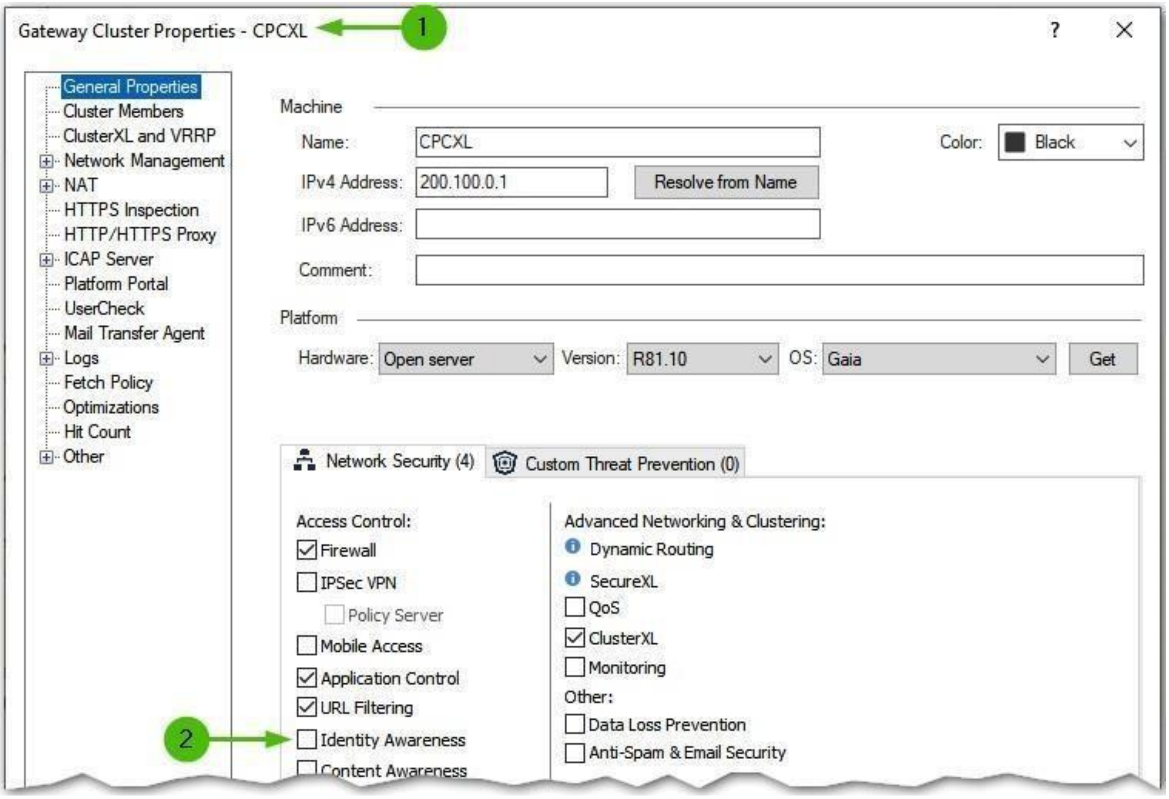
Website categorization mode:

● Hold - requests are blocked until categorization is complete
○ Background - requests are allowed until categorization is complete
○ Custom - configure different settings depending on the service

URL filtering: Background

Social networking widgets: Background

☑ Categorize social networking widgets



Gateway Cluster Properties - CPCXL

Machine

Name: CPCXL

IPv4 Address: 200.100.0.1

IPv6 Address:

Comment:

Color: Black

Platform

Hardware: Open server

Version: R81.10

OS: Gaia

Access Control:

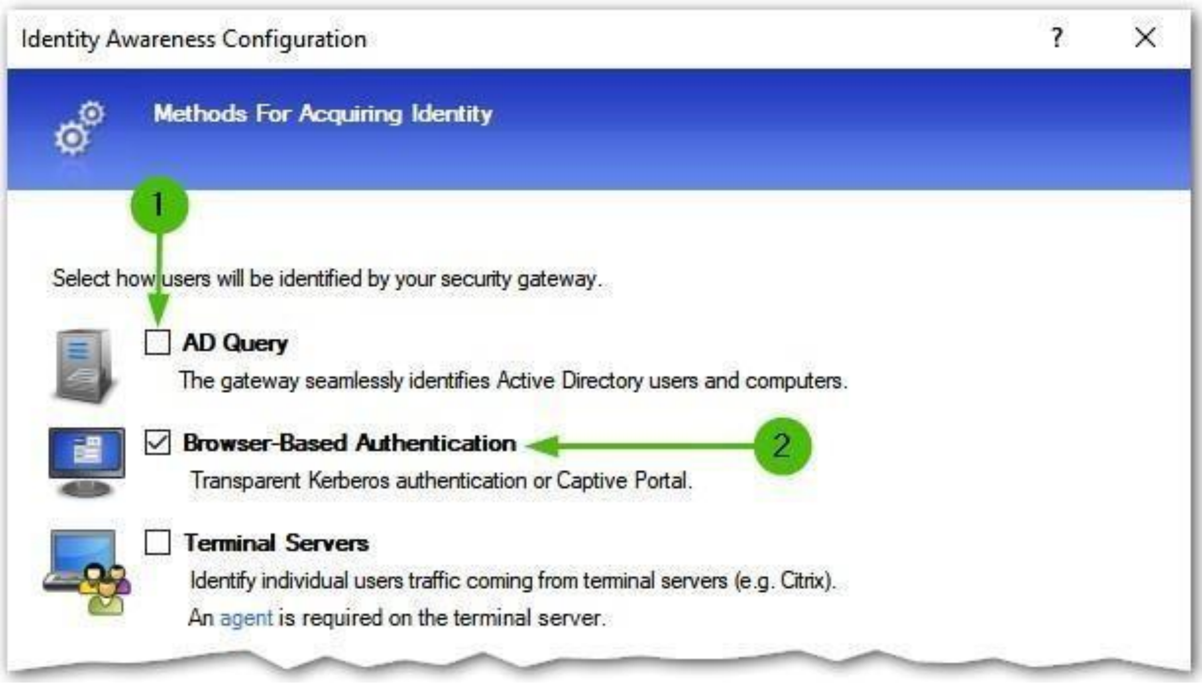
☑ Firewall
□ IPSec VPN
□ Policy Server
□ Mobile Access
☑ Application Control
☑ URL Filtering
□ Identity Awareness
□ Content Awareness

Advanced Networking & Clustering:

Dynamic Routing
SecureXL
□ QoS
☑ ClusterXL
□ Monitoring

Other:

□ Data Loss Prevention
□ Anti-Spam & Email Security



Identity Awareness Configuration

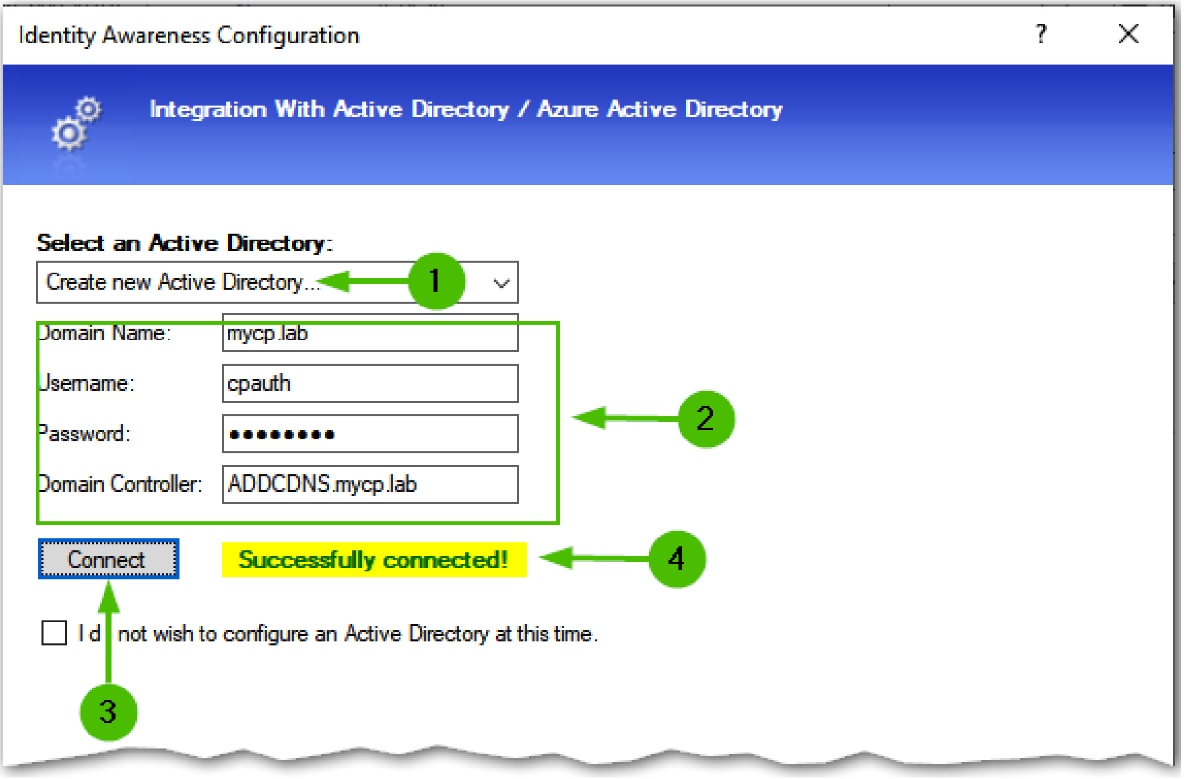
Methods For Acquiring Identity

Select how users will be identified by your security gateway.

☐ **AD Query**
The gateway seamlessly identifies Active Directory users and computers.

☑ **Browser-Based Authentication**
Transparent Kerberos authentication or Captive Portal.

☐ **Terminal Servers**
Identify individual users traffic coming from terminal servers (e.g. Citrix).
An agent is required on the terminal server.



Identity Awareness Configuration

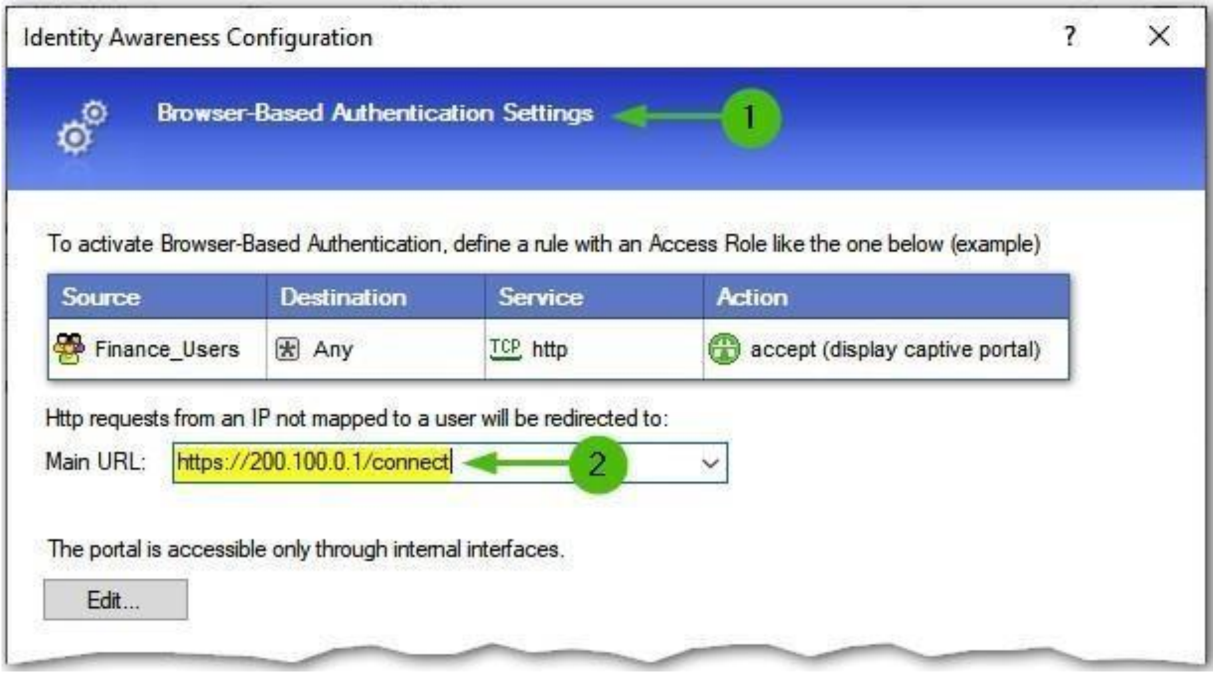
Integration With Active Directory / Azure Active Directory

Select an Active Directory:
Create new Active Directory...

Domain Name: mycp.lab
Username: cpauth
Password: ••••••••
Domain Controller: ADDCDNS.mycp.lab

Connect | **Successfully connected!**

☐ I do not wish to configure an Active Directory at this time.


Identity Awareness Configuration

Browser-Based Authentication Settings

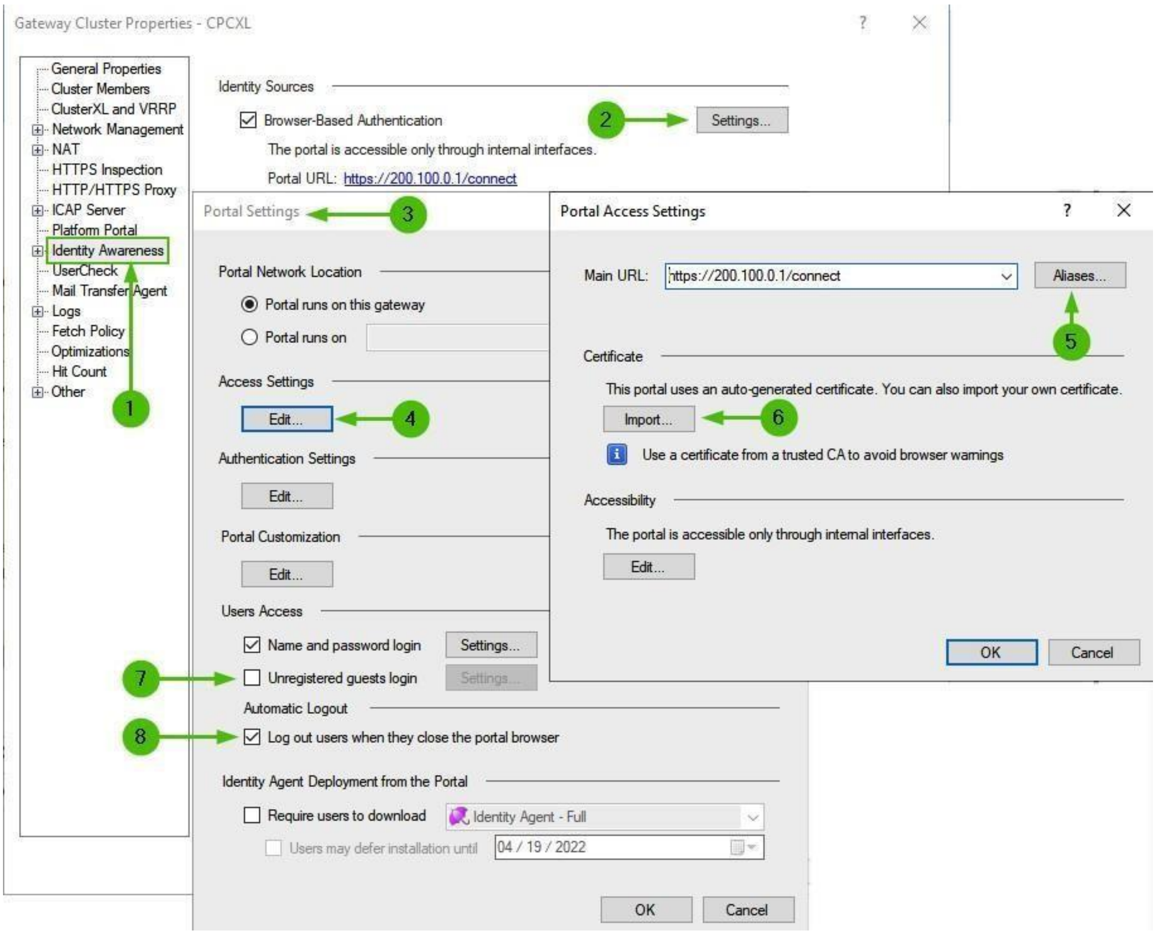
To activate Browser-Based Authentication, define a rule with an Access Role like the one below (example)

Source	Destination	Service	Action
Finance_Users	Any	TCP http	accept (display captive portal)

Http requests from an IP not mapped to a user will be redirected to:

Main URL: https://200.100.0.1/connect

The portal is accessible only through internal interfaces.


Gateway Cluster Properties - CPCXL

Identity Sources

☑ Browser-Based Authentication

The portal is accessible only through internal interfaces.

Portal URL: https://200.100.0.1/connect

Portal Settings

Portal Network Location

● Portal runs on this gateway

○ Portal runs on

Access Settings

Authentication Settings

Portal Customization

Users Access

☑ Name and password login

☐ Unregistered guests login

Automatic Logout

☑ Log out users when they close the portal browser

Identity Agent Deployment from the Portal

☐ Require users to download: Identity Agent - Full

☐ Users may defer installation until 04 / 19 / 2022

Portal Access Settings

Main URL: https://200.100.0.1/connect

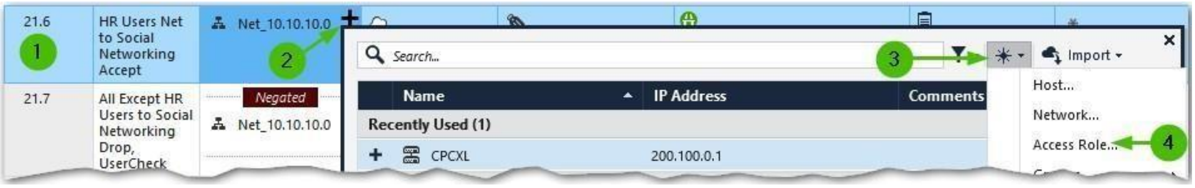
Certificate

This portal uses an auto-generated certificate. You can also import your own certificate.

Use a certificate from a trusted CA to avoid browser warnings

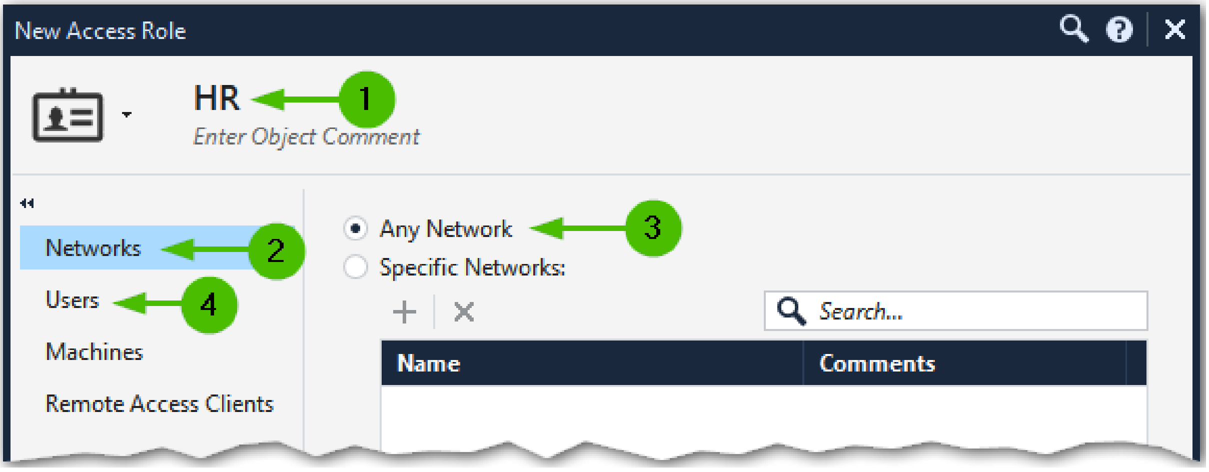
Accessibility

The portal is accessible only through internal interfaces.



21.6	HR Users Net to Social Networking Accept	Net_10.10.10.0
21.7	All Except HR Users to Social Networking Drop, UserCheck	Negated Net_10.10.10.0

Name	IP Address	Comments
Recently Used (1)		
CPCXL	200.100.0.1	

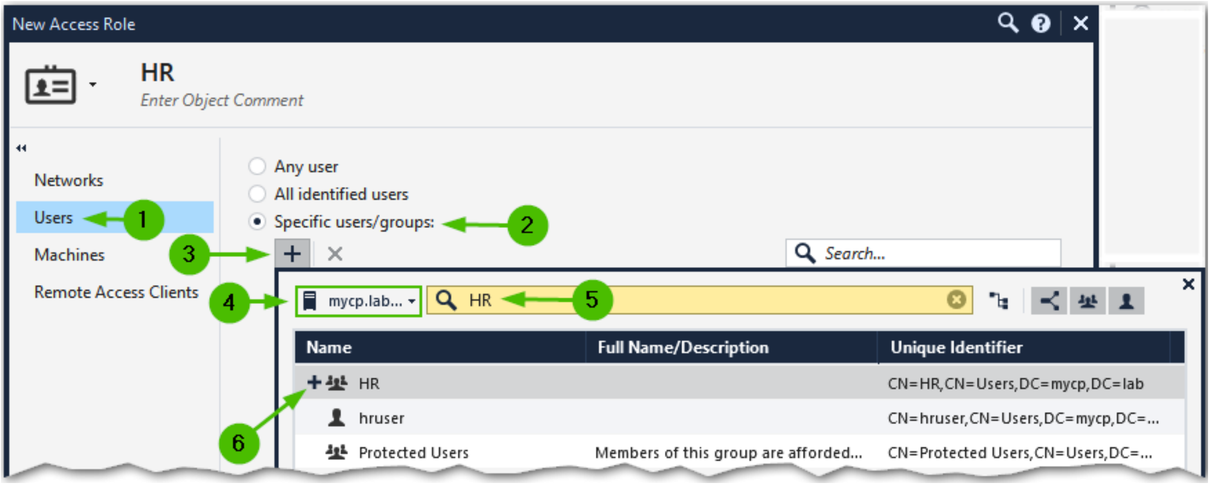


New Access Role

HR
Enter Object Comment

● Any Network
○ Specific Networks:

Name	Comments



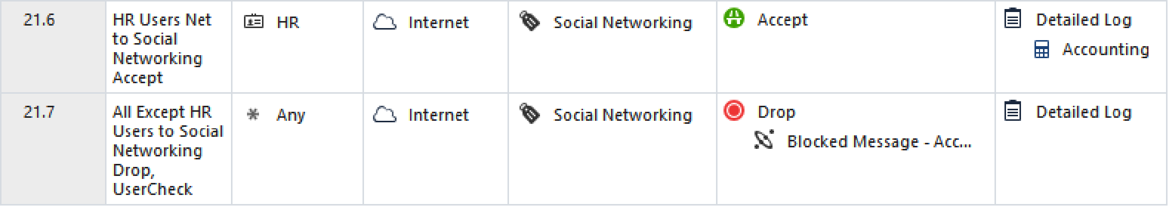
New Access Role

HR
Enter Object Comment

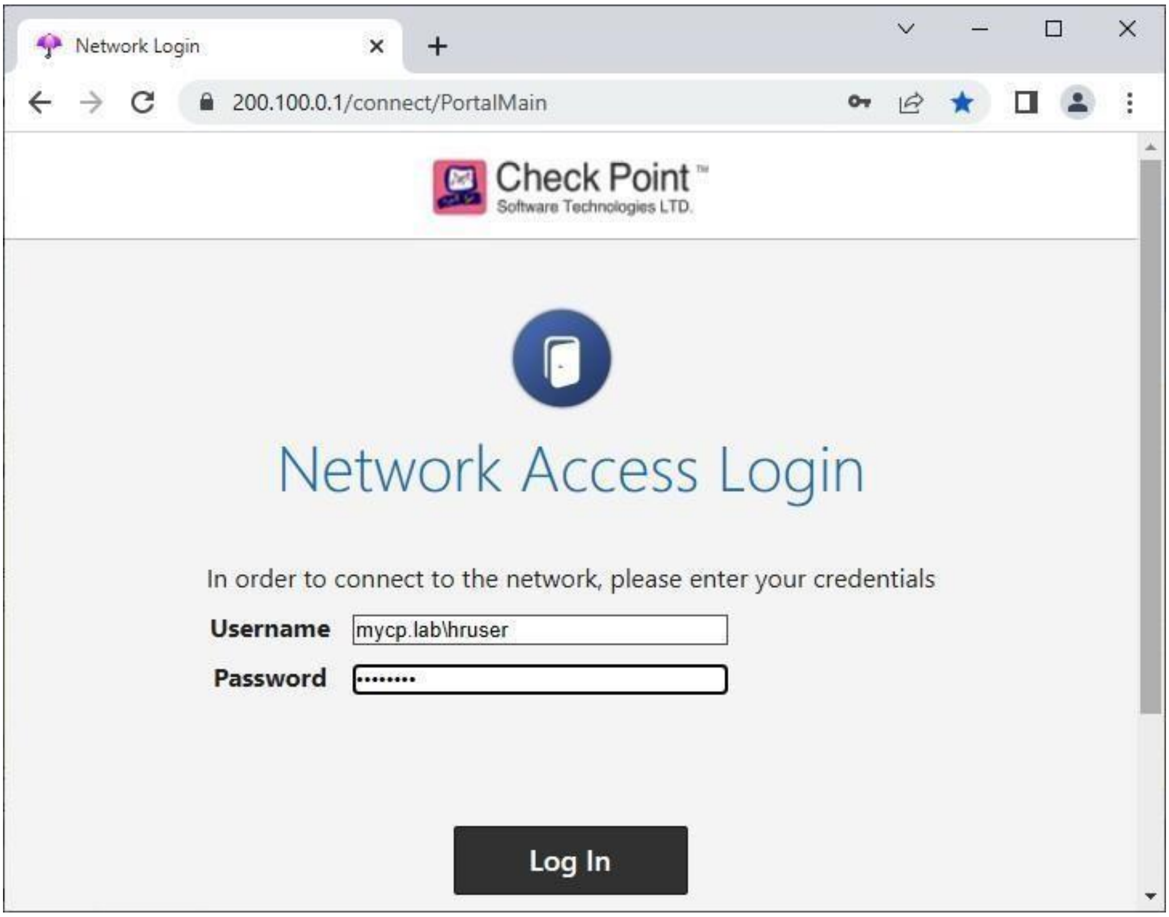
○ Any user
○ All identified users
● Specific users/groups:

mycp.lab...
HR

Name	Full Name/Description	Unique Identifier
HR		CN=HR,CN=Users,DC=mycp,DC=lab
hruser		CN=hruser,CN=Users,DC=mycp,DC=...
Protected Users	Members of this group are afforded...	CN=Protected Users,CN=Users,DC=...



21.6	HR Users Net to Social Networking Accept	HR	Internet	Social Networking	Accept	Detailed Log Accounting
21.7	All Except HR Users to Social Networking Drop, UserCheck	Any	Internet	Social Networking	Drop Blocked Message - Acc...	Detailed Log

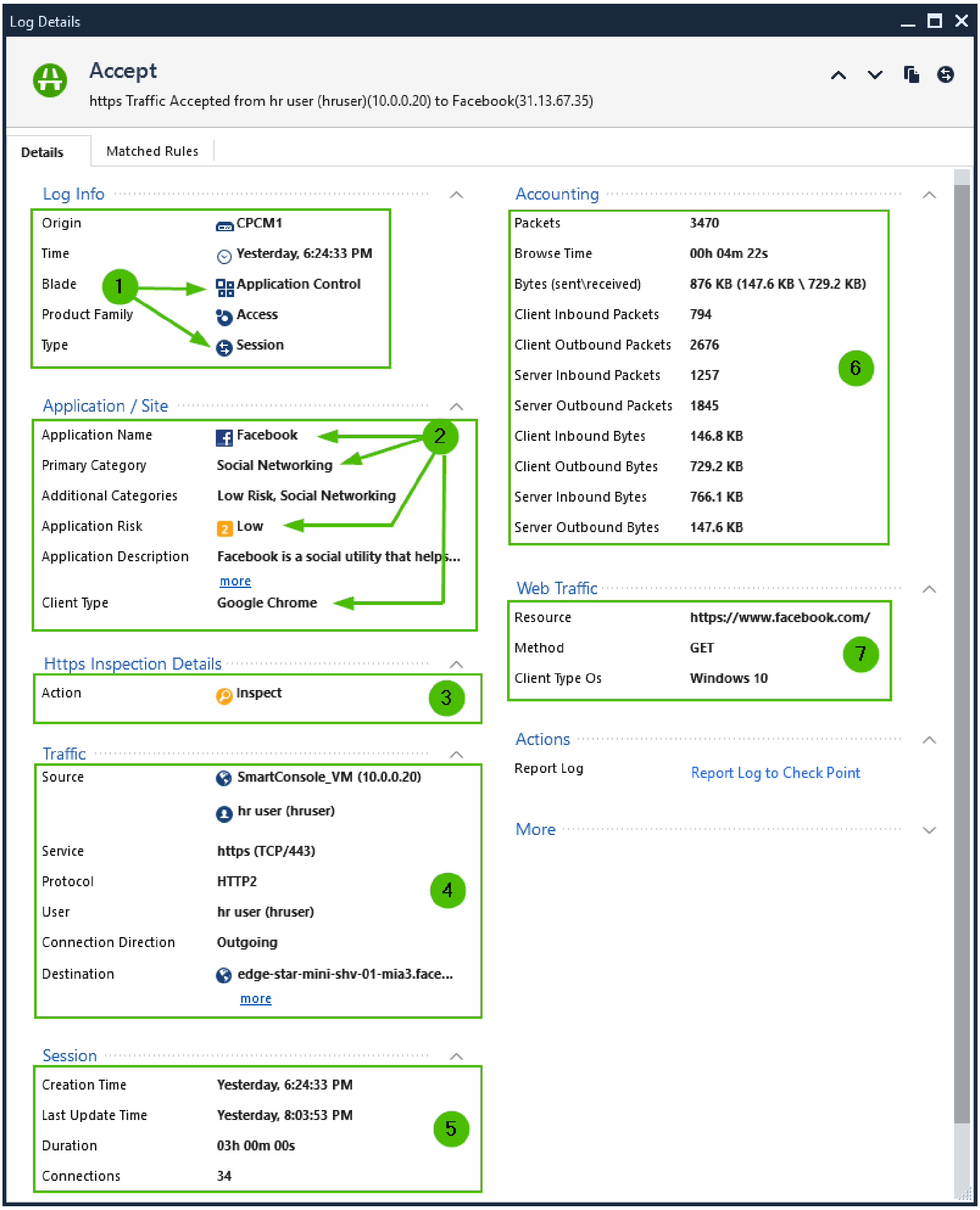


Network Access Login

In order to connect to the network, please enter your credentials

Username mycp.lab\hruser

Password ••••••••



Accept

https Traffic Accepted from hr user (hruser)(10.0.0.20) to Facebook(31.13.67.35)

Log Info

Origin	CPCM1
Time	Yesterday, 6:24:33 PM
Blade	Application Control
Product Family	Access
Type	Session

Application / Site

Application Name	Facebook
Primary Category	Social Networking
Additional Categories	Low Risk, Social Networking
Application Risk	2 Low
Application Description	Facebook is a social utility that helps... more
Client Type	Google Chrome

Https Inspection Details

Action	Inspect

Traffic

Source	SmartConsole_VM (10.0.0.20) hr user (hruser)
Service	https (TCP/443)
Protocol	HTTP2
User	hr user (hruser)
Connection Direction	Outgoing
Destination	edge-star-mini-shv-01-mia3.face... more

Session

Creation Time	Yesterday, 6:24:33 PM
Last Update Time	Yesterday, 8:03:53 PM
Duration	03h 00m 00s
Connections	34

Accounting

Packets	3470
Browse Time	00h 04m 22s
Bytes (sent\received)	876 KB (147.6 KB \ 729.2 KB)
Client Inbound Packets	794
Client Outbound Packets	2676
Server Inbound Packets	1257
Server Outbound Packets	1845
Client Inbound Bytes	146.8 KB
Client Outbound Bytes	729.2 KB
Server Inbound Bytes	766.1 KB
Server Outbound Bytes	147.6 KB

Web Traffic

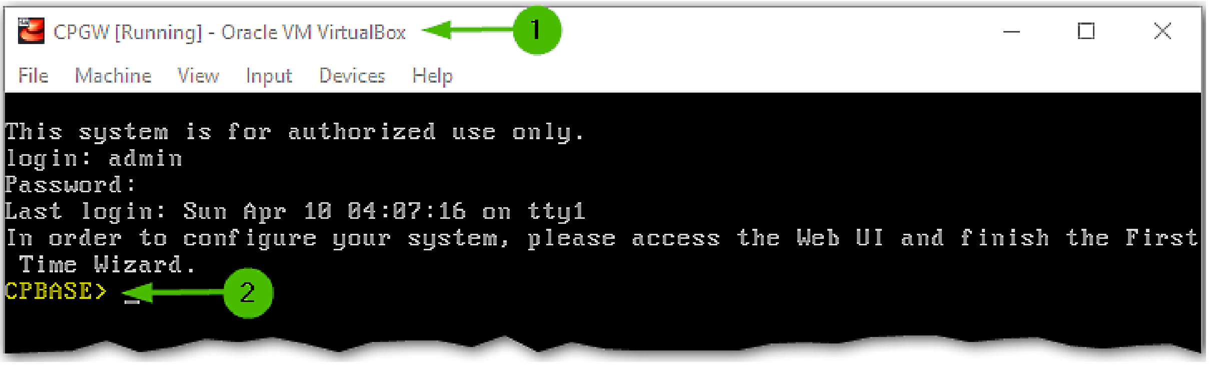
Resource	https://www.facebook.com/
Method	GET
Client Type Os	Windows 10

Actions

Report Log	Report Log to Check Point

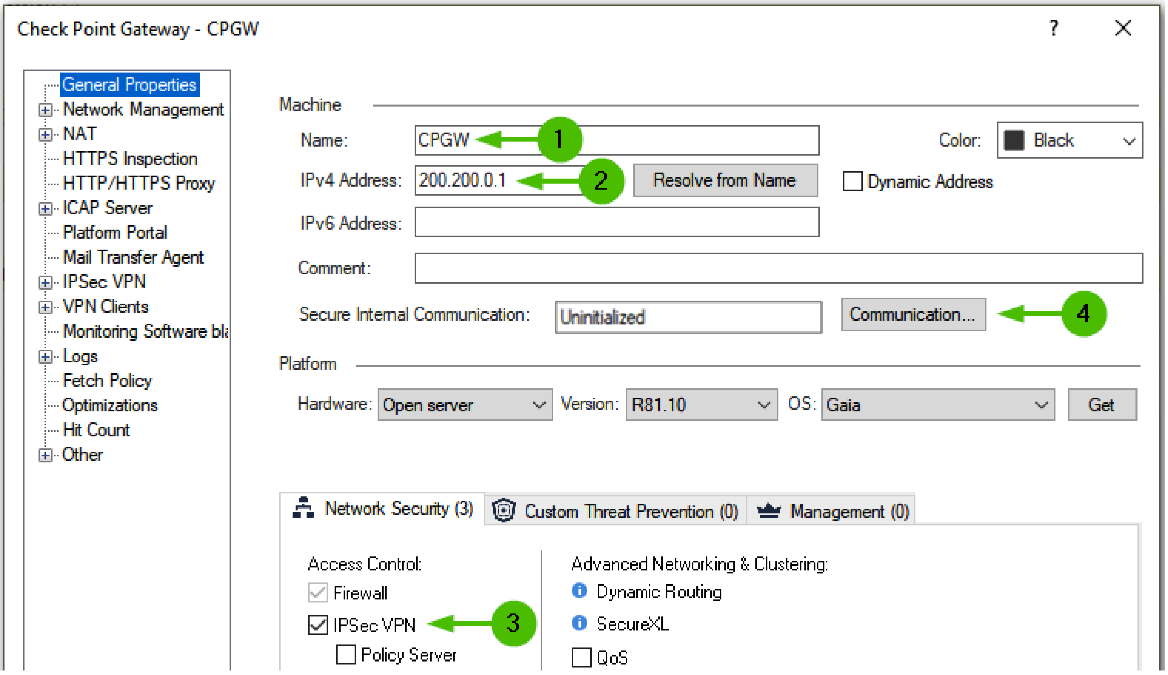
More

Chapter 12: Configuring Site-to-Site and Remote Access VPNs



CPGW [Running] - Oracle VM VirtualBox

```
This system is for authorized use only.
login: admin
Password:
Last login: Sun Apr 10 04:07:16 on tty1
In order to configure your system, please access the Web UI and finish the First
 Time Wizard.
CPBASE> _
```



Check Point Gateway - CPGW

Machine

Name: CPGW

Color: Black

IPv4 Address: 200.200.0.1

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Uninitialized

Platform

Hardware: Open server

Version: R81.10

OS: Gaia

Network Security (3)

Access Control:

☑ Firewall

☑ IPSec VPN

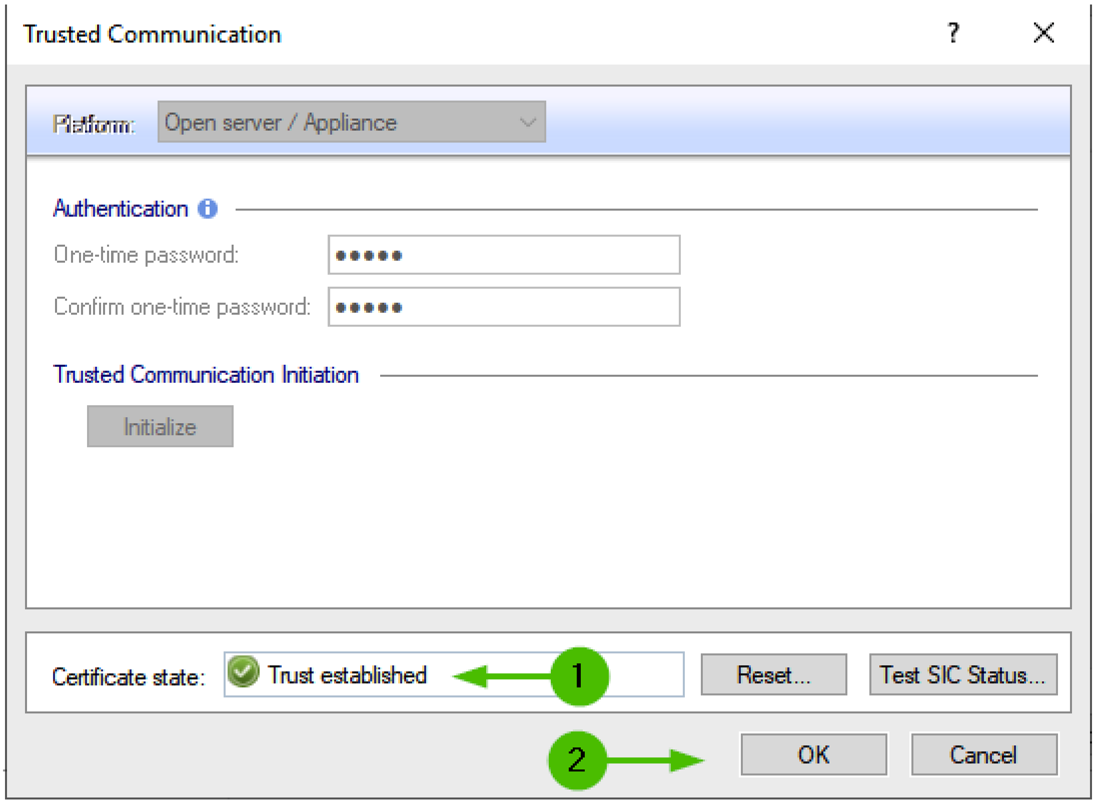
□ Policy Server

Advanced Networking & Clustering:

Dynamic Routing

SecureXL

□ QoS



Trusted Communication

Platform: Open server / Appliance

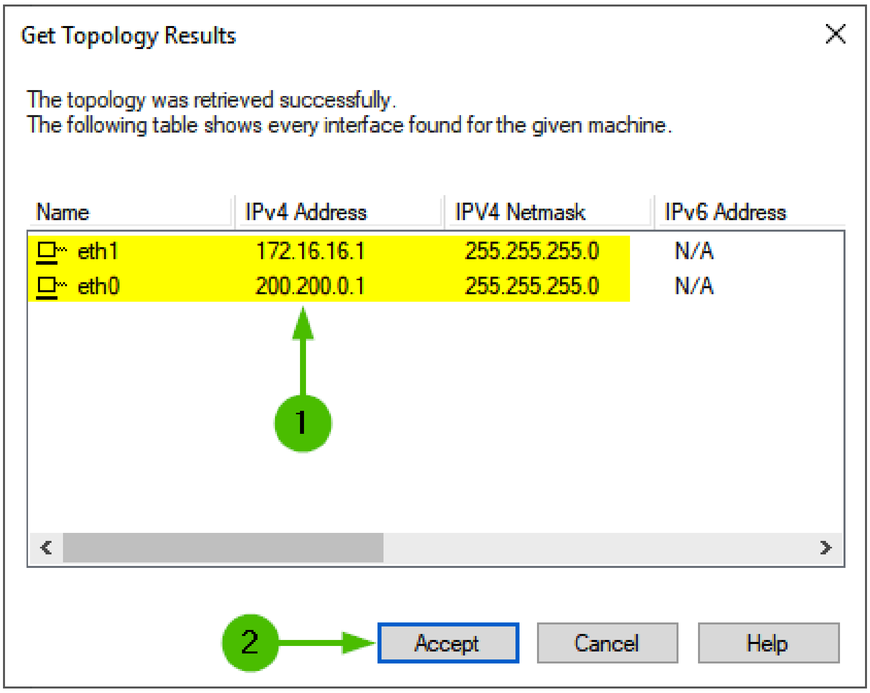
Authentication

One-time password: •••••

Confirm one-time password: •••••

Trusted Communication Initiation

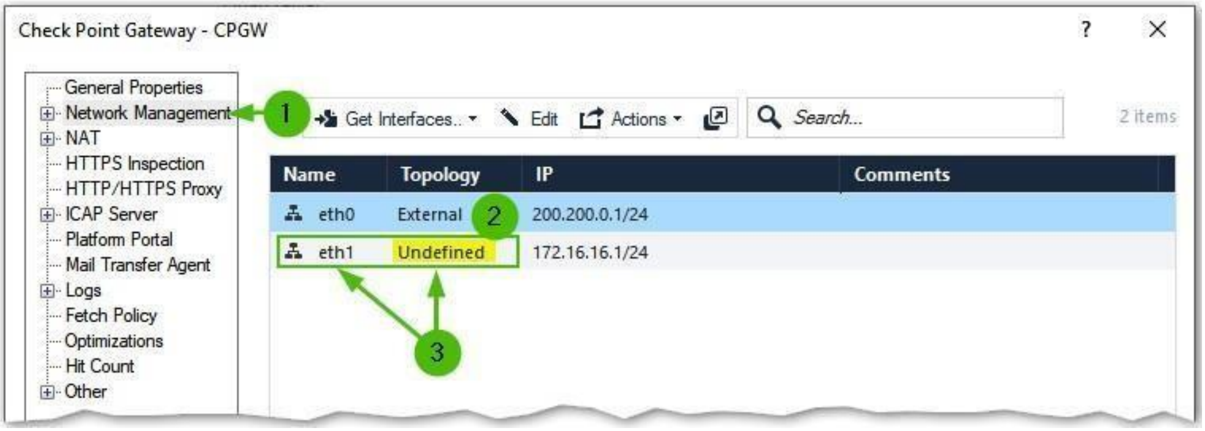
Certificate state: Trust established



Get Topology Results

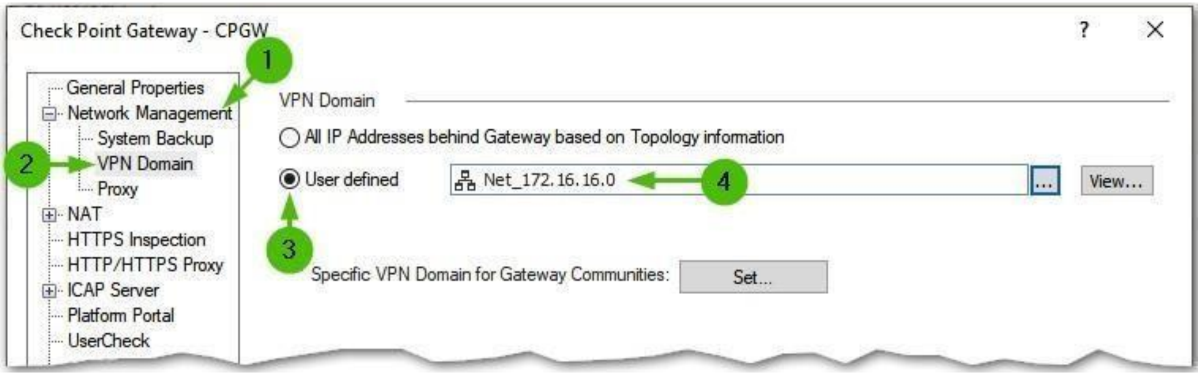
The topology was retrieved successfully.
The following table shows every interface found for the given machine.

Name	IPv4 Address	IPV4 Netmask	IPv6 Address
eth1	172.16.16.1	255.255.255.0	N/A
eth0	200.200.0.1	255.255.255.0	N/A



Check Point Gateway - CPGW

Name	Topology	IP	Comments
eth0	External	200.200.0.1/24	
eth1	Undefined	172.16.16.1/24	



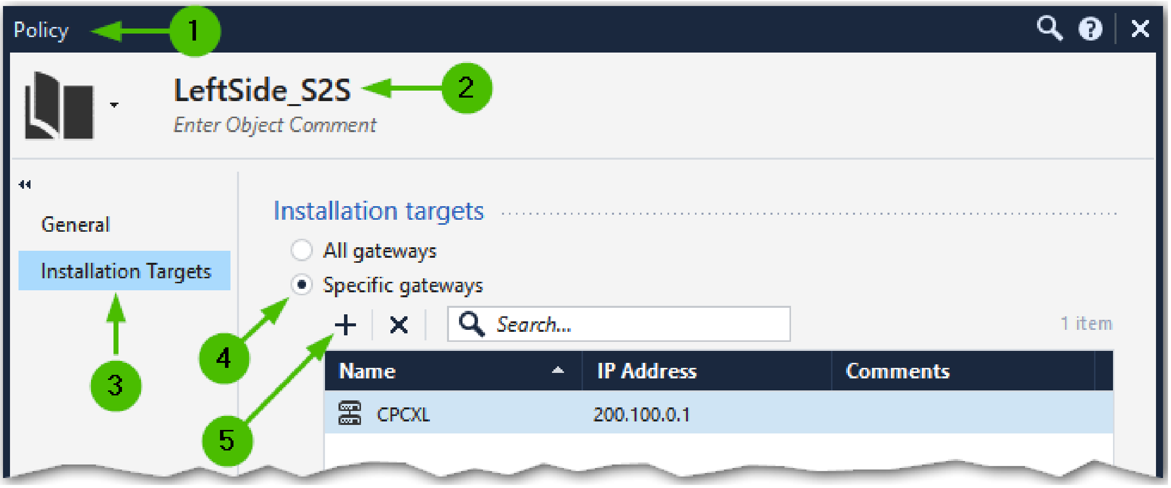
Check Point Gateway - CPGW

VPN Domain

○ All IP Addresses behind Gateway based on Topology information

● User defined: Net_172.16.16.0

Specific VPN Domain for Gateway Communities: Set...



Policy

LeftSide_S2S

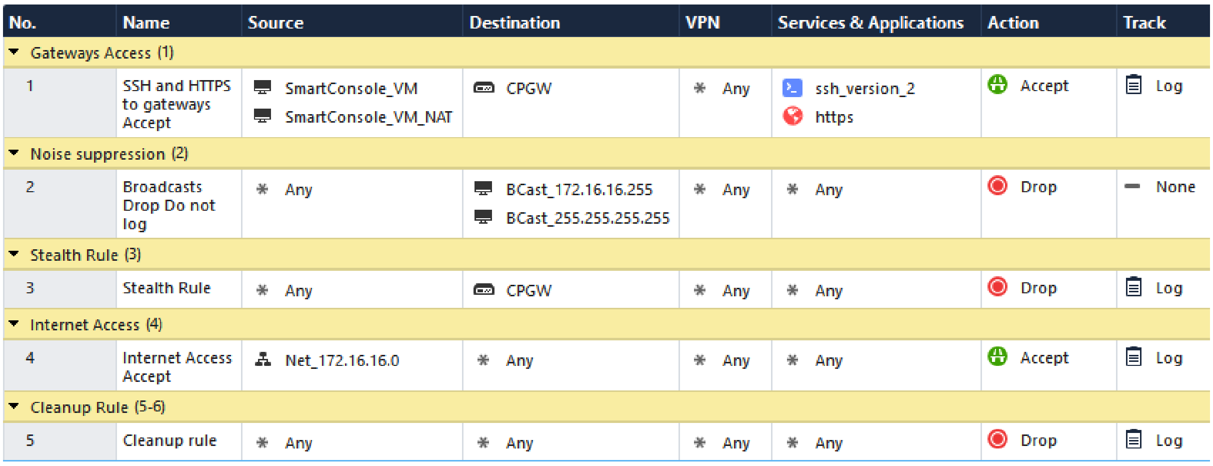
Enter Object Comment

Installation targets

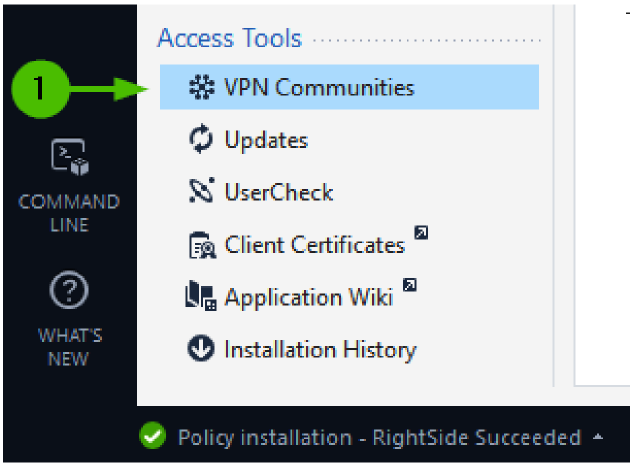
○ All gateways

● Specific gateways

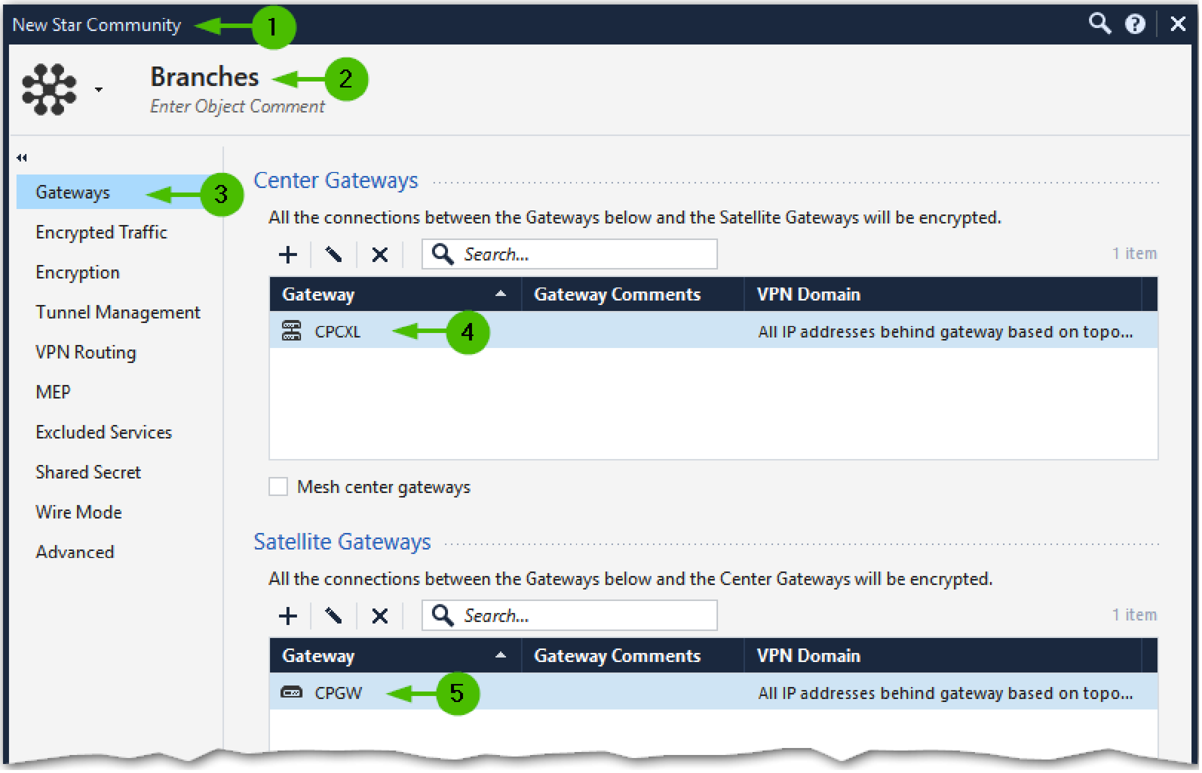
Name	IP Address	Comments
CPCXL	200.100.0.1	



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
▾ Gateways Access (1)							
1	SSH and HTTPS to gateways Accept	SmartConsole_VM SmartConsole_VM_NAT	CPGW	* Any	ssh_version_2 https	Accept	Log
▾ Noise suppression (2)							
2	Broadcasts Drop Do not log	* Any	BCast_172.16.16.255 BCast_255.255.255.255	* Any	* Any	Drop	None
▾ Stealth Rule (3)							
3	Stealth Rule	* Any	CPGW	* Any	* Any	Drop	Log
▾ Internet Access (4)							
4	Internet Access Accept	Net_172.16.16.0	* Any	* Any	* Any	Accept	Log
▾ Cleanup Rule (5-6)							
5	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log



Policy installation - RightSide Succeeded



New Star Community

Branches

Enter Object Comment

Center Gateways

All the connections between the Gateways below and the Satellite Gateways will be encrypted.

Search... 1 item

Gateway	Gateway Comments	VPN Domain
CPCXL		All IP addresses behind gateway based on topo...

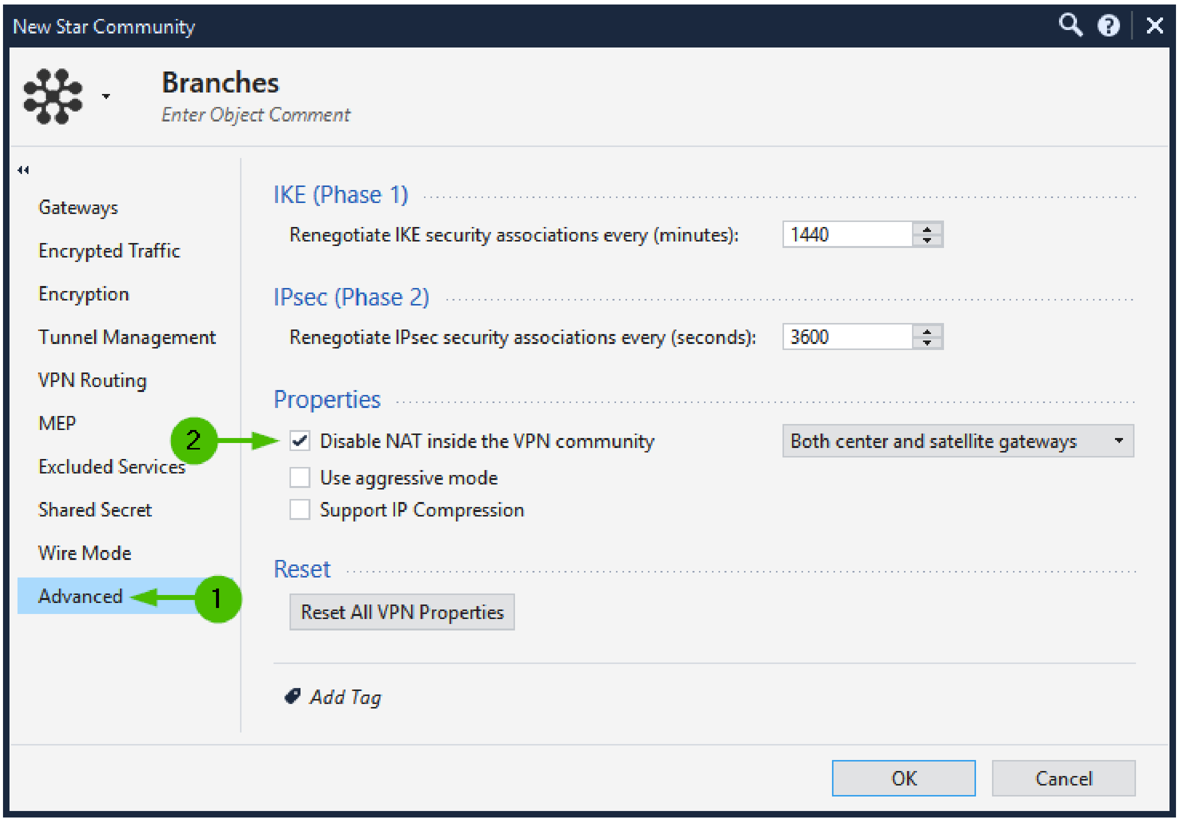
□ Mesh center gateways

Satellite Gateways

All the connections between the Gateways below and the Center Gateways will be encrypted.

Search... 1 item

Gateway	Gateway Comments	VPN Domain
CPGW		All IP addresses behind gateway based on topo...



New Star Community

Branches

Enter Object Comment

IKE (Phase 1)

Renegotiate IKE security associations every (minutes): 1440

IPsec (Phase 2)

Renegotiate IPsec security associations every (seconds): 3600

Properties

☑ Disable NAT inside the VPN community — Both center and satellite gateways

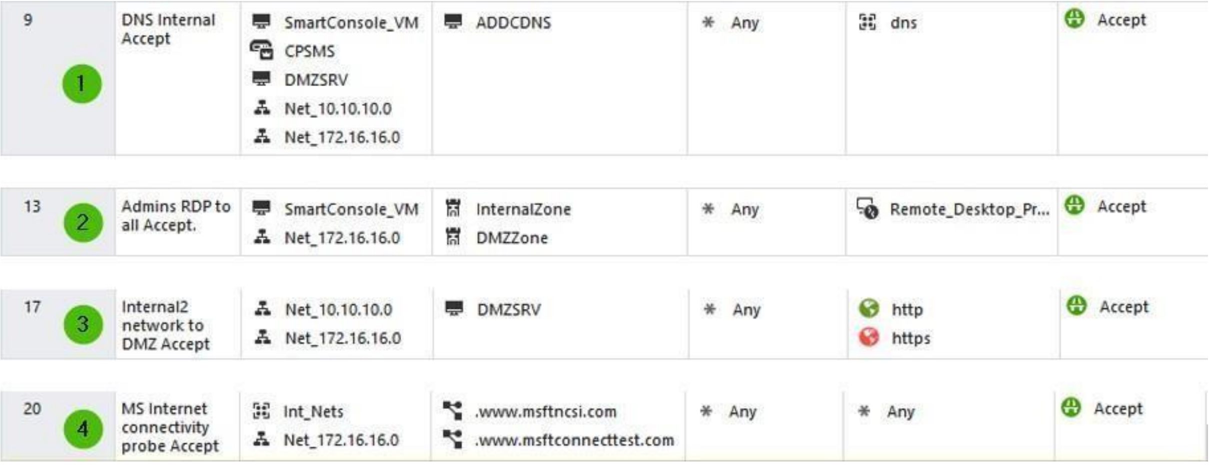
□ Use aggressive mode

□ Support IP Compression

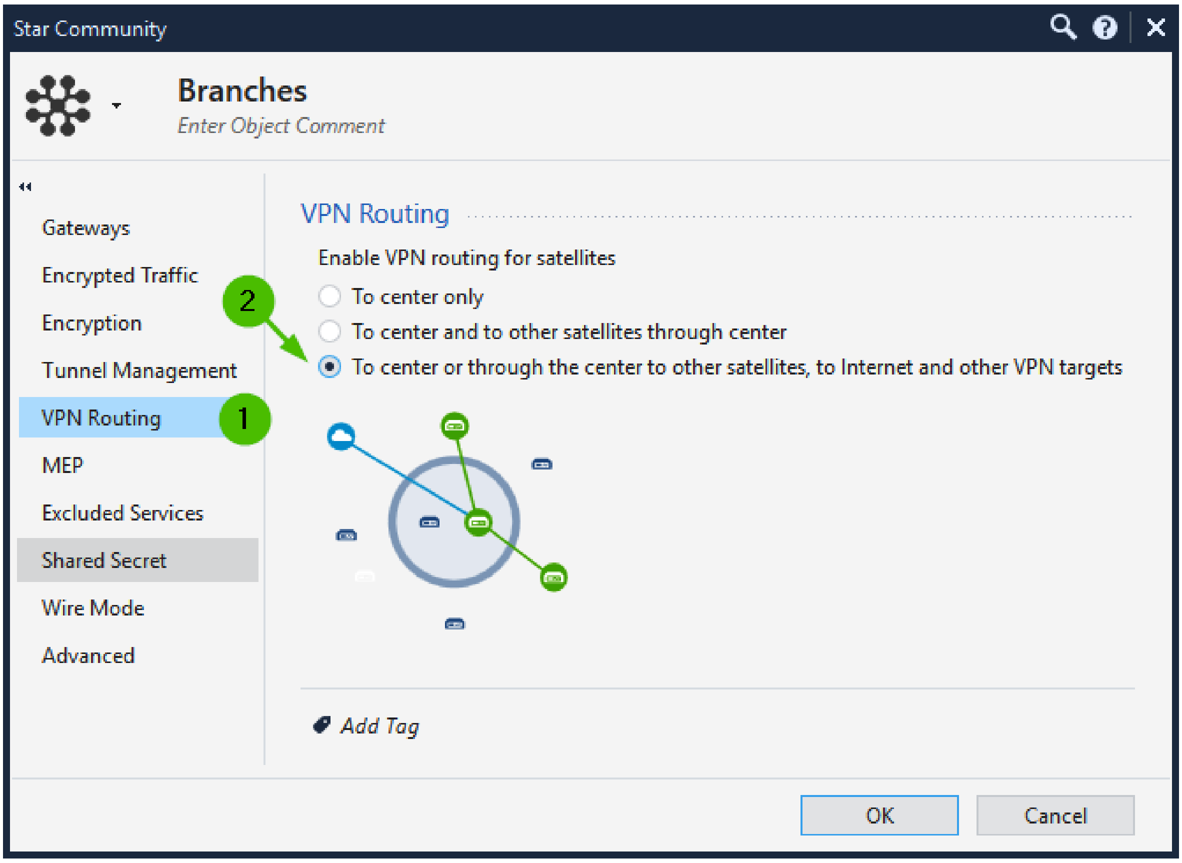
Reset

Reset All VPN Properties

Add Tag



9 1	DNS Internal Accept	SmartConsole_VM CPSMS DMZSRV Net_10.10.10.0 Net_172.16.16.0	ADDCDNS	Any	dns	Accept
13 2	Admins RDP to all Accept.	SmartConsole_VM Net_172.16.16.0	InternalZone DMZZone	Any	Remote_Desktop_Pr...	Accept
17 3	Internal2 network to DMZ Accept	Net_10.10.10.0 Net_172.16.16.0	DMZSRV	Any	http https	Accept
20 4	MS Internet connectivity probe Accept	Int_Nets Net_172.16.16.0	.www.msftncsi.com .www.msftconnecttest.com	Any	Any	Accept



Star Community

Branches

Enter Object Comment

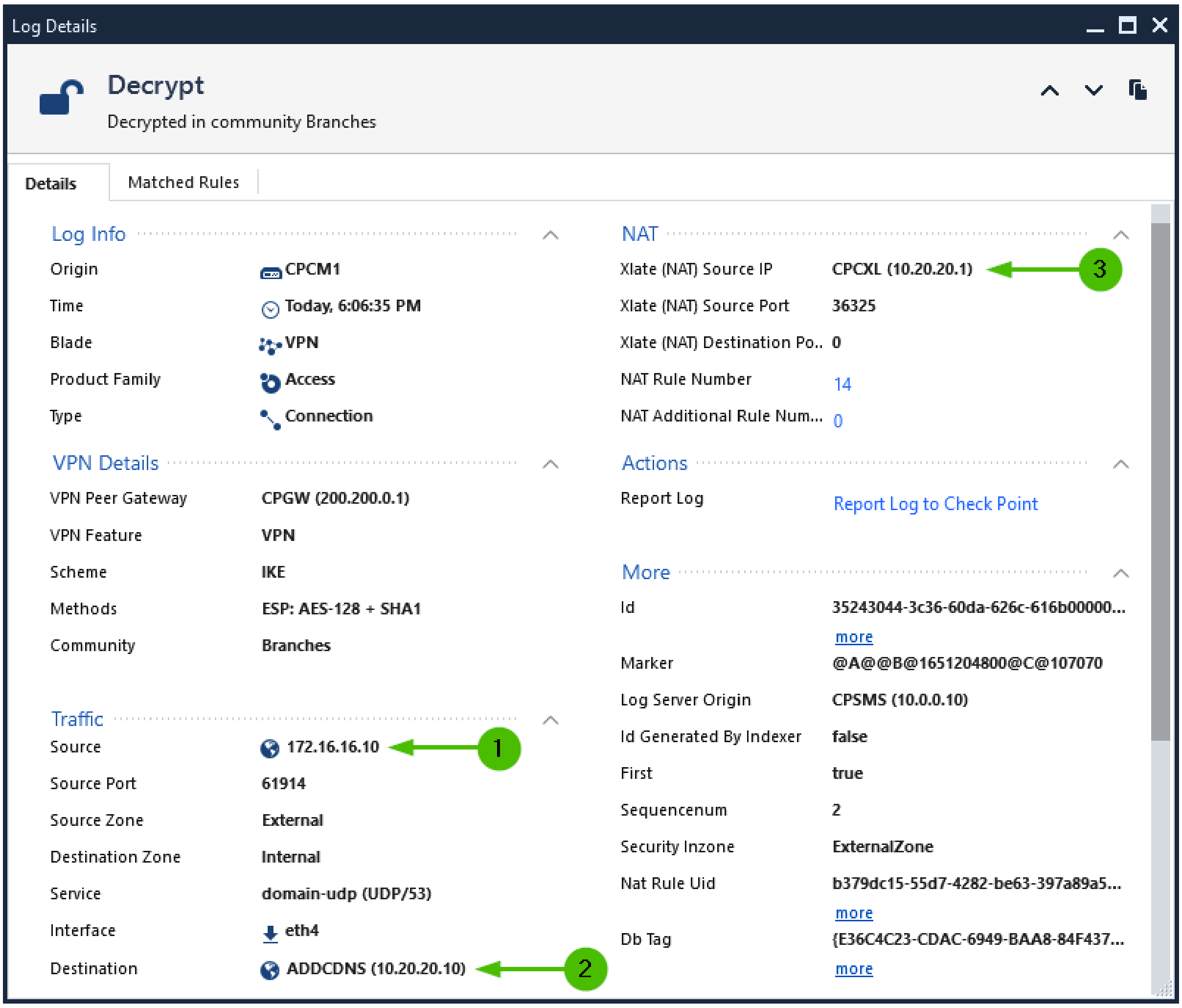
VPN Routing

Enable VPN routing for satellites

○ To center only

○ To center and to other satellites through center

● To center or through the center to other satellites, to Internet and other VPN targets



Log Details

Decrypt

Decrypted in community Branches

Details | Matched Rules

Log Info

Origin	CPCM1
Time	Today, 6:06:35 PM
Blade	VPN
Product Family	Access
Type	Connection

VPN Details

VPN Peer Gateway	CPGW (200.200.0.1)
VPN Feature	VPN
Scheme	IKE
Methods	ESP: AES-128 + SHA1
Community	Branches

Traffic

Source	172.16.16.10 ← 1
Source Port	61914
Source Zone	External
Destination Zone	Internal
Service	domain-udp (UDP/53)
Interface	eth4
Destination	ADDCDNS (10.20.20.10) ← 2

NAT

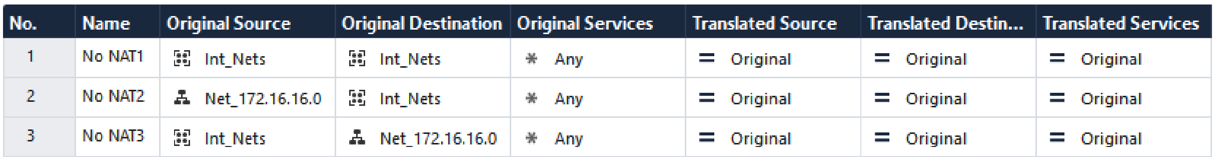
Xlate (NAT) Source IP	CPCXL (10.20.20.1) ← 3
Xlate (NAT) Source Port	36325
Xlate (NAT) Destination Po..	0
NAT Rule Number	14
NAT Additional Rule Num...	0

Actions

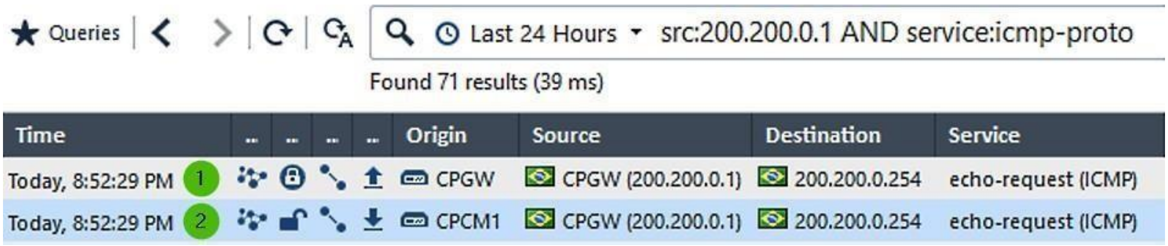
Report Log	Report Log to Check Point

More

Id	35243044-3c36-60da-626c-616b00000... more
Marker	@A@@B@1651204800@C@107070
Log Server Origin	CPSMS (10.0.0.10)
Id Generated By Indexer	false
First	true
Sequencenum	2
Security Inzone	ExternalZone
Nat Rule Uid	b379dc15-55d7-4282-be63-397a89a5... more
Db Tag	{E36C4C23-CDAC-6949-BAA8-84F437... more



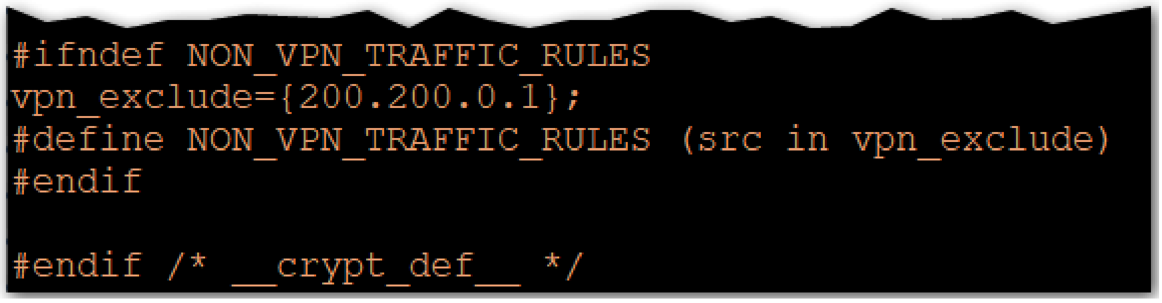
No.	Name	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services
1	No NAT1	Int_Nets	Int_Nets	Any	= Original	= Original	= Original
2	No NAT2	Net_172.16.16.0	Int_Nets	Any	= Original	= Original	= Original
3	No NAT3	Int_Nets	Net_172.16.16.0	Any	= Original	= Original	= Original



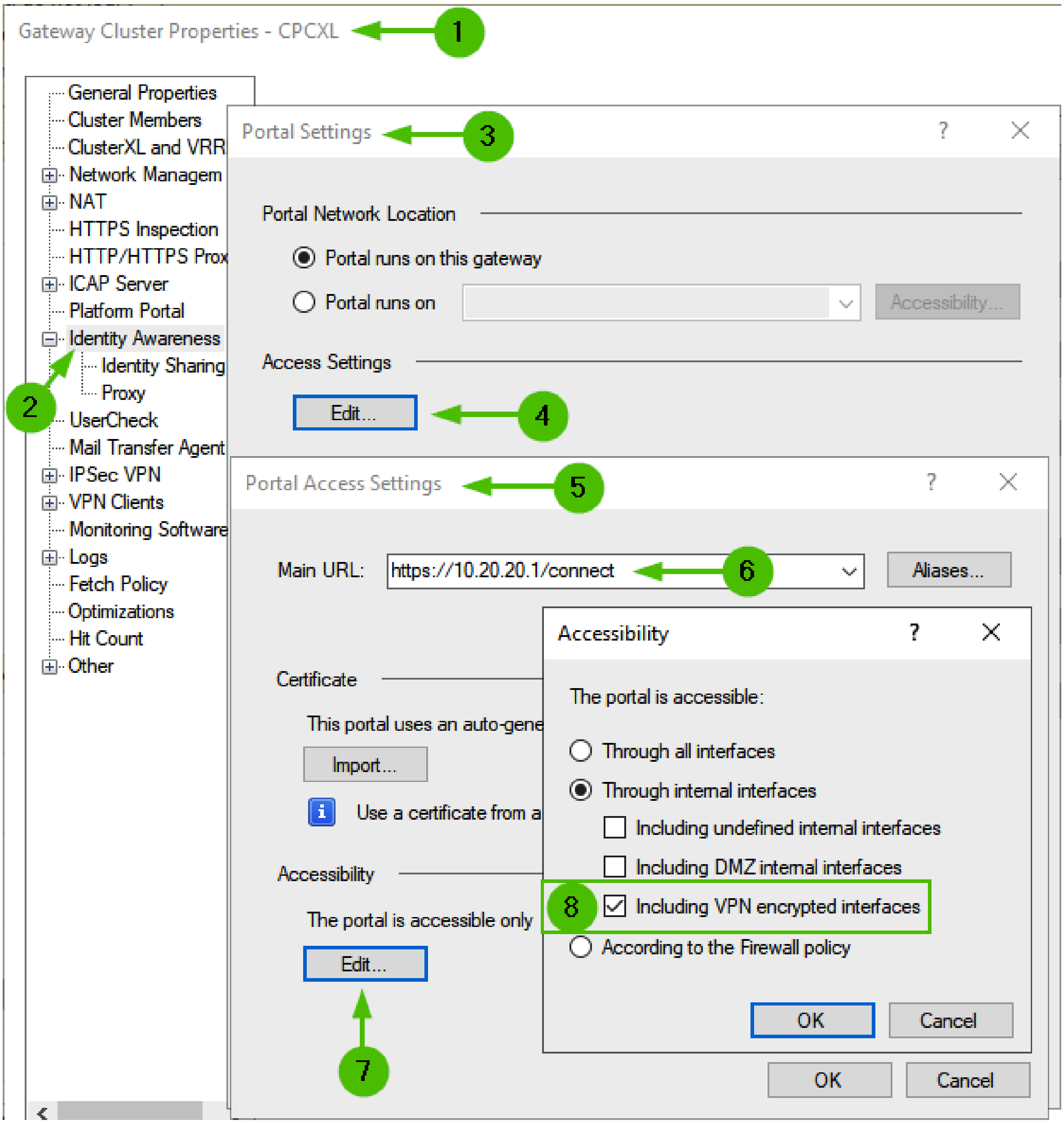
Last 24 Hours ▾ src:200.200.0.1 AND service:icmp-proto

Found 71 results (39 ms)

Time	...	...	...	...	Origin	Source	Destination	Service
Today, 8:52:29 PM 1					CPGW	CPGW (200.200.0.1)	200.200.0.254	echo-request (ICMP)
Today, 8:52:29 PM 2					CPCM1	CPGW (200.200.0.1)	200.200.0.254	echo-request (ICMP)



```
#ifndef NON_VPN_TRAFFIC_RULES
vpn_exclude={200.200.0.1};
#define NON_VPN_TRAFFIC_RULES (src in vpn_exclude)
#endif

#endif /* __crypt_def__ */
```



Gateway Cluster Properties - CPCXL

Portal Settings

Portal Network Location

● Portal runs on this gateway

○ Portal runs on

Access Settings

Portal Access Settings

Main URL: https://10.20.20.1/connect

Certificate

This portal uses an auto-gene

Use a certificate from a

Accessibility

The portal is accessible only

Accessibility

The portal is accessible:

○ Through all interfaces

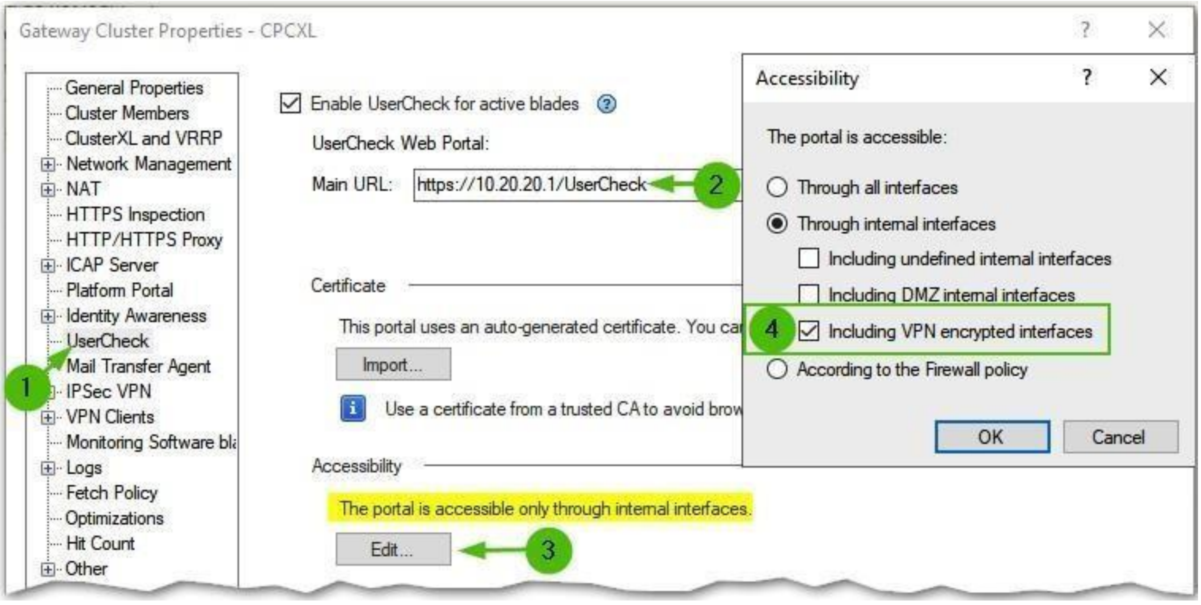
● Through internal interfaces

□ Including undefined internal interfaces

□ Including DMZ internal interfaces

☑ Including VPN encrypted interfaces

○ According to the Firewall policy



Gateway Cluster Properties - CPCXL

☑ Enable UserCheck for active blades

UserCheck Web Portal:

Main URL: https://10.20.20.1/UserCheck

Certificate

This portal uses an auto-generated certificate. You ca

Use a certificate from a trusted CA to avoid brow

Accessibility

The portal is accessible only through internal interfaces.

Accessibility

The portal is accessible:

○ Through all interfaces

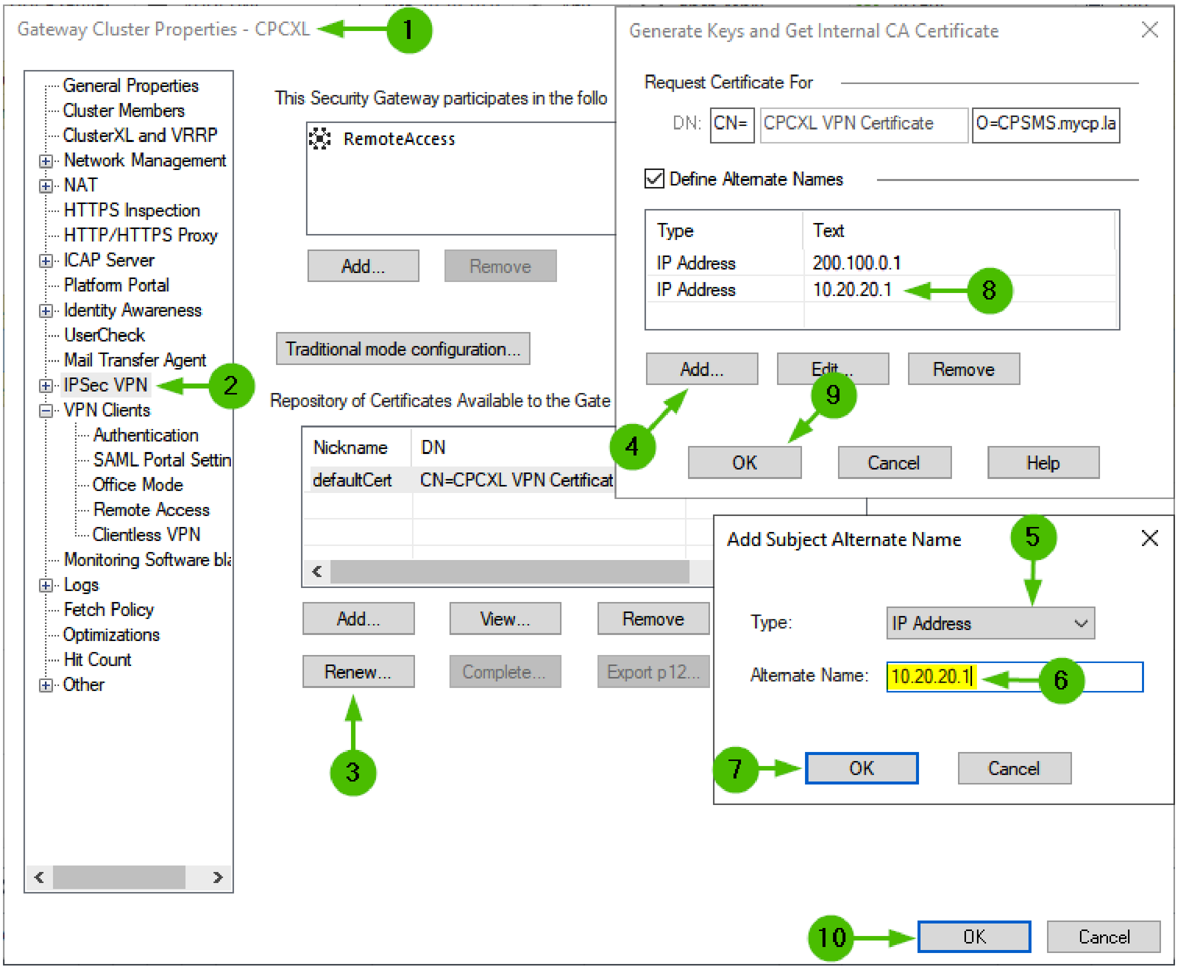
● Through internal interfaces

□ Including undefined internal interfaces

□ Including DMZ internal interfaces

☑ Including VPN encrypted interfaces

○ According to the Firewall policy



Gateway Cluster Properties - CPCXL

This Security Gateway participates in the follo

RemoteAccess

Repository of Certificates Available to the Gate

Nickname	DN
defaultCert	CN=CPCXL VPN Certificat

Generate Keys and Get Internal CA Certificate

Request Certificate For

DN: CN= CPCXL VPN Certificate O=CPSMS.mycp.la

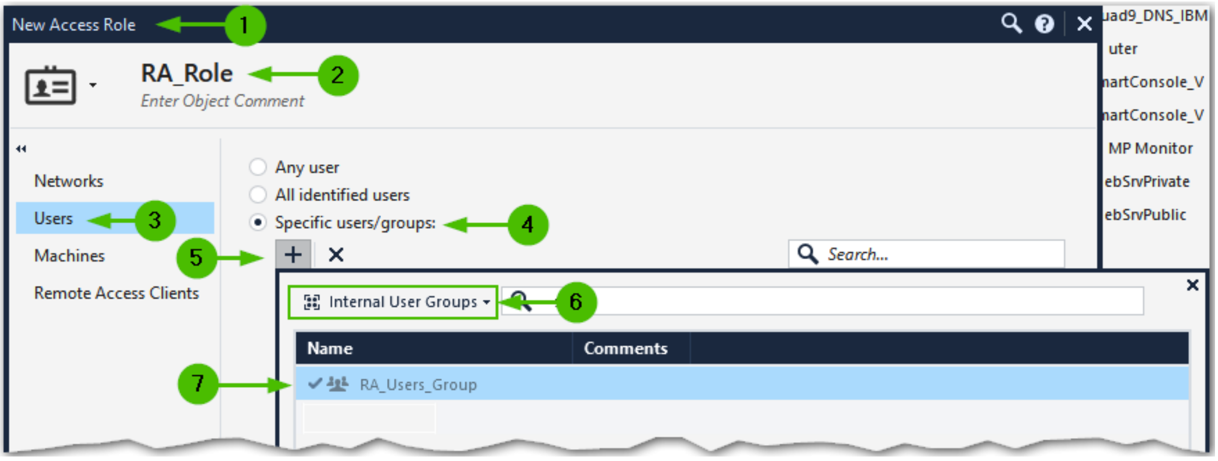
☑ Define Alternate Names

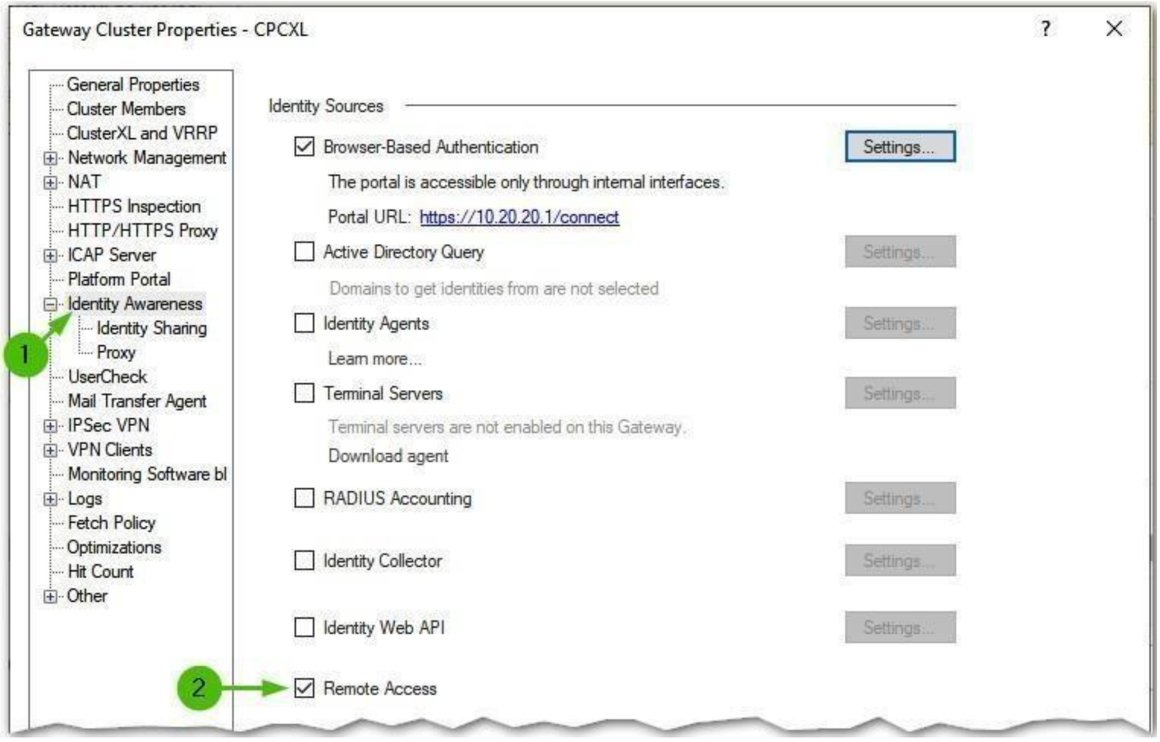
Type	Text
IP Address	200.100.0.1
IP Address	10.20.20.1

Add Subject Alternate Name

Type: IP Address

Alternate Name: 10.20.20.1



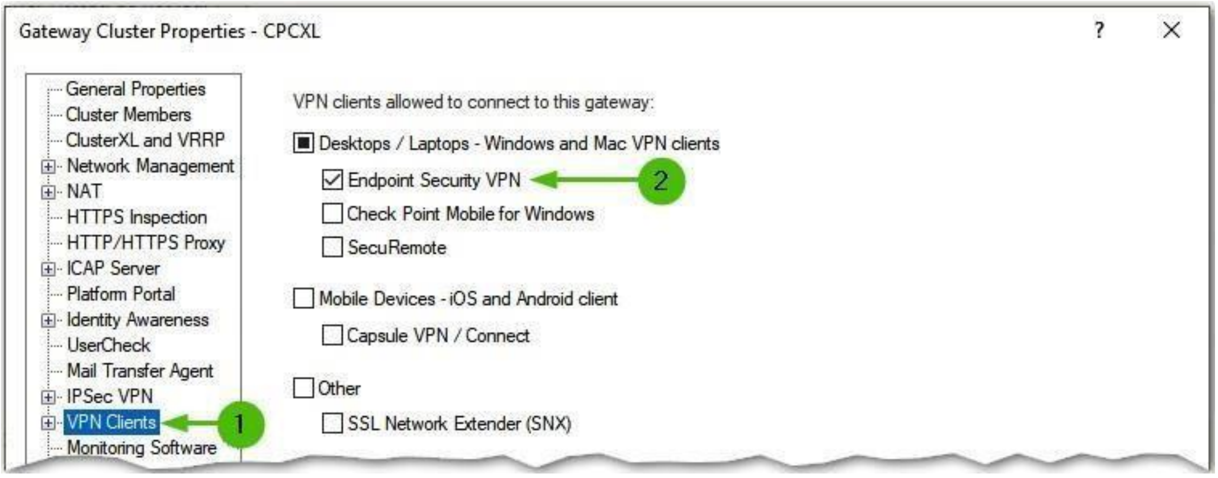


The portal is accessible only through internal interfaces.

Portal URL: https://10.20.20.1/connect

Domains to get identities from are not selected

Terminal servers are not enabled on this Gateway.



Gateway Cluster Properties - CPCXL

VPN clients allowed to connect to this gateway:

■ Desktops / Laptops - Windows and Mac VPN clients

☑ Endpoint Security VPN

□ Check Point Mobile for Windows

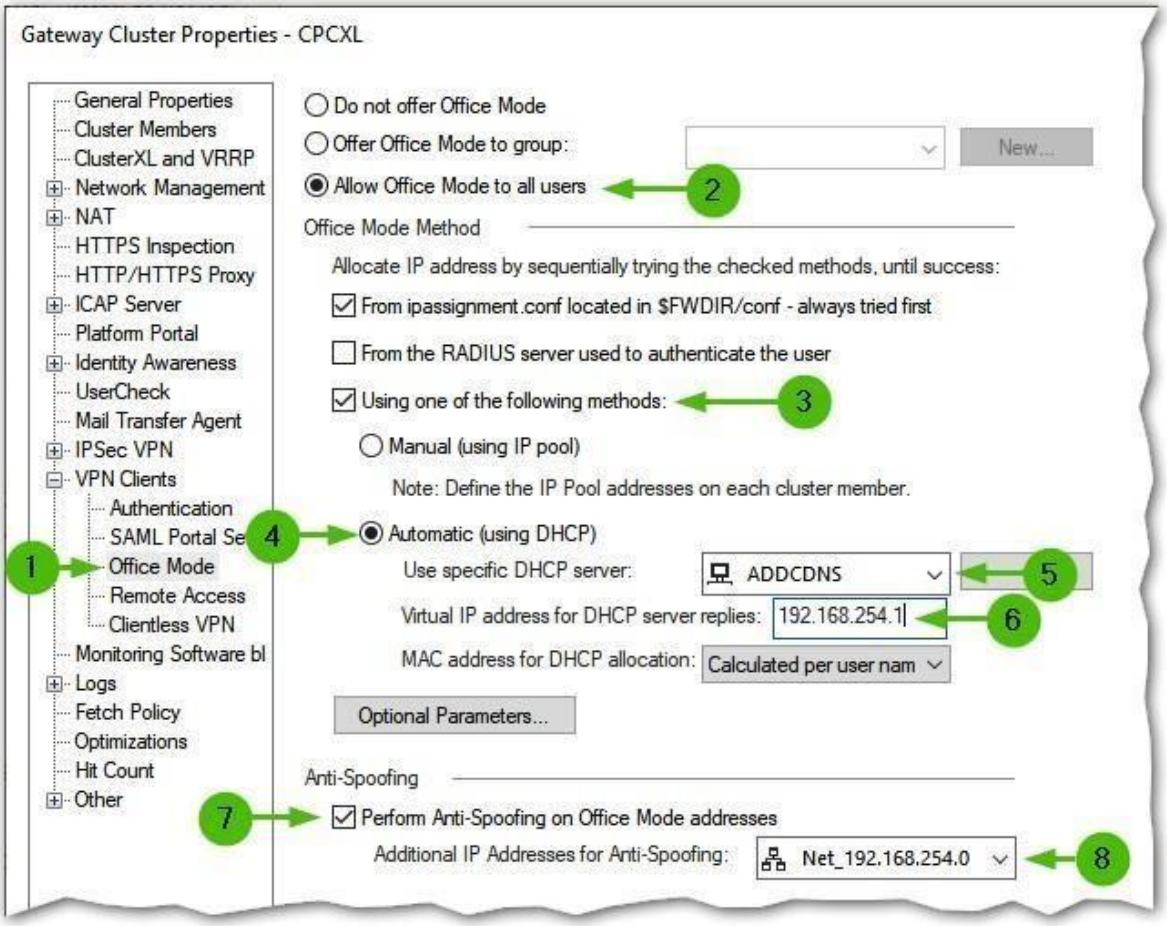
□ SecuRemote

□ Mobile Devices - iOS and Android client

□ Capsule VPN / Connect

□ Other

□ SSL Network Extender (SNX)



Gateway Cluster Properties - CPCXL

○ Do not offer Office Mode

○ Offer Office Mode to group:

● Allow Office Mode to all users

Office Mode Method

Allocate IP address by sequentially trying the checked methods, until success:

☑ From ipassignment.conf located in $FWDIR/conf - always tried first

□ From the RADIUS server used to authenticate the user

☑ Using one of the following methods:

○ Manual (using IP pool)

Note: Define the IP Pool addresses on each cluster member.

● Automatic (using DHCP)

Use specific DHCP server: ADDCDNS

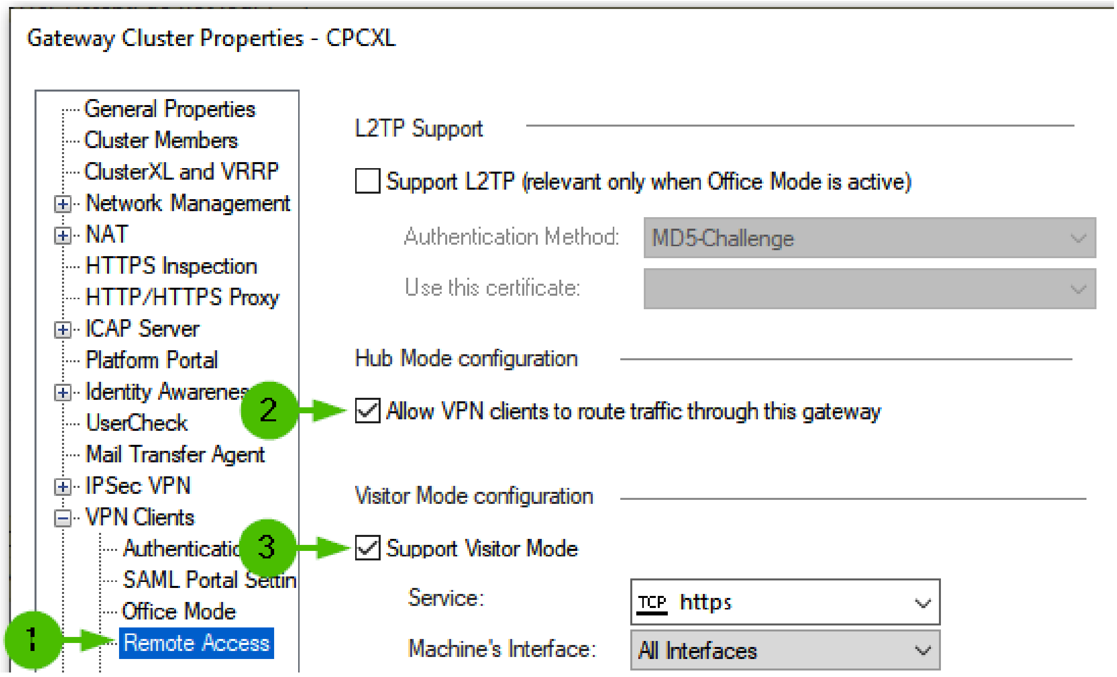
Virtual IP address for DHCP server replies: 192.168.254.1

MAC address for DHCP allocation: Calculated per user nam

Anti-Spoofing

☑ Perform Anti-Spoofing on Office Mode addresses

Additional IP Addresses for Anti-Spoofing: Net_192.168.254.0



Gateway Cluster Properties - CPCXL

L2TP Support

□ Support L2TP (relevant only when Office Mode is active)

Authentication Method: MD5-Challenge

Use this certificate:

Hub Mode configuration

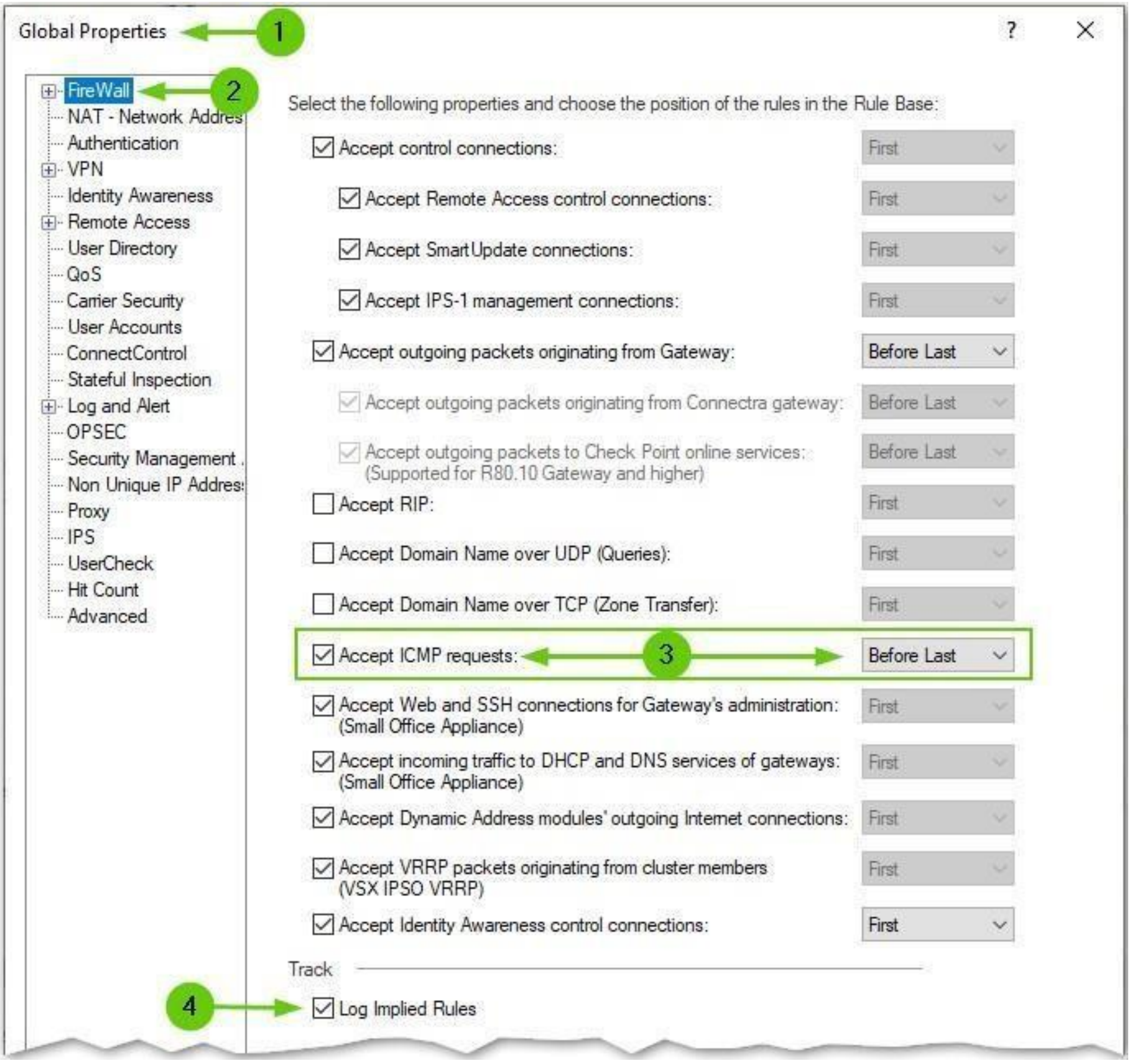
☑ Allow VPN clients to route traffic through this gateway

Visitor Mode configuration

☑ Support Visitor Mode

Service: TCP https

Machine's Interface: All Interfaces

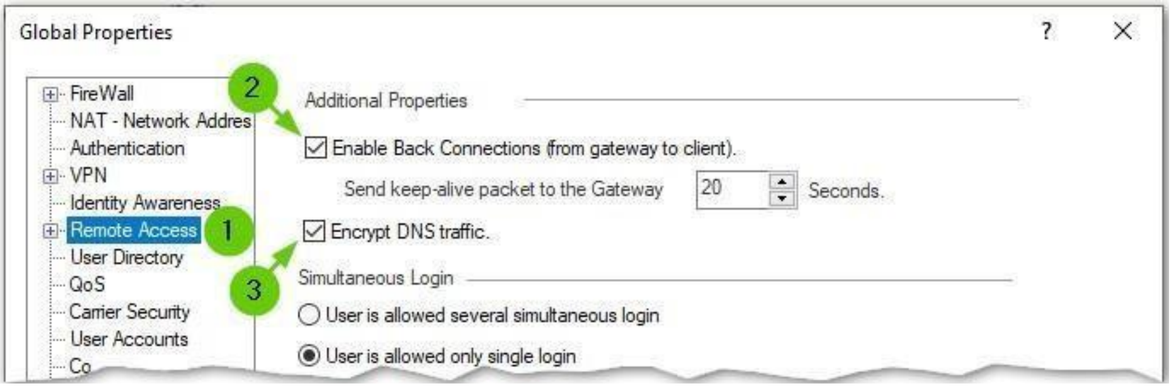


Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept control connections:	First
☑ Accept Remote Access control connections:	First
☑ Accept SmartUpdate connections:	First
☑ Accept IPS-1 management connections:	First
☑ Accept outgoing packets originating from Gateway:	Before Last
☑ Accept outgoing packets originating from Connectra gateway:	Before Last
☑ Accept outgoing packets to Check Point online services: (Supported for R80.10 Gateway and higher)	Before Last
□ Accept RIP:	First
□ Accept Domain Name over UDP (Queries):	First
□ Accept Domain Name over TCP (Zone Transfer):	First
☑ Accept ICMP requests:	Before Last
☑ Accept Web and SSH connections for Gateway's administration: (Small Office Appliance)	First
☑ Accept incoming traffic to DHCP and DNS services of gateways: (Small Office Appliance)	First
☑ Accept Dynamic Address modules' outgoing Internet connections:	First
☑ Accept VRRP packets originating from cluster members (VSX IPSO VRRP)	First
☑ Accept Identity Awareness control connections:	First

Track

☑ Log Implied Rules



Additional Properties

☑ Enable Back Connections (from gateway to client).

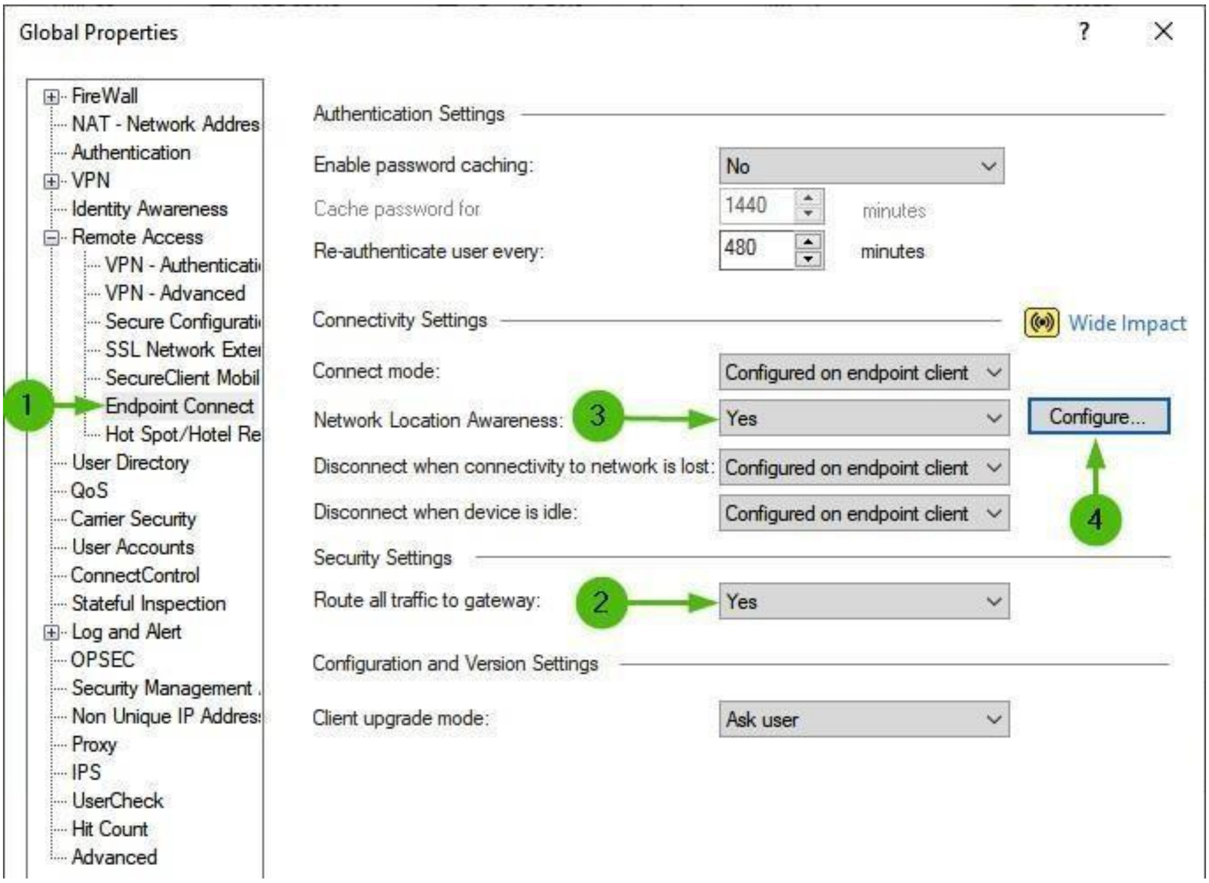
Send keep-alive packet to the Gateway 20 Seconds.

☑ Encrypt DNS traffic.

Simultaneous Login

○ User is allowed several simultaneous login

● User is allowed only single login



Global Properties

Authentication Settings

Enable password caching: No

Cache password for 1440 minutes

Re-authenticate user every: 480 minutes

Connectivity Settings

Connect mode: Configured on endpoint client

Network Location Awareness: Yes

Disconnect when connectivity to network is lost: Configured on endpoint client

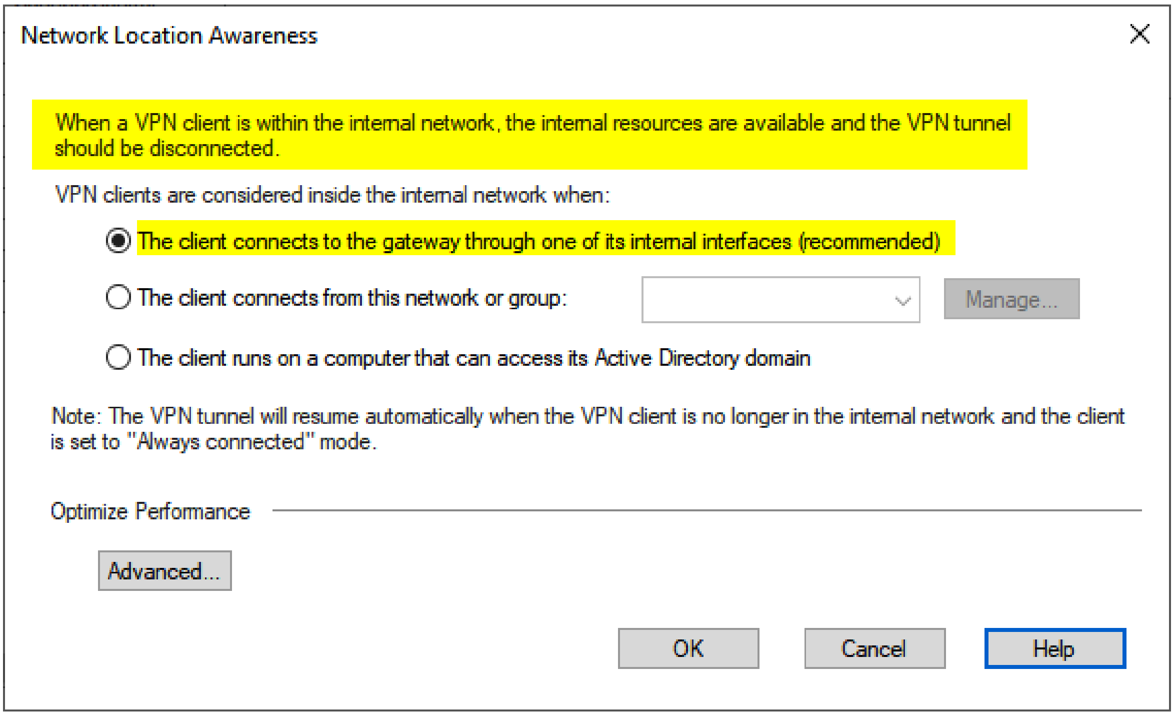
Disconnect when device is idle: Configured on endpoint client

Security Settings

Route all traffic to gateway: Yes

Configuration and Version Settings

Client upgrade mode: Ask user



Network Location Awareness

When a VPN client is within the internal network, the internal resources are available and the VPN tunnel should be disconnected.

VPN clients are considered inside the internal network when:

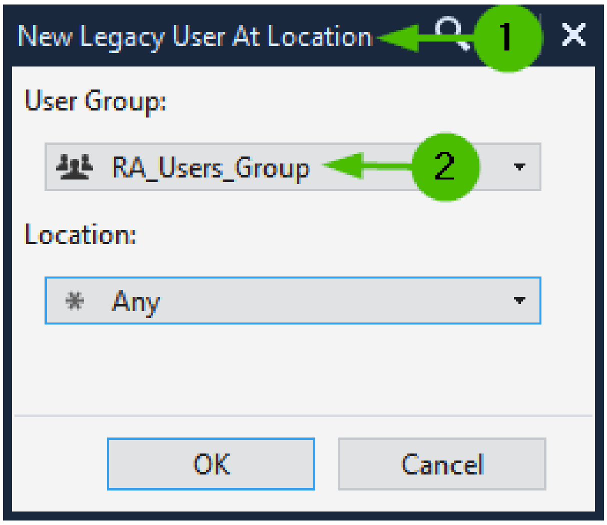
● The client connects to the gateway through one of its internal interfaces (recommended)

○ The client connects from this network or group:

○ The client runs on a computer that can access its Active Directory domain

Note: The VPN tunnel will resume automatically when the VPN client is no longer in the internal network and the client is set to "Always connected" mode.

Optimize Performance

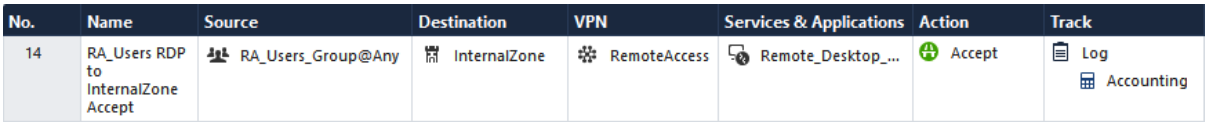


New Legacy User At Location

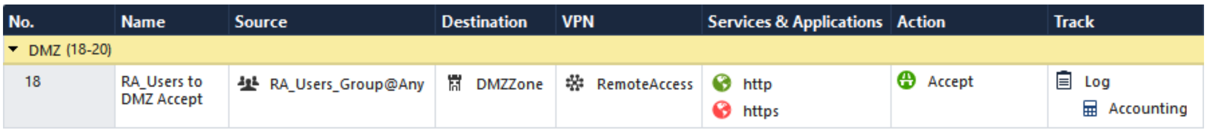
User Group: RA_Users_Group

Location: Any

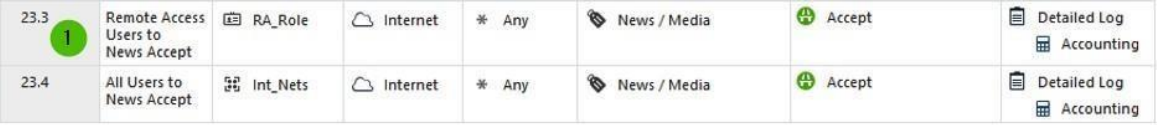
OK | Cancel



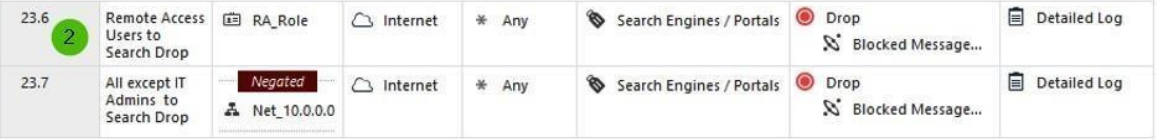
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
14	RA_Users RDP to InternalZone Accept	RA_Users_Group@Any	InternalZone	RemoteAccess	Remote_Desktop_...	Accept	Log Accounting



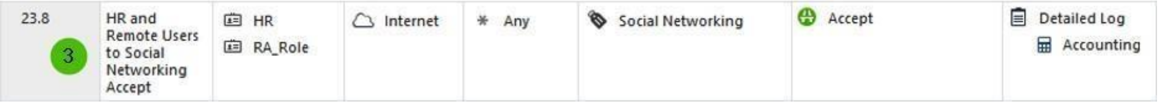
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
DMZ (18-20)							
18	RA_Users to DMZ Accept	RA_Users_Group@Any	DMZZone	RemoteAccess	http https	Accept	Log Accounting



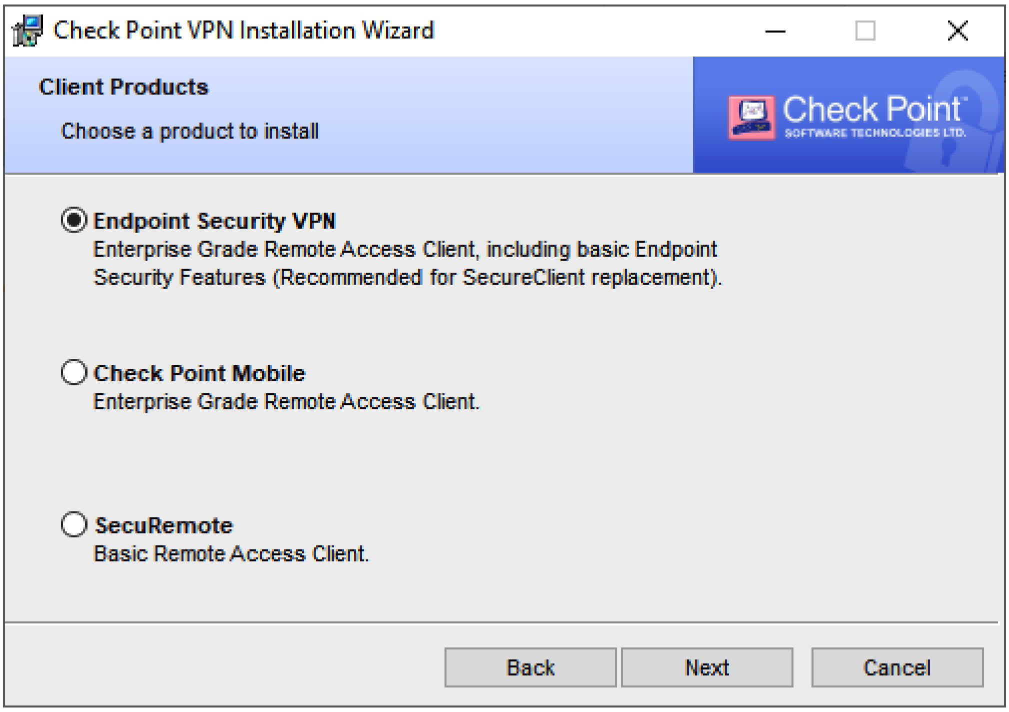
23.3 1	Remote Access Users to News Accept	RA_Role	Internet	Any	News / Media	Accept	Detailed Log Accounting
23.4	All Users to News Accept	Int_Nets	Internet	Any	News / Media	Accept	Detailed Log Accounting



23.6 2	Remote Access Users to Search Drop	RA_Role	Internet	Any	Search Engines / Portals	Drop Blocked Message...	Detailed Log
23.7	All except IT Admins to Search Drop	Negated Net_10.0.0.0	Internet	Any	Search Engines / Portals	Drop Blocked Message...	Detailed Log



23.8 3	HR and Remote Users to Social Networking Accept	HR RA_Role	Internet	Any	Social Networking	Accept	Detailed Log Accounting



Check Point VPN Installation Wizard

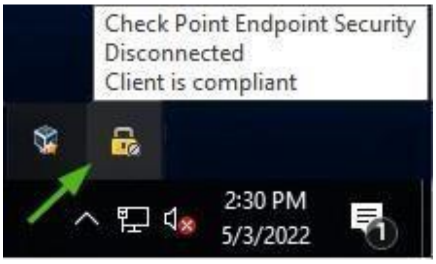
Client Products

Choose a product to install

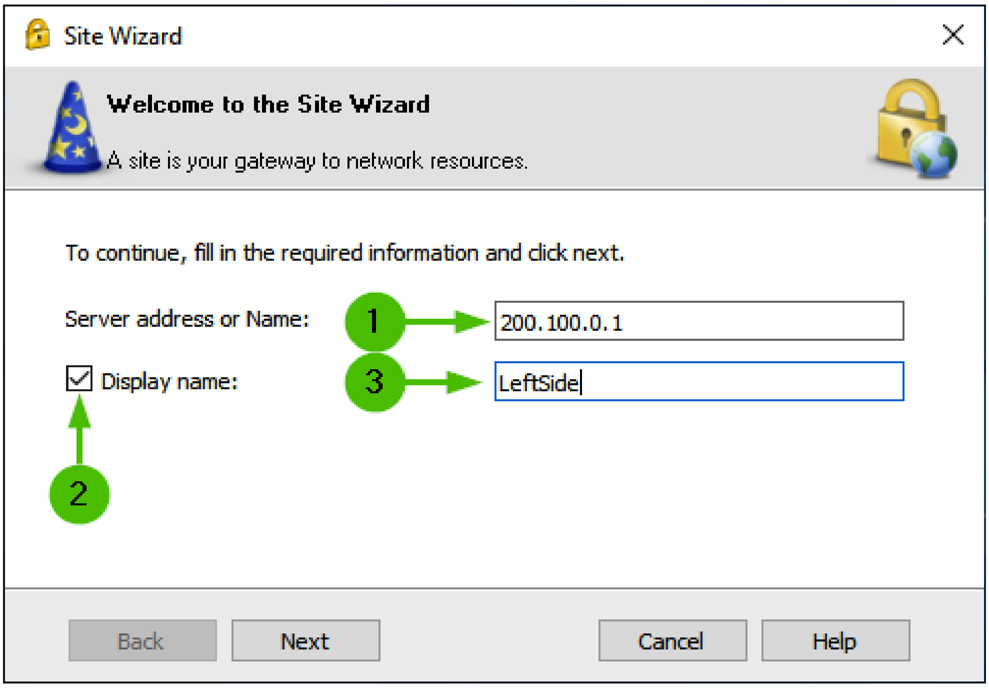
● **Endpoint Security VPN**
Enterprise Grade Remote Access Client, including basic Endpoint Security Features (Recommended for SecureClient replacement).

○ **Check Point Mobile**
Enterprise Grade Remote Access Client.

○ **SecuRemote**
Basic Remote Access Client.



Check Point Endpoint Security
Disconnected
Client is compliant



Site Wizard

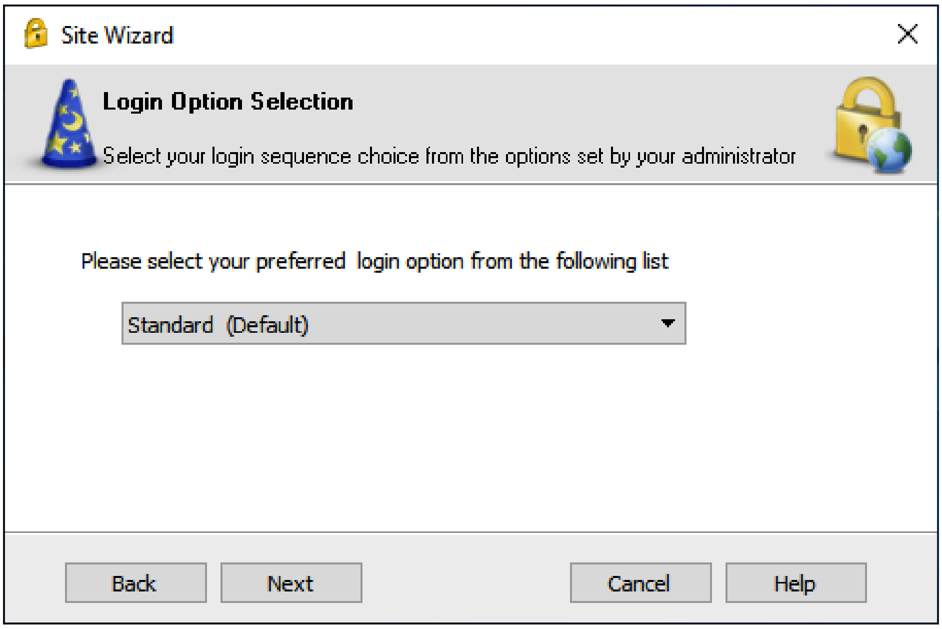
Welcome to the Site Wizard

A site is your gateway to network resources.

To continue, fill in the required information and click next.

Server address or Name: 200.100.0.1

☑ Display name: LeftSide



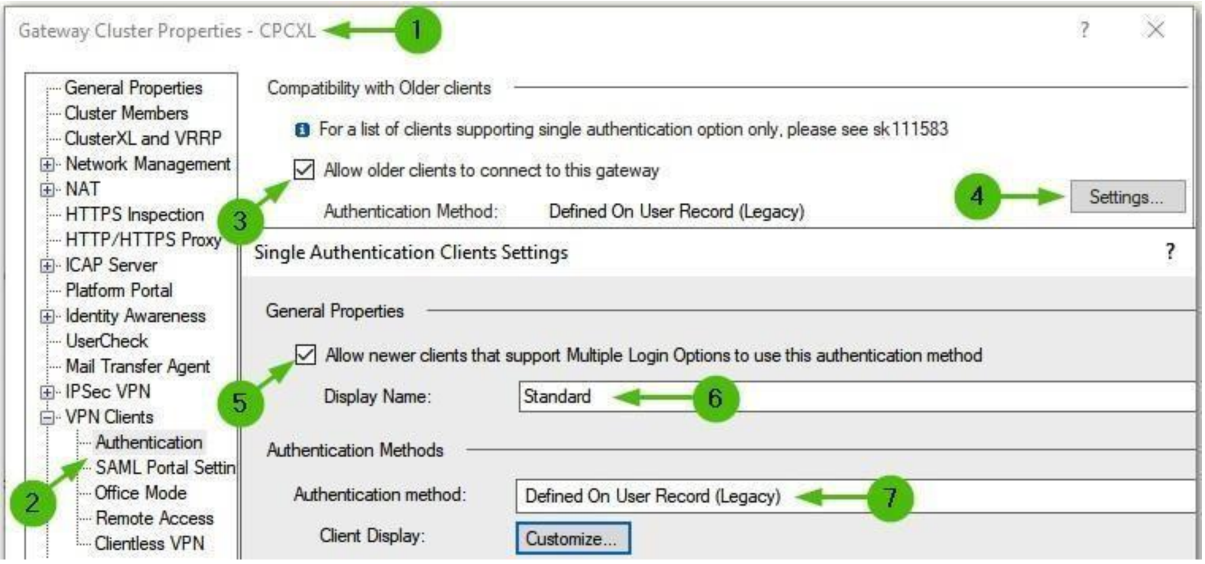
Site Wizard

Login Option Selection

Select your login sequence choice from the options set by your administrator

Please select your preferred login option from the following list

Standard (Default)



Gateway Cluster Properties - CPCXL

- General Properties
- Cluster Members
- ClusterXL and VRRP
- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- ICAP Server
- Platform Portal
- Identity Awareness
- UserCheck
- Mail Transfer Agent
- IPSec VPN
- VPN Clients
  - Authentication
  - SAML Portal Settin
  - Office Mode
  - Remote Access
  - Clientless VPN

Compatibility with Older clients

For a list of clients supporting single authentication option only, please see sk111583

☑ Allow older clients to connect to this gateway

Authentication Method: Defined On User Record (Legacy)

Settings...

Single Authentication Clients Settings

General Properties

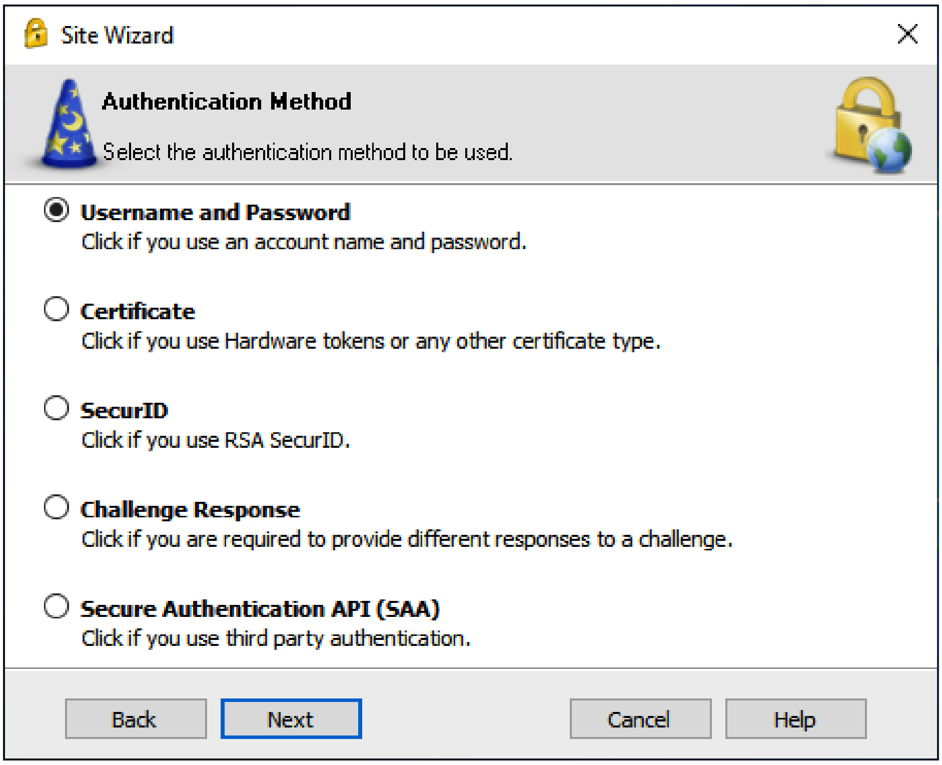
☑ Allow newer clients that support Multiple Login Options to use this authentication method

Display Name: Standard

Authentication Methods

Authentication method: Defined On User Record (Legacy)

Client Display: Customize...



Site Wizard

Authentication Method

Select the authentication method to be used.

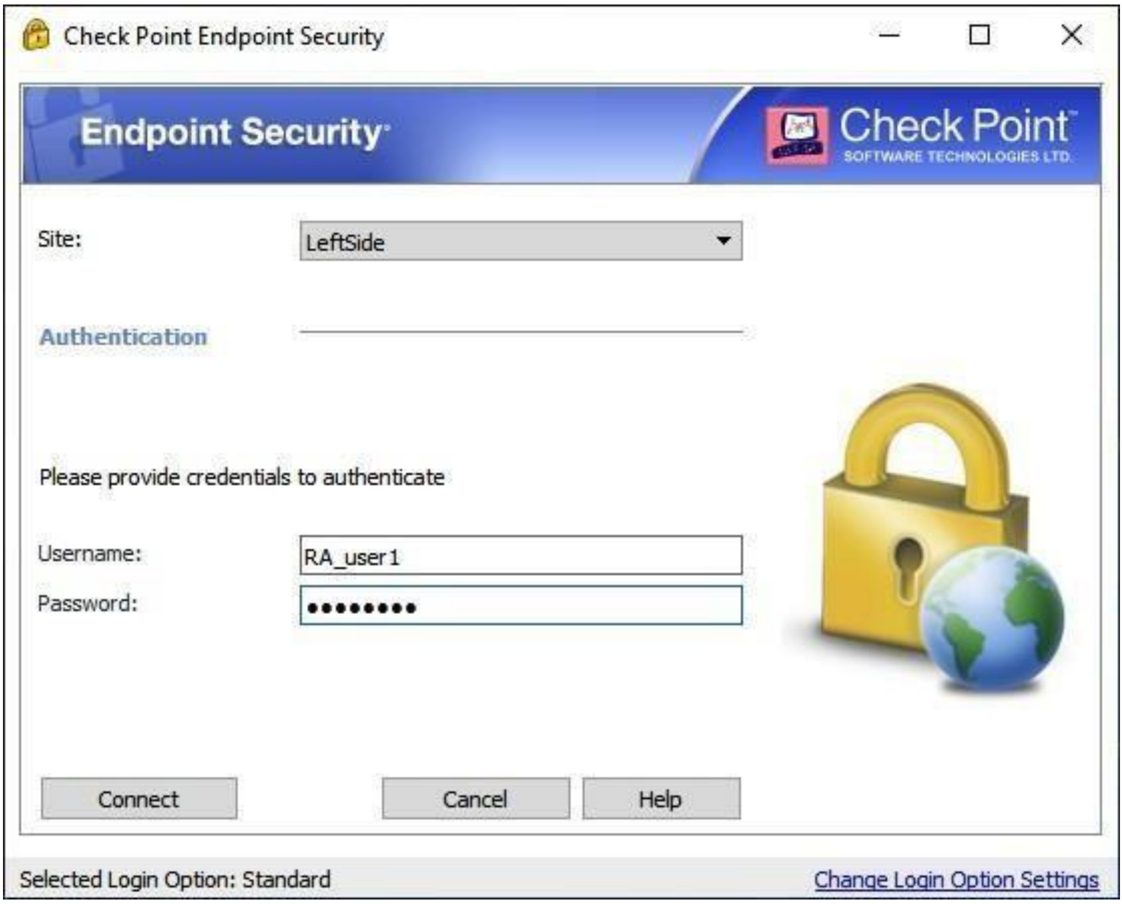
● **Username and Password**
Click if you use an account name and password.

○ **Certificate**
Click if you use Hardware tokens or any other certificate type.

○ **SecurID**
Click if you use RSA SecurID.

○ **Challenge Response**
Click if you are required to provide different responses to a challenge.

○ **Secure Authentication API (SAA)**
Click if you use third party authentication.



Check Point Endpoint Security

Site: LeftSide

Authentication

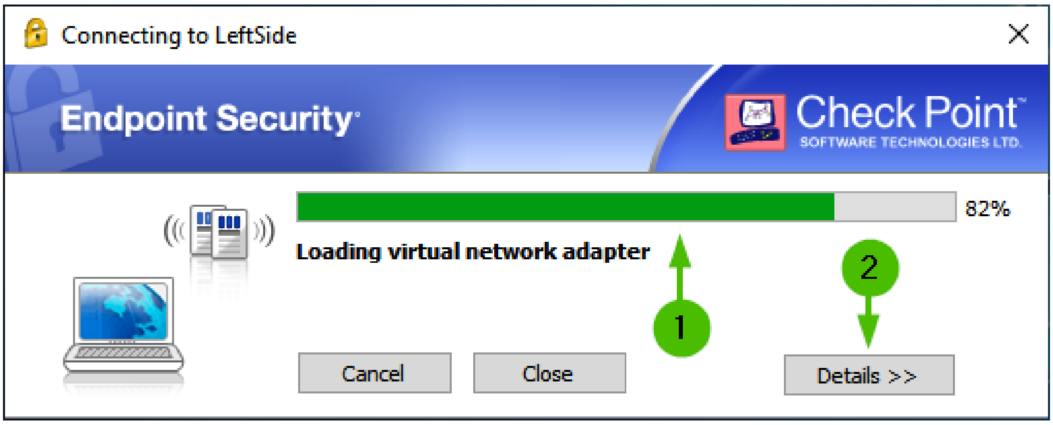
Please provide credentials to authenticate

Username: RA_user1

Password: ●●●●●●●●●

Selected Login Option: Standard

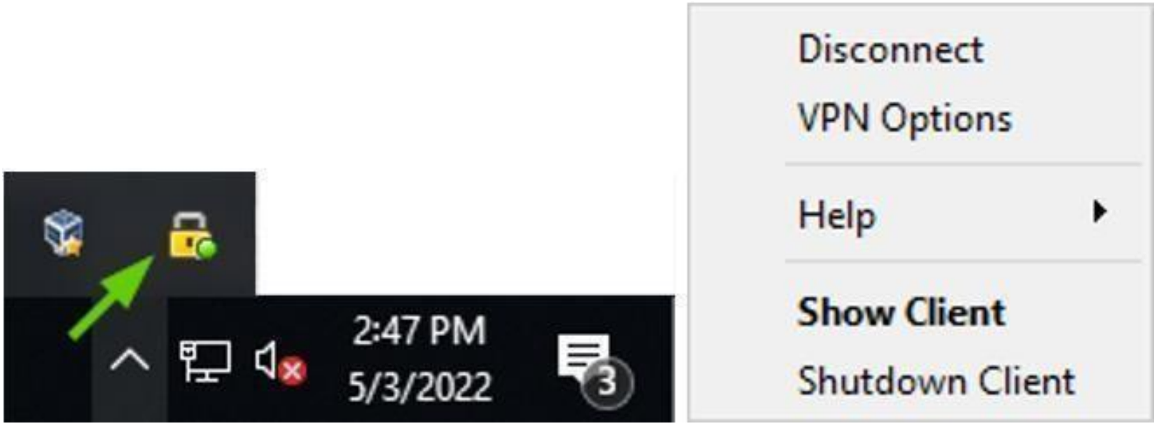
Change Login Option Settings

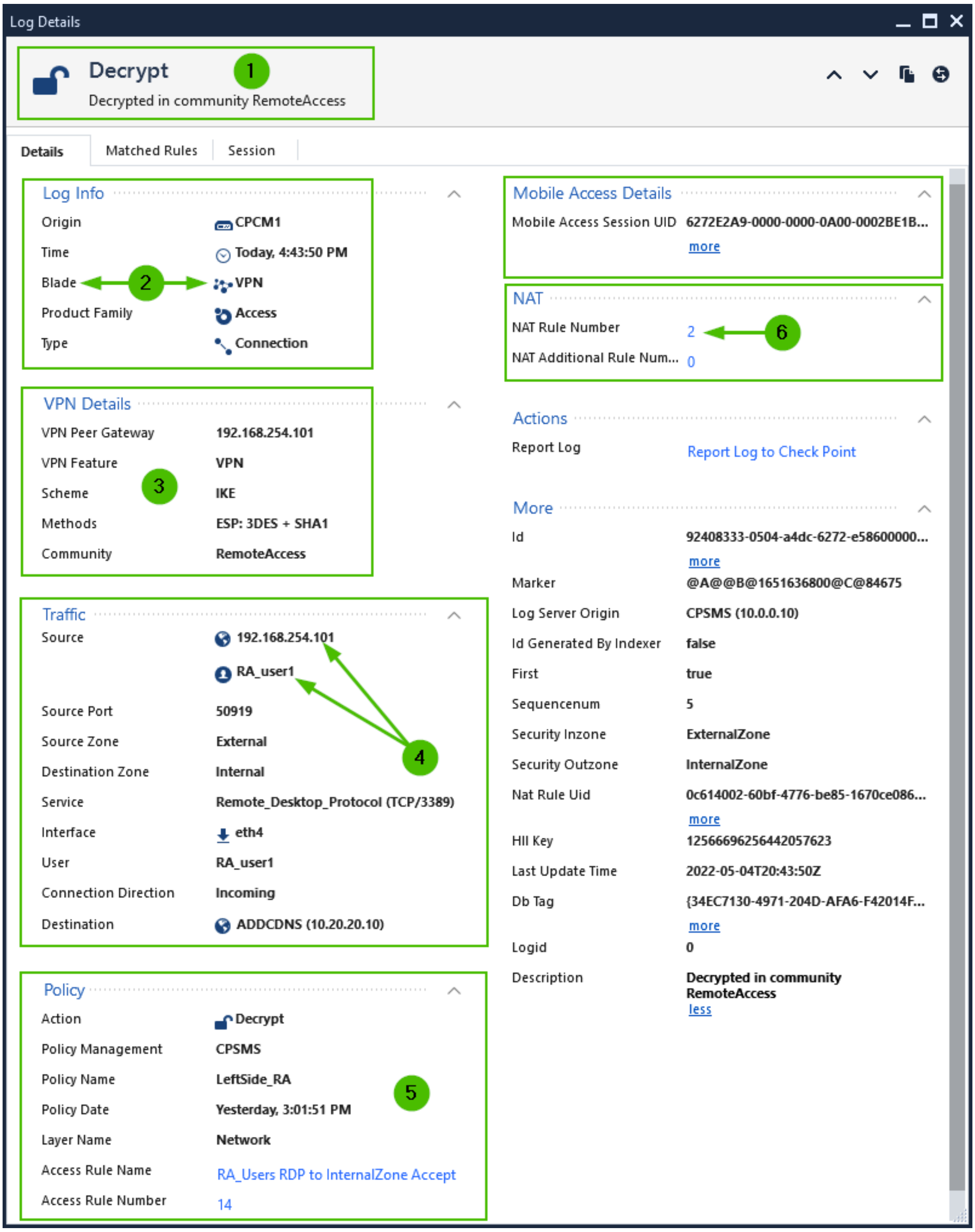


Connecting to LeftSide

82%

Loading virtual network adapter


2:47 PM
5/3/2022
3
Disconnect
VPN Options
Help
Show Client
Shutdown Client



Decrypt

Decrypted in community RemoteAccess

Log Info

Origin	CPCM1
Time	Today, 4:43:50 PM
Blade	VPN
Product Family	Access
Type	Connection

VPN Details

VPN Peer Gateway	192.168.254.101
VPN Feature	VPN
Scheme	IKE
Methods	ESP: 3DES + SHA1
Community	RemoteAccess

Traffic

Source	192.168.254.101 RA_user1
Source Port	50919
Source Zone	External
Destination Zone	Internal
Service	Remote_Desktop_Protocol (TCP/3389)
Interface	eth4
User	RA_user1
Connection Direction	Incoming
Destination	ADDCDNS (10.20.20.10)

Policy

Action	Decrypt
Policy Management	CPSMS
Policy Name	LeftSide_RA
Policy Date	Yesterday, 3:01:51 PM
Layer Name	Network
Access Rule Name	RA_Users RDP to InternalZone Accept
Access Rule Number	14

Mobile Access Details

Mobile Access Session UID	6272E2A9-0000-0000-0A00-0002BE1B... more

NAT

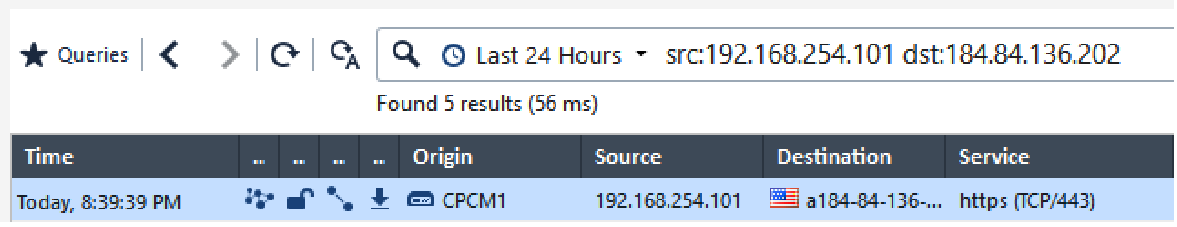
NAT Rule Number	2
NAT Additional Rule Num...	0

Actions

Report Log	Report Log to Check Point

More

Id	92408333-0504-a4dc-6272-e58600000... more
Marker	@A@@B@1651636800@C@84675
Log Server Origin	CPSMS (10.0.0.10)
Id Generated By Indexer	false
First	true
Sequencenum	5
Security Inzone	ExternalZone
Security Outzone	InternalZone
Nat Rule Uid	0c614002-60bf-4776-be85-1670ce086... more
Hll Key	12566696256442057623
Last Update Time	2022-05-04T20:43:50Z
Db Tag	{34EC7130-4971-204D-AFA6-F42014F... more
Logid	0
Description	Decrypted in community RemoteAccess less

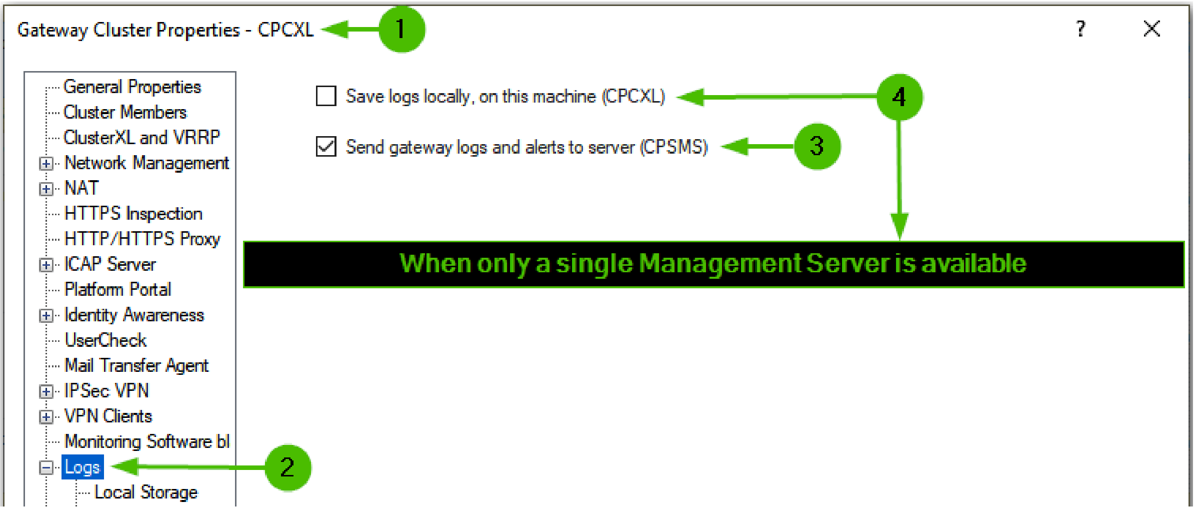


src:192.168.254.101 dst:184.84.136.202

Found 5 results (56 ms)

Time	...	...	...	...	Origin	Source	Destination	Service
Today, 8:39:39 PM					CPCM1	192.168.254.101	a184-84-136-...	https (TCP/443)

Chapter 13: Introduction to Logging and SmartEvent

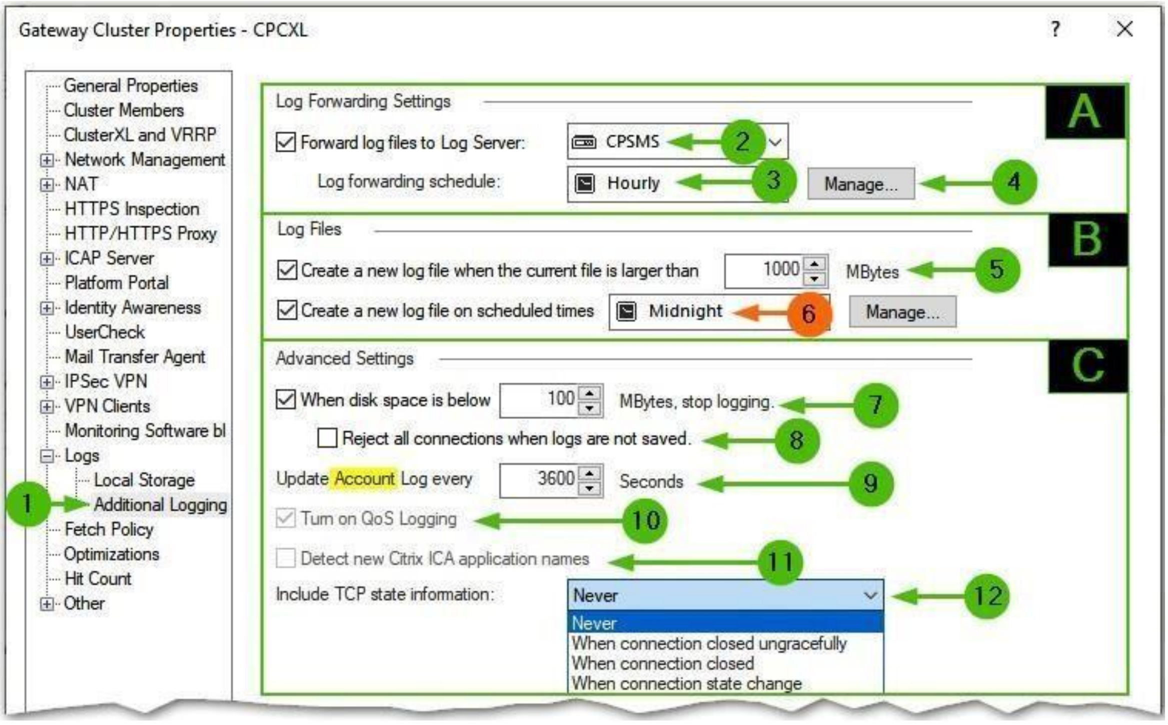


Gateway Cluster Properties - CPCXL

☐ Save logs locally, on this machine (CPCXL)

☑ Send gateway logs and alerts to server (CPSMS)

When only a single Management Server is available



Gateway Cluster Properties - CPCXL

Log Forwarding Settings

☑ Forward log files to Log Server: CPSMS

Log forwarding schedule: Hourly [Manage...]

Log Files

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

☑ Create a new log file on scheduled times Midnight [Manage...]

Advanced Settings

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

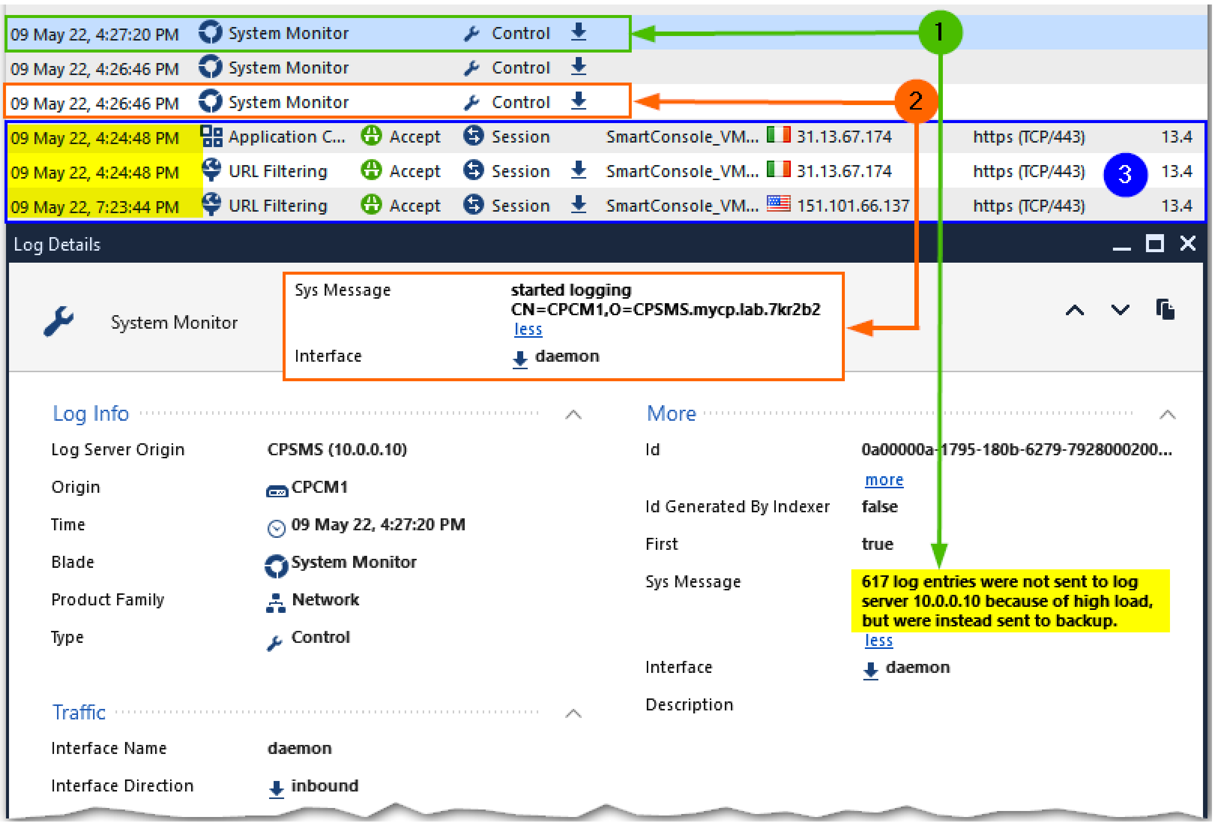
☐ Reject all connections when logs are not saved.

Update Account Log every 3600 Seconds

☑ Turn on QoS Logging

☐ Detect new Citrix ICA application names

Include TCP state information: Never



```
09 May 22, 4:27:20 PM  System Monitor                     Control
09 May 22, 4:26:46 PM  System Monitor                     Control
09 May 22, 4:26:46 PM  System Monitor                     Control
09 May 22, 4:24:48 PM  Application C...  Accept  Session  SmartConsole_VM...  31.13.67.174   https (TCP/443)  13.4
09 May 22, 4:24:48 PM  URL Filtering     Accept  Session  SmartConsole_VM...  31.13.67.174   https (TCP/443)  13.4
09 May 22, 7:23:44 PM  URL Filtering     Accept  Session  SmartConsole_VM...  151.101.66.137 https (TCP/443)  13.4
```

Log Details

System Monitor

Sys Message: started logging CN=CPCM1,O=CPSMS.mycp.lab.7kr2b2 less

Interface: daemon

Log Info

Log Server Origin: CPSMS (10.0.0.10)

Origin: CPCM1

Time: 09 May 22, 4:27:20 PM

Blade: System Monitor

Product Family: Network

Type: Control

Traffic

Interface Name: daemon

Interface Direction: inbound

More

Id: 0a00000a-1795-180b-6279-7928000200... more

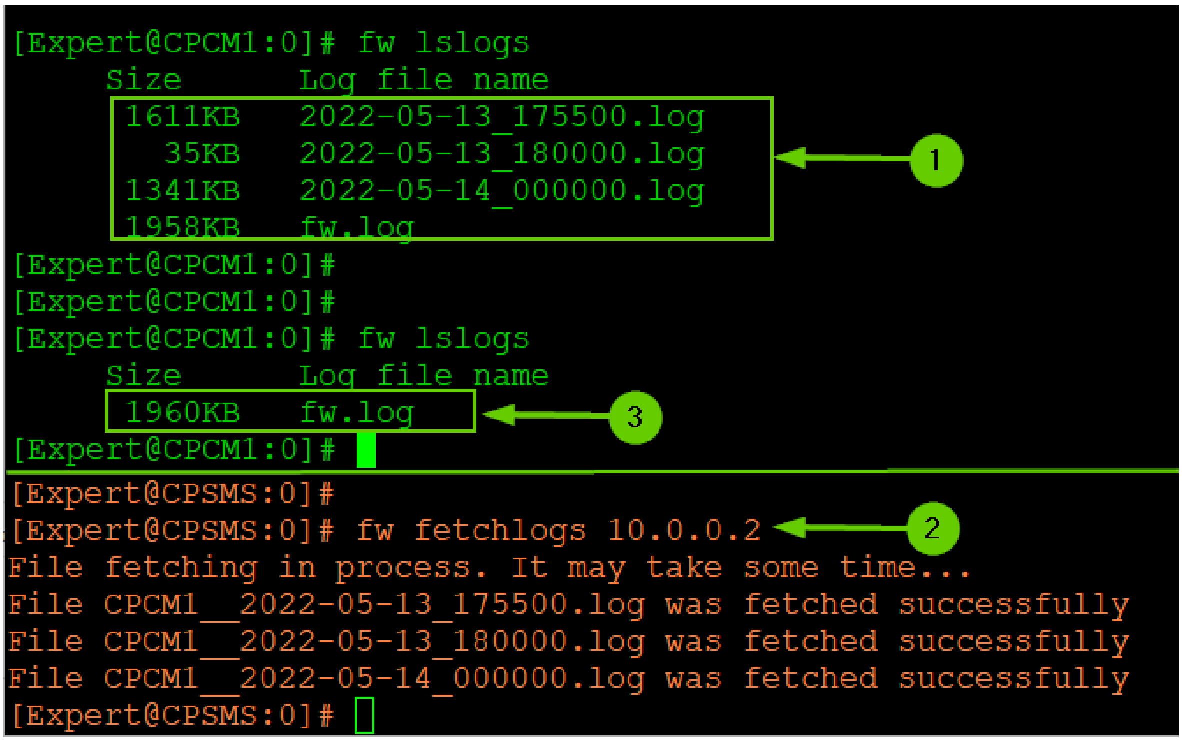
Id Generated By Indexer: false

First: true

Sys Message: 617 log entries were not sent to log server 10.0.0.10 because of high load, but were instead sent to backup. less

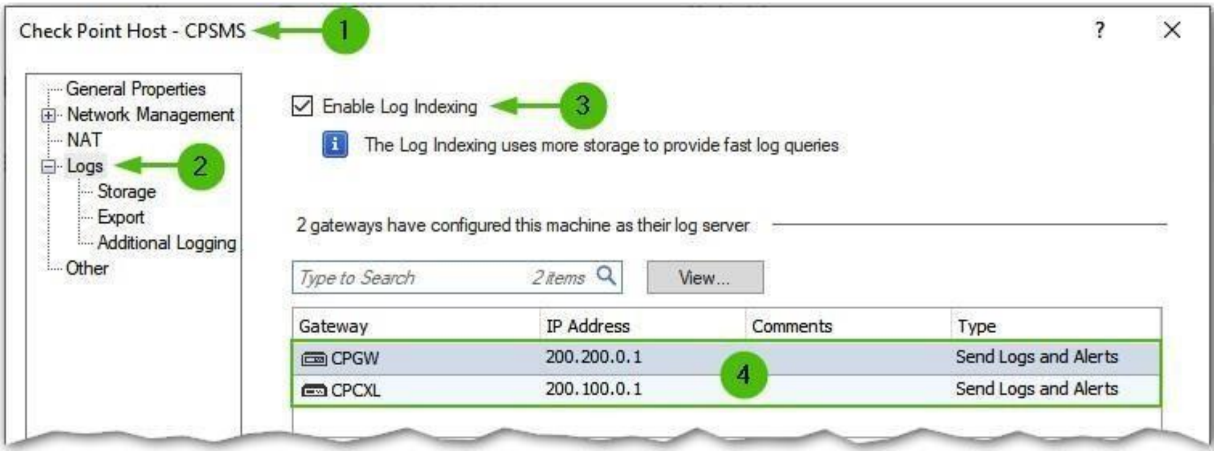
Interface: daemon

Description:



```
[Expert@CPCM1:0]# fw lslogs
     Size      Log file name
     1611KB    2022-05-13_175500.log
       35KB    2022-05-13_180000.log
     1341KB    2022-05-14_000000.log
     1958KB    fw.log
[Expert@CPCM1:0]#
[Expert@CPCM1:0]#
[Expert@CPCM1:0]# fw lslogs
     Size      Log file name
     1960KB    fw.log
[Expert@CPCM1:0]#
```

```
[Expert@CPSMS:0]#
[Expert@CPSMS:0]# fw fetchlogs 10.0.0.2
File fetching in process. It may take some time...
File CPCM1__2022-05-13_175500.log was fetched successfully
File CPCM1__2022-05-13_180000.log was fetched successfully
File CPCM1__2022-05-14_000000.log was fetched successfully
[Expert@CPSMS:0]#
```



Check Point Host - CPSMS

- General Properties
- Network Management
- NAT
- Logs
  - Storage
  - Export
  - Additional Logging
- Other

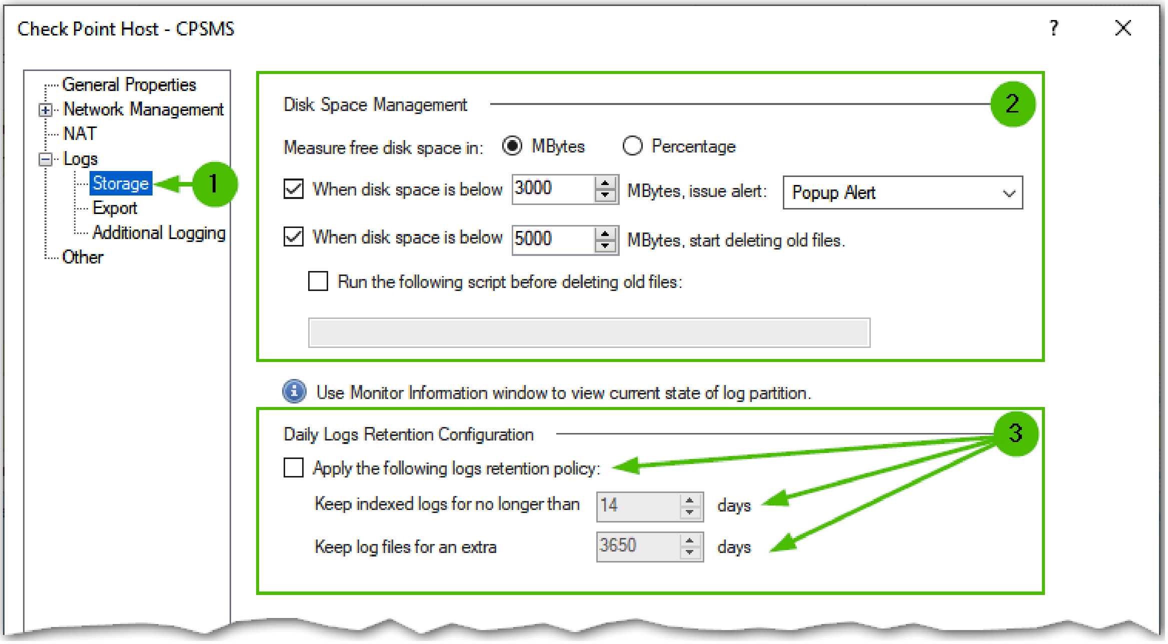
☑ Enable Log Indexing

The Log Indexing uses more storage to provide fast log queries

2 gateways have configured this machine as their log server

Type to Search 2 items

Gateway	IP Address	Comments	Type
CPGW	200.200.0.1		Send Logs and Alerts
CPCXL	200.100.0.1		Send Logs and Alerts



Check Point Host - CPSMS

- General Properties
- Network Management
- NAT
- Logs
  - Storage
  - Export
  - Additional Logging
- Other

Disk Space Management

Measure free disk space in: ● MBytes ○ Percentage

☑ When disk space is below 3000 MBytes, issue alert: Popup Alert

☑ When disk space is below 5000 MBytes, start deleting old files.

□ Run the following script before deleting old files:

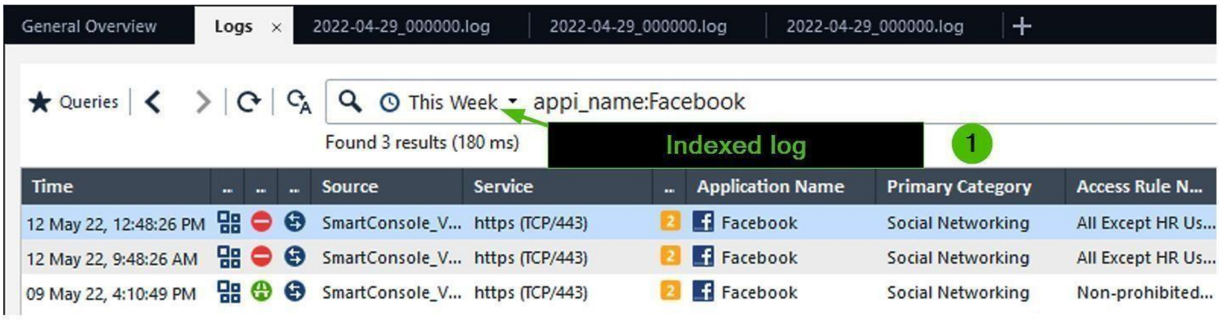
Use Monitor Information window to view current state of log partition.

Daily Logs Retention Configuration

□ Apply the following logs retention policy:

Keep indexed logs for no longer than 14 days

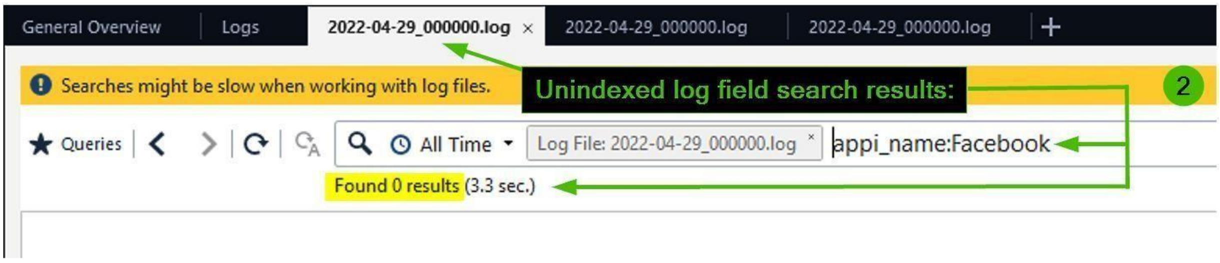
Keep log files for an extra 3650 days



appi_name:Facebook

Found 3 results (180 ms)

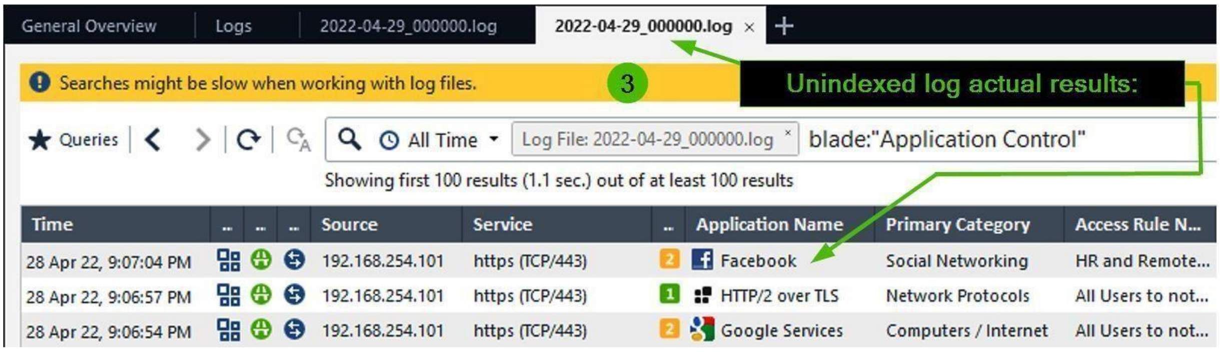
Time	...	...	...	Source	Service	...	Application Name	Primary Category	Access Rule N...
12 May 22, 12:48:26 PM				SmartConsole_V...	https (TCP/443)	2	Facebook	Social Networking	All Except HR Us...
12 May 22, 9:48:26 AM				SmartConsole_V...	https (TCP/443)	2	Facebook	Social Networking	All Except HR Us...
09 May 22, 4:10:49 PM				SmartConsole_V...	https (TCP/443)	2	Facebook	Social Networking	Non-prohibited...



Searches might be slow when working with log files.

appi_name:Facebook

Found 0 results (3.3 sec.)

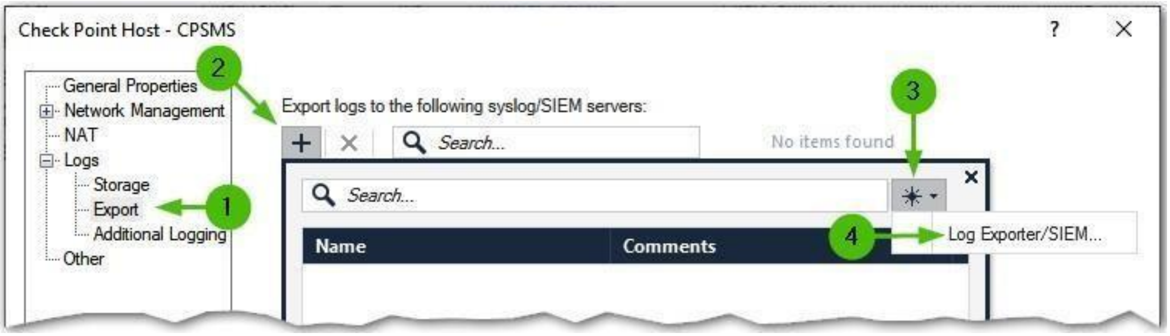


Searches might be slow when working with log files.

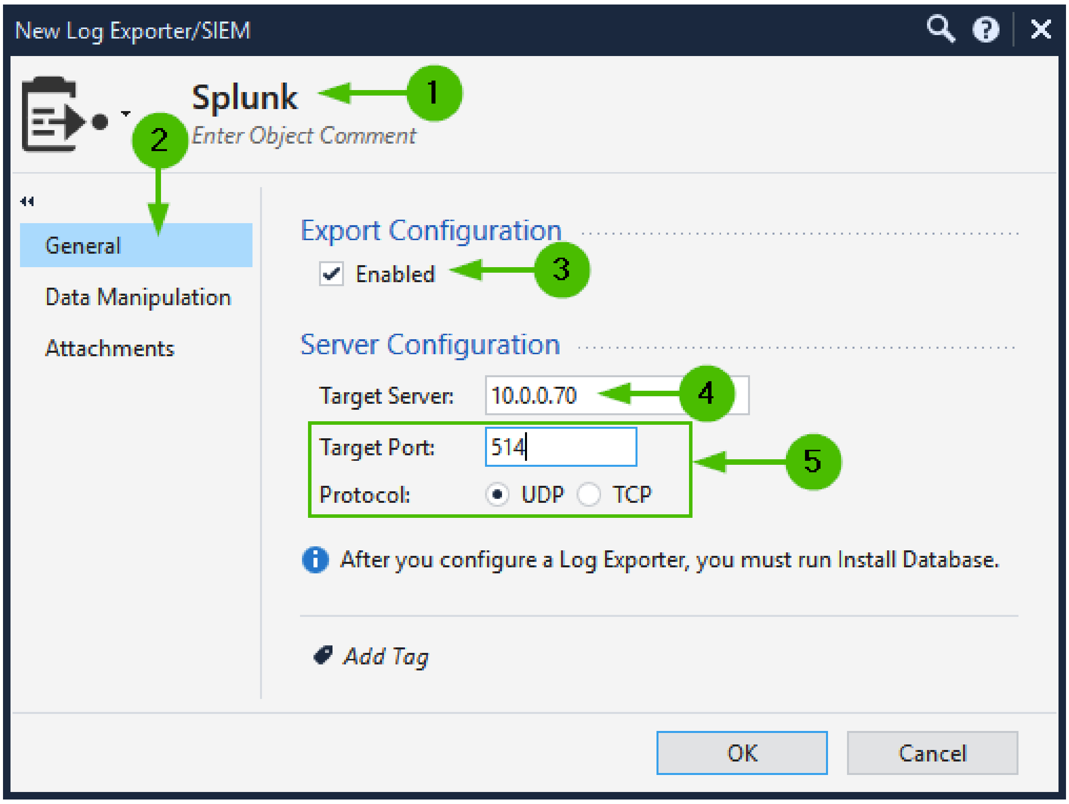
blade:"Application Control"

Showing first 100 results (1.1 sec.) out of at least 100 results

Time	...	...	...	Source	Service	...	Application Name	Primary Category	Access Rule N...
28 Apr 22, 9:07:04 PM				192.168.254.101	https (TCP/443)	2	Facebook	Social Networking	HR and Remote...
28 Apr 22, 9:06:57 PM				192.168.254.101	https (TCP/443)	1	HTTP/2 over TLS	Network Protocols	All Users to not...
28 Apr 22, 9:06:54 PM				192.168.254.101	https (TCP/443)	2	Google Services	Computers / Internet	All Users to not...



Export logs to the following syslog/SIEM servers:



New Log Exporter/SIEM

Splunk

Enter Object Comment

Export Configuration

☑ Enabled

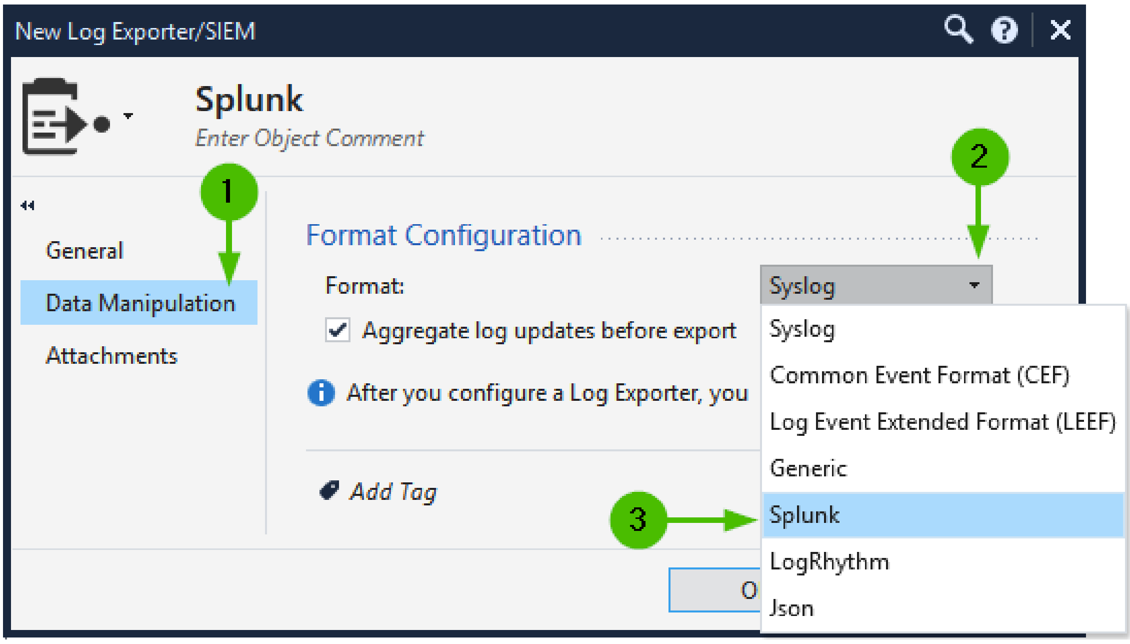
Server Configuration

Target Server: 10.0.0.70

Target Port: 514

Protocol: ● UDP ○ TCP

After you configure a Log Exporter, you must run Install Database.



New Log Exporter/SIEM

Splunk

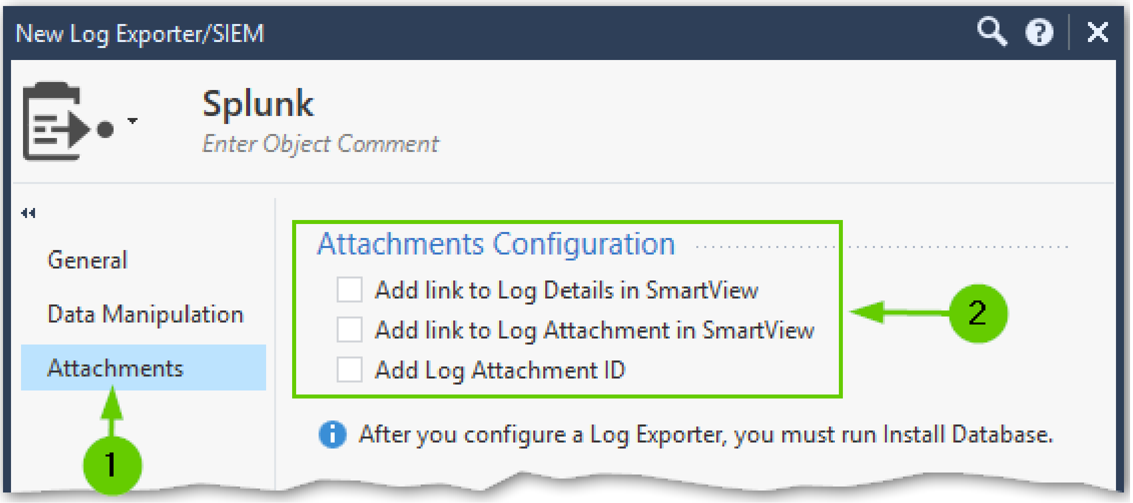
Enter Object Comment

Format Configuration

Format: Syslog

☑ Aggregate log updates before export

After you configure a Log Exporter, you



Splunk

Enter Object Comment

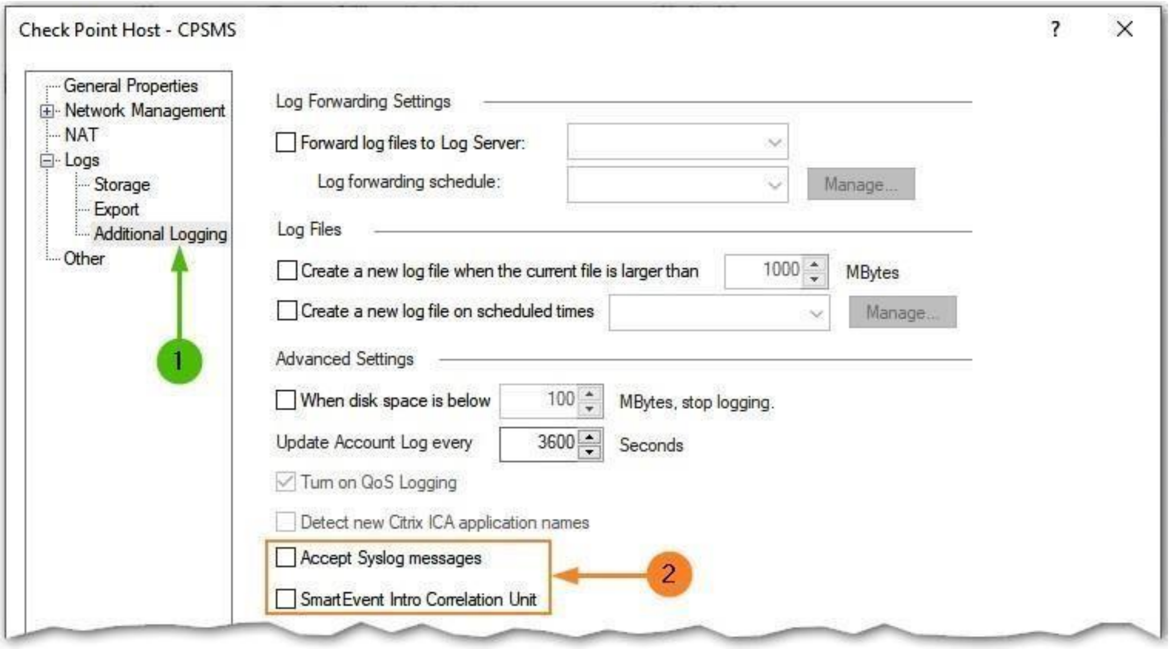
Attachments Configuration

□ Add link to Log Details in SmartView

□ Add link to Log Attachment in SmartView

□ Add Log Attachment ID

After you configure a Log Exporter, you must run Install Database.



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.

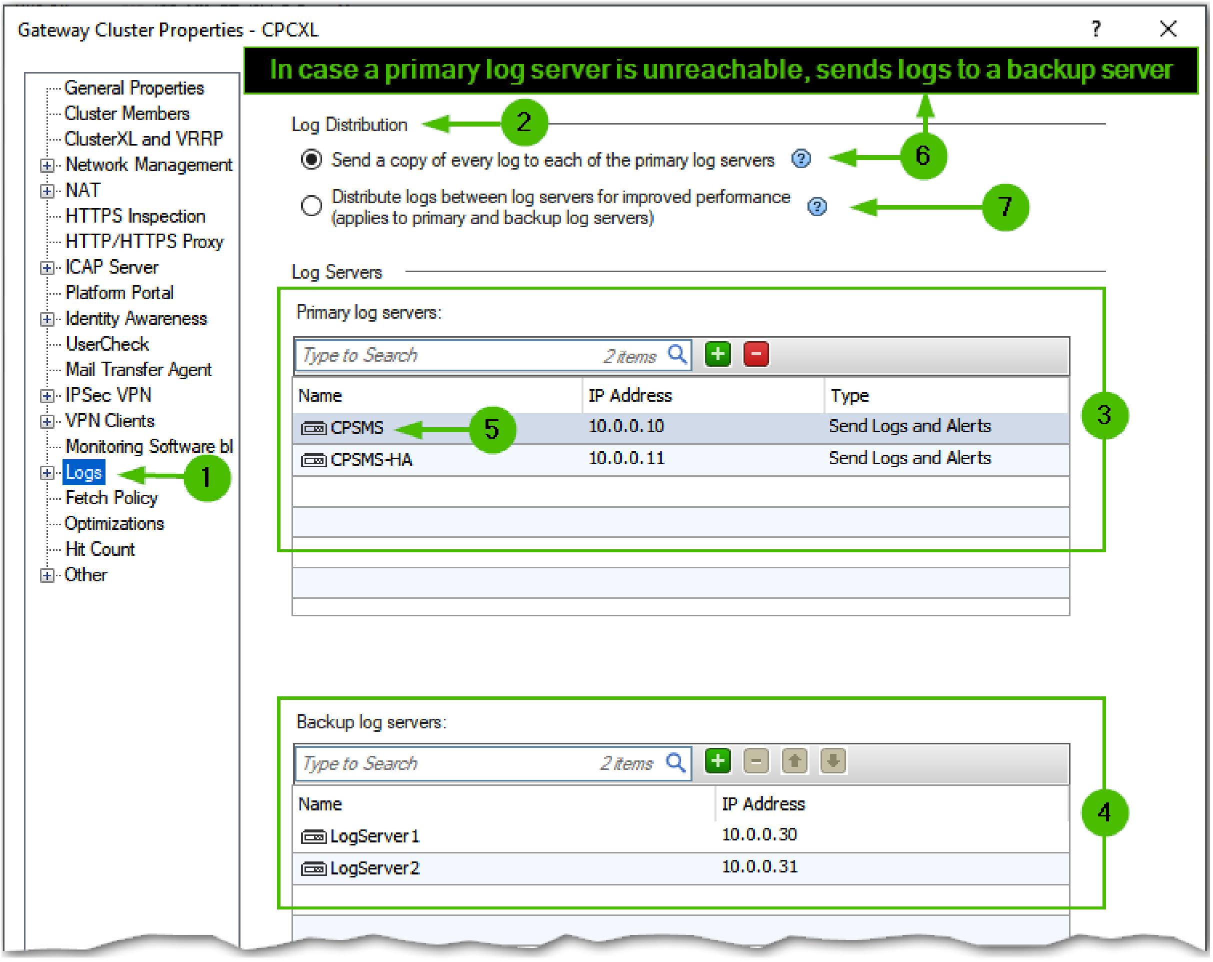
Update Account Log every 3600 Seconds

☑ Turn on QoS Logging

□ Detect new Citrix ICA application names

□ Accept Syslog messages

□ SmartEvent Intro Correlation Unit



Gateway Cluster Properties - CPCXL

In case a primary log server is unreachable, sends logs to a backup server

Log Distribution

● Send a copy of every log to each of the primary log servers

○ Distribute logs between log servers for improved performance (applies to primary and backup log servers)

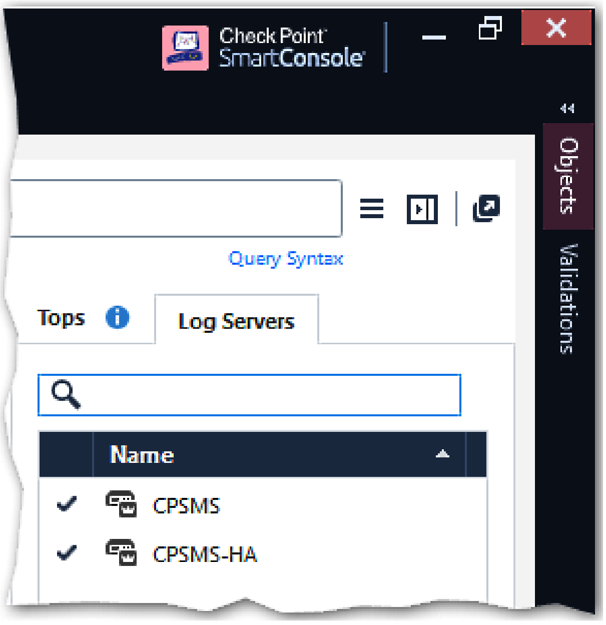
Log Servers

Primary log servers:

Name	IP Address	Type
CPSMS	10.0.0.10	Send Logs and Alerts
CPSMS-HA	10.0.0.11	Send Logs and Alerts

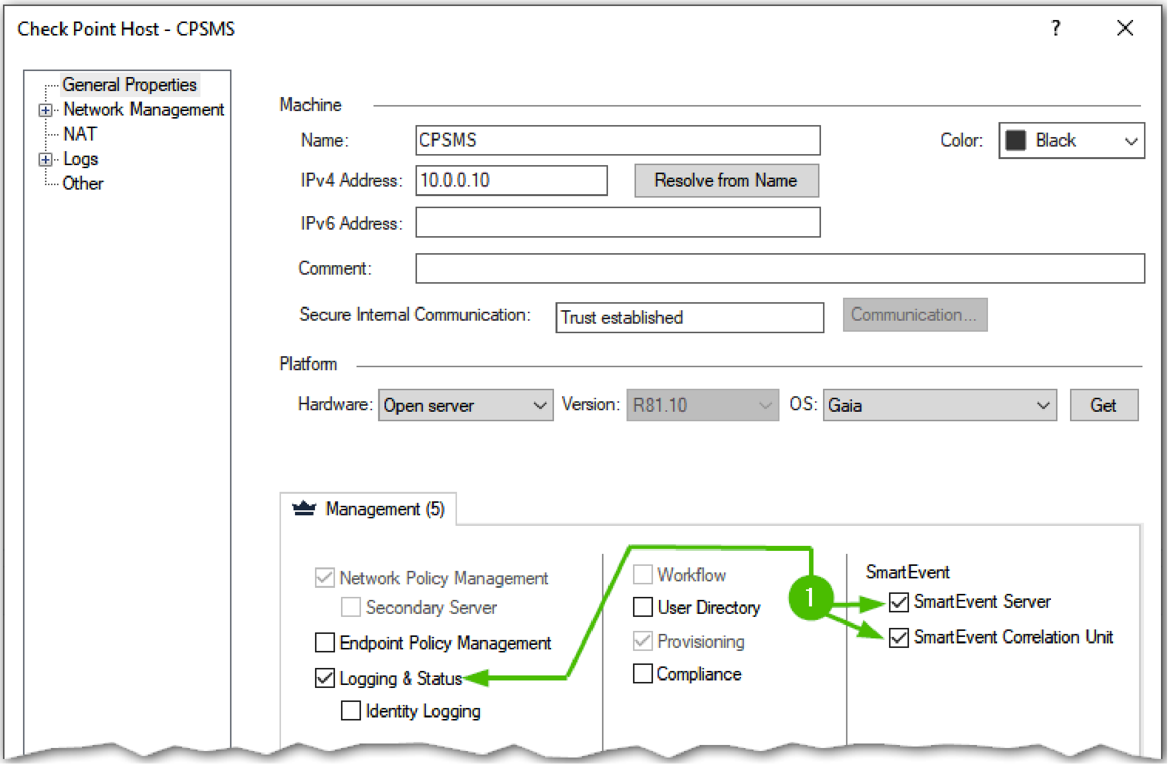
Backup log servers:

Name	IP Address
LogServer1	10.0.0.30
LogServer2	10.0.0.31



Log Servers

Name
✓ CPSMS
✓ CPSMS-HA



Machine

Name: CPSMS

Color: Black

IPv4 Address: 10.0.0.10

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

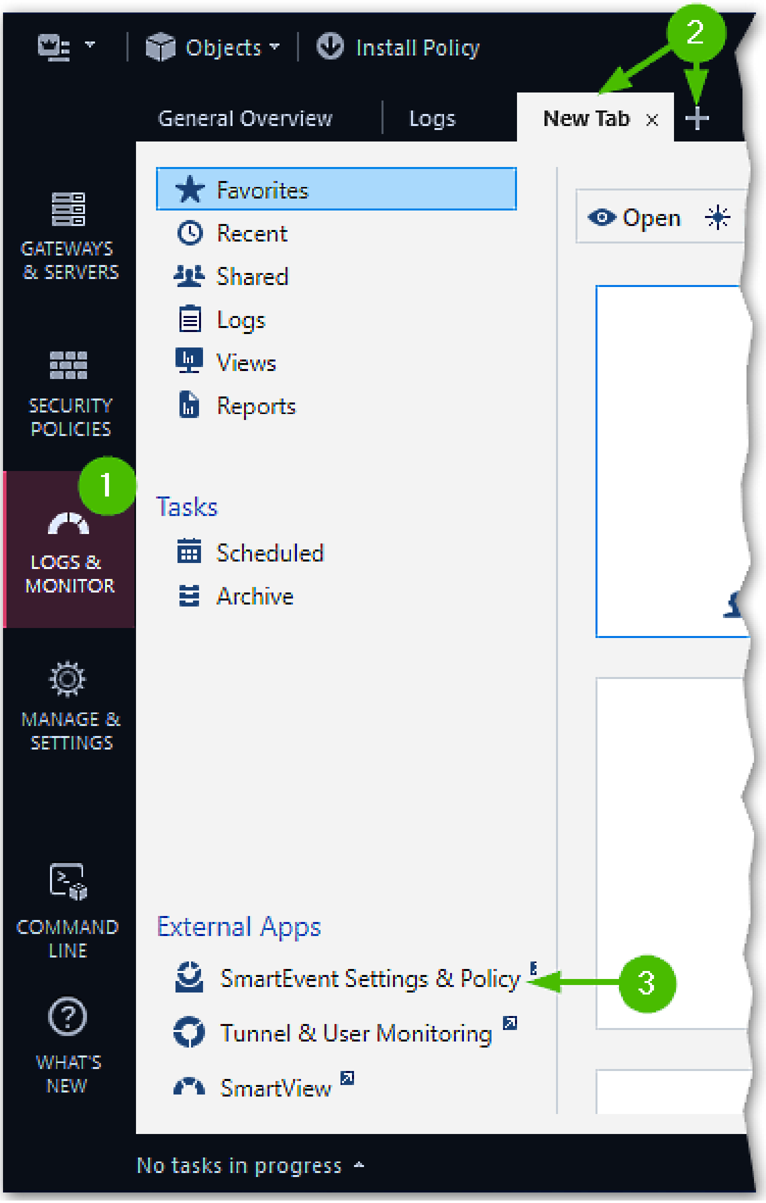
Platform

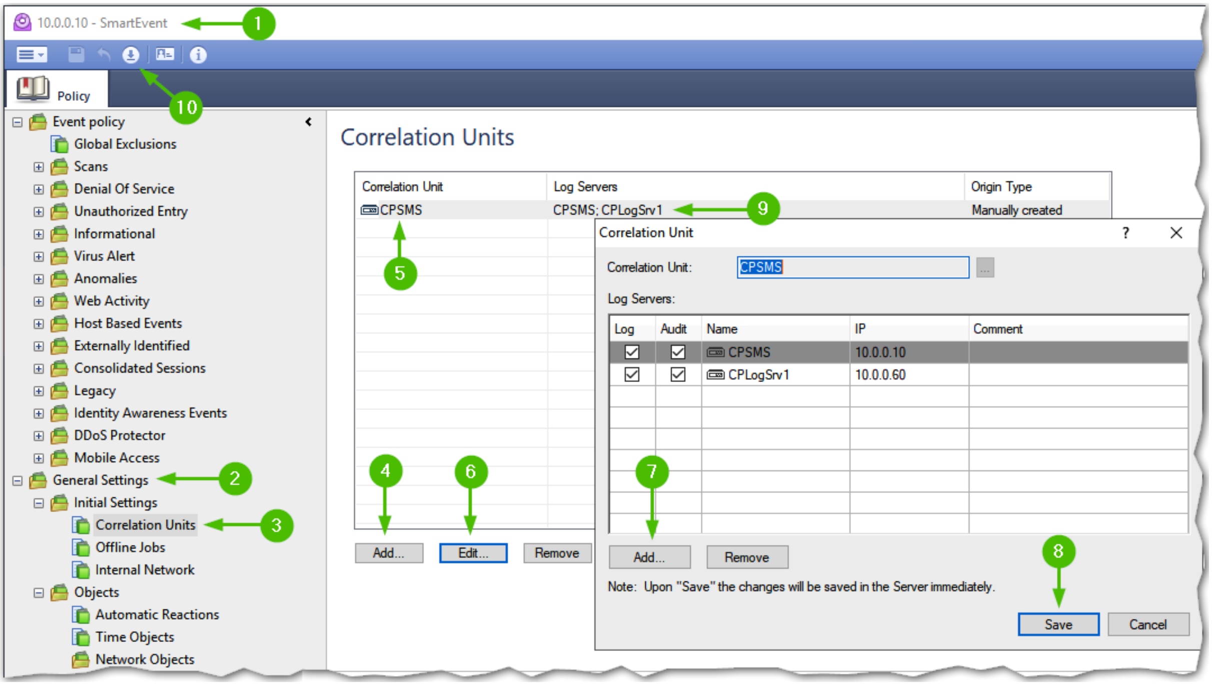
Hardware: Open server Version: R81.10 OS: Gaia

☑ Network Policy Management
□ Secondary Server
□ Endpoint Policy Management
☑ Logging & Status
□ Identity Logging

□ Workflow
□ User Directory
☑ Provisioning
□ Compliance

SmartEvent
☑ SmartEvent Server
☑ SmartEvent Correlation Unit


Objects
Install Policy
2
General Overview
Logs
New Tab
GATEWAYS & SERVERS
SECURITY POLICIES
1
LOGS & MONITOR
MANAGE & SETTINGS
COMMAND LINE
WHAT'S NEW
Favorites
Recent
Shared
Logs
Views
Reports
Tasks
Scheduled
Archive
External Apps
SmartEvent Settings & Policy
3
Tunnel & User Monitoring
SmartView
Open
No tasks in progress



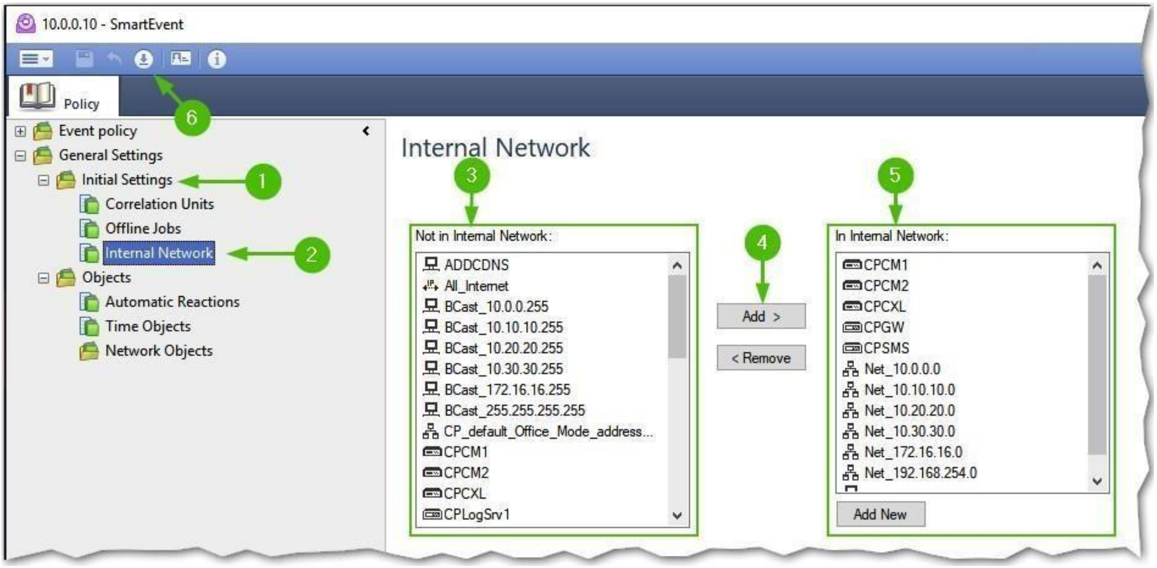
Correlation Unit	Log Servers	Origin Type
CPSMS	CPSMS; CPLogSrv1	Manually created

Correlation Unit: CPSMS

Log Servers:

Log	Audit	Name	IP	Comment
☑	☑	CPSMS	10.0.0.10	
☑	☑	CPLogSrv1	10.0.0.60	

Note: Upon "Save" the changes will be saved in the Server immediately.

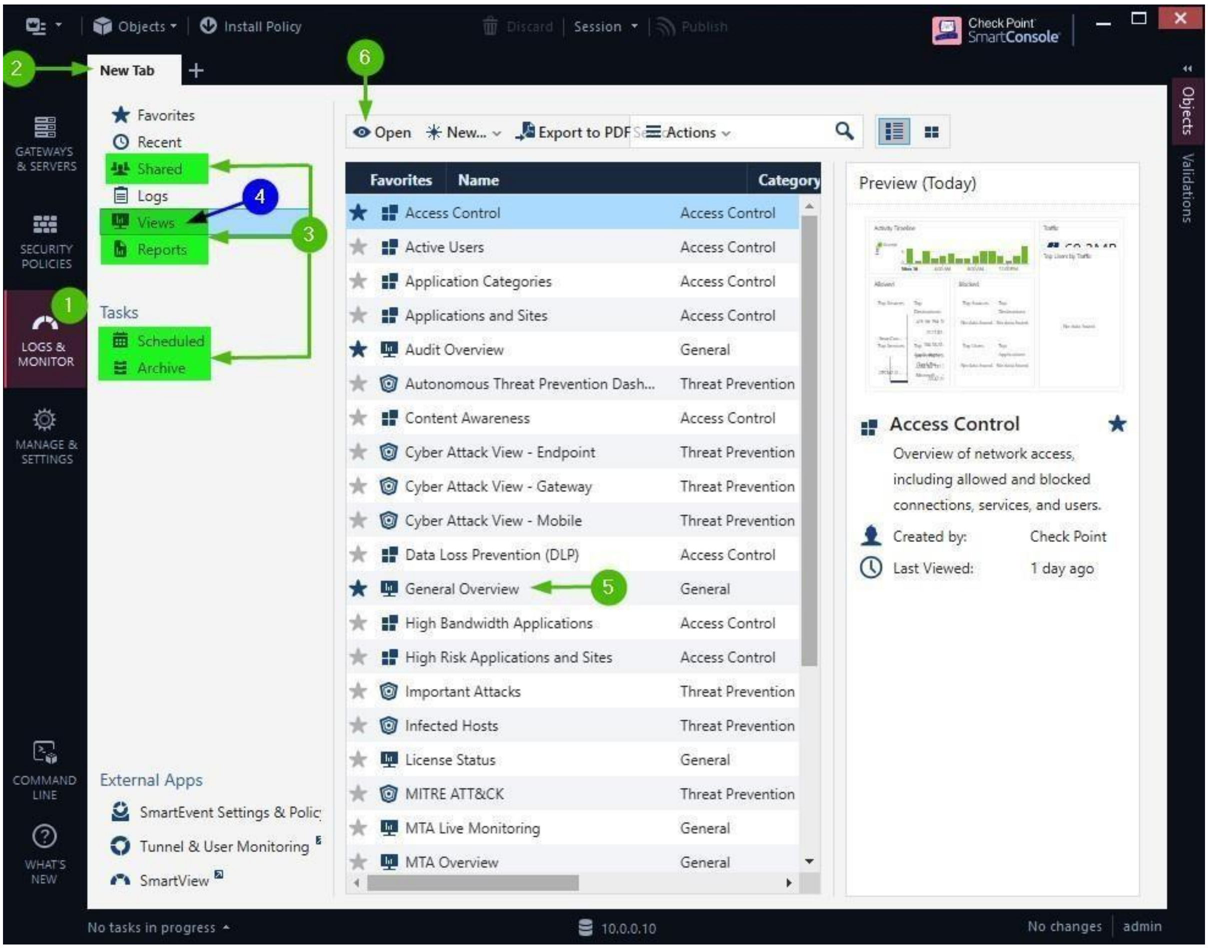


Not in Internal Network:

- ADDCDNS
- All_Internet
- BCast_10.0.0.255
- BCast_10.10.10.255
- BCast_10.20.20.255
- BCast_10.30.30.255
- BCast_172.16.16.255
- BCast_255.255.255.255
- CP_default_Office_Mode_address...
- CPCM1
- CPCM2
- CPCXL
- CPLogSrv1

In Internal Network:

- CPCM1
- CPCM2
- CPCXL
- CPGW
- CPSMS
- Net_10.0.0.0
- Net_10.10.10.0
- Net_10.20.20.0
- Net_10.30.30.0
- Net_172.16.16.0
- Net_192.168.254.0



Favorites	Name	Category
★	Access Control	Access Control
☆	Active Users	Access Control
☆	Application Categories	Access Control
☆	Applications and Sites	Access Control
★	Audit Overview	General
☆	Autonomous Threat Prevention Dash...	Threat Prevention
☆	Content Awareness	Access Control
☆	Cyber Attack View - Endpoint	Threat Prevention
☆	Cyber Attack View - Gateway	Threat Prevention
☆	Cyber Attack View - Mobile	Threat Prevention
☆	Data Loss Prevention (DLP)	Access Control
★	General Overview	General
☆	High Bandwidth Applications	Access Control
☆	High Risk Applications and Sites	Access Control
☆	Important Attacks	Threat Prevention
☆	Infected Hosts	Threat Prevention
☆	License Status	General
☆	MITRE ATT&CK	Threat Prevention
☆	MTA Live Monitoring	General
☆	MTA Overview	General

Preview (Today)

Access Control ★

Overview of network access, including allowed and blocked connections, services, and users.

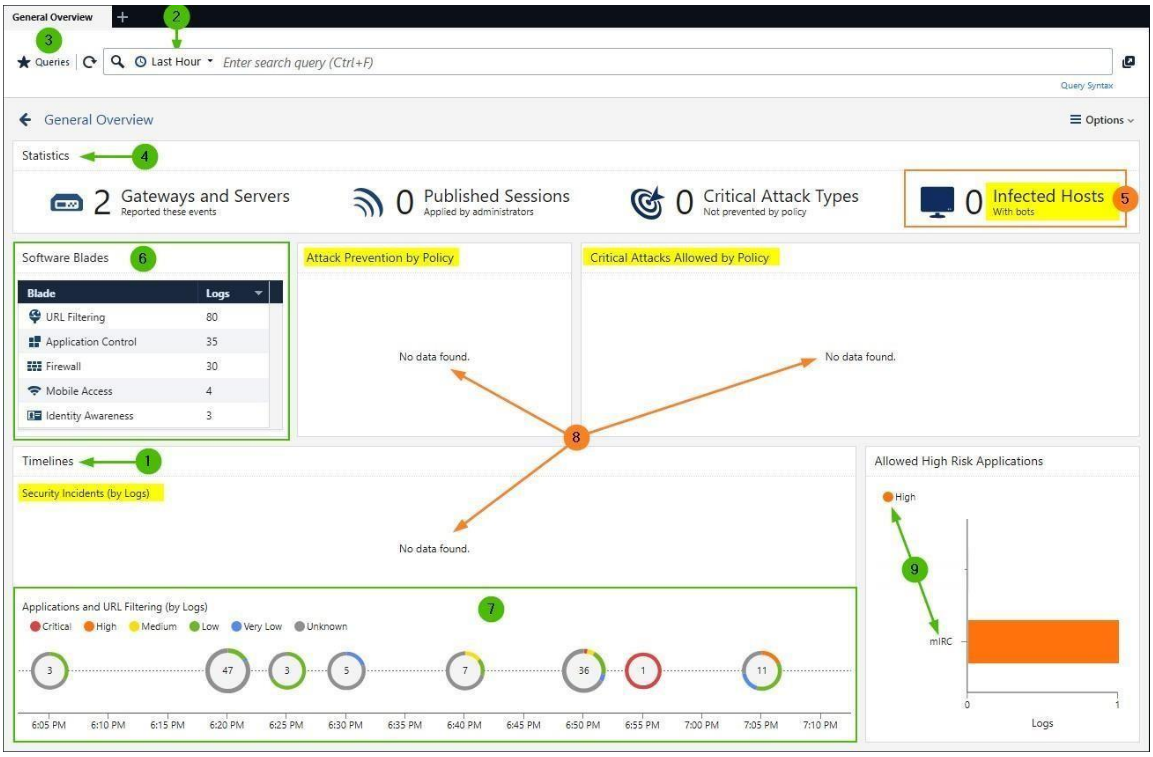
Created by: Check Point

Last Viewed: 1 day ago

No tasks in progress

10.0.0.10

No changes | admin



Statistics

2 Gateways and Servers — Reported these events

0 Published Sessions — Applied by administrators

0 Critical Attack Types — Not prevented by policy

0 Infected Hosts — With bots

Software Blades

Blade	Logs
URL Filtering	80
Application Control	35
Firewall	30
Mobile Access	4
Identity Awareness	3

Attack Prevention by Policy

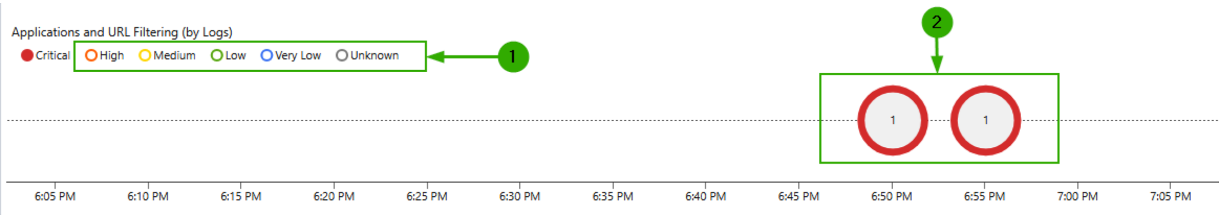
Critical Attacks Allowed by Policy

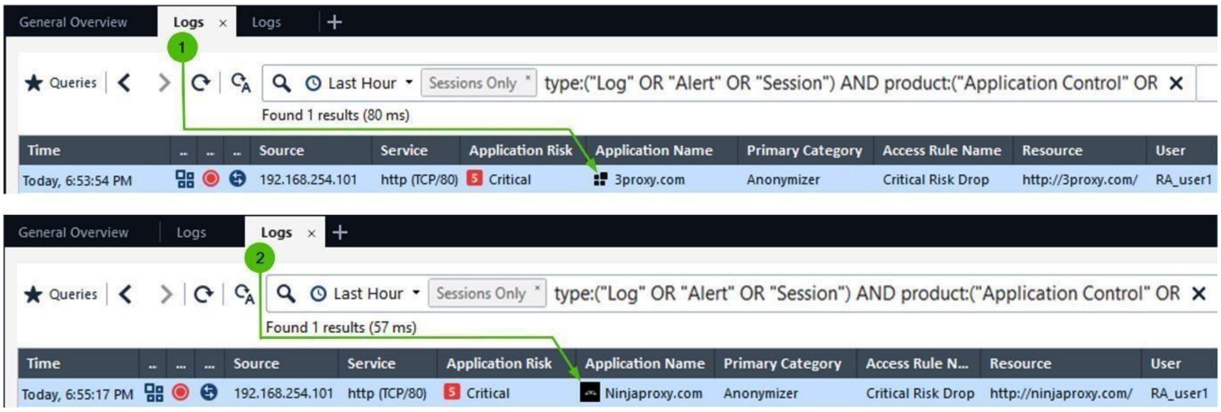
Timelines

Security Incidents (by Logs)

Applications and URL Filtering (by Logs)

Allowed High Risk Applications





type:("Log" OR "Alert" OR "Session") AND product:("Application Control" OR

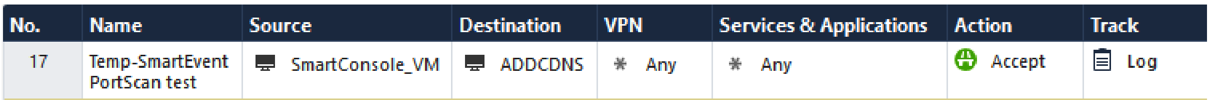
Found 1 results (80 ms)

Time	...	...	...	Source	Service	Application Risk	Application Name	Primary Category	Access Rule Name	Resource	User
Today, 6:53:54 PM				192.168.254.101	http (TCP/80)	Critical	3proxy.com	Anonymizer	Critical Risk Drop	http://3proxy.com/	RA_user1

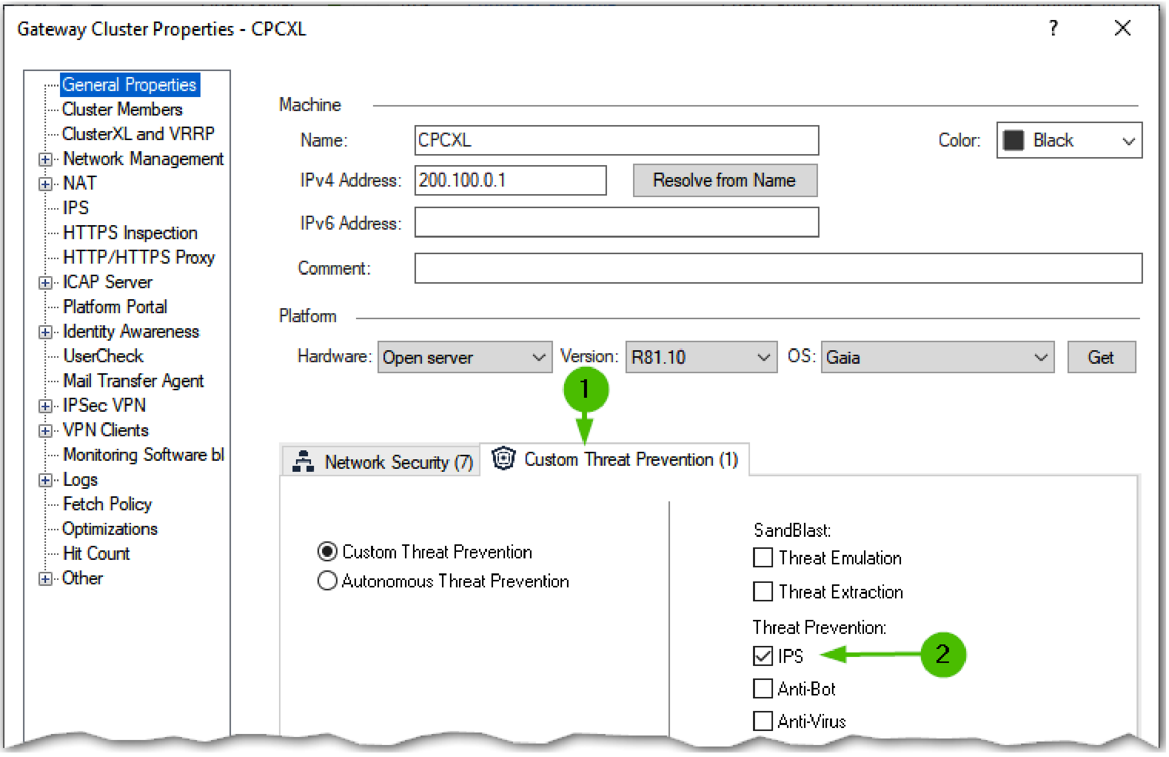
type:("Log" OR "Alert" OR "Session") AND product:("Application Control" OR

Found 1 results (57 ms)

Time	...	...	...	Source	Service	Application Risk	Application Name	Primary Category	Access Rule N...	Resource	User
Today, 6:55:17 PM				192.168.254.101	http (TCP/80)	Critical	Ninjaproxy.com	Anonymizer	Critical Risk Drop	http://ninjaproxy.com/	RA_user1



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
17	Temp-SmartEvent PortScan test	SmartConsole_VM	ADDCDNS	Any	Any	Accept	Log



Gateway Cluster Properties - CPCXL

Machine

Name: CPCXL

Color: Black

IPv4 Address: 200.100.0.1

IPv6 Address:

Comment:

Platform

Hardware: Open server

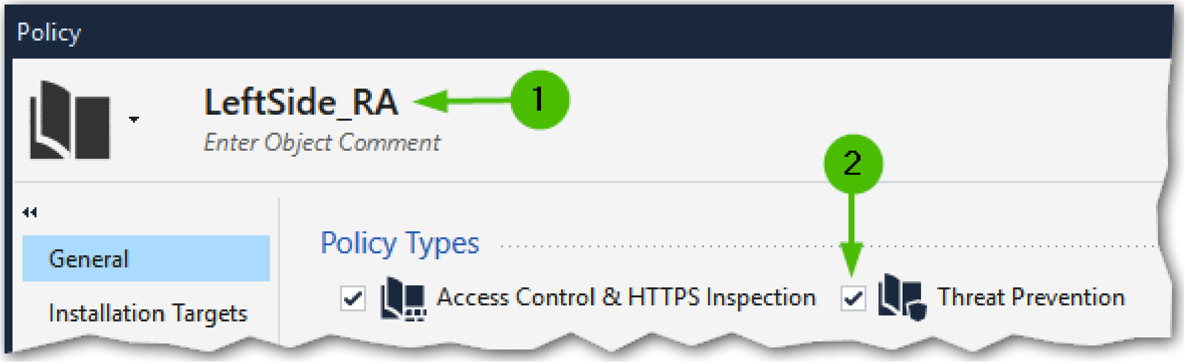
Version: R81.10

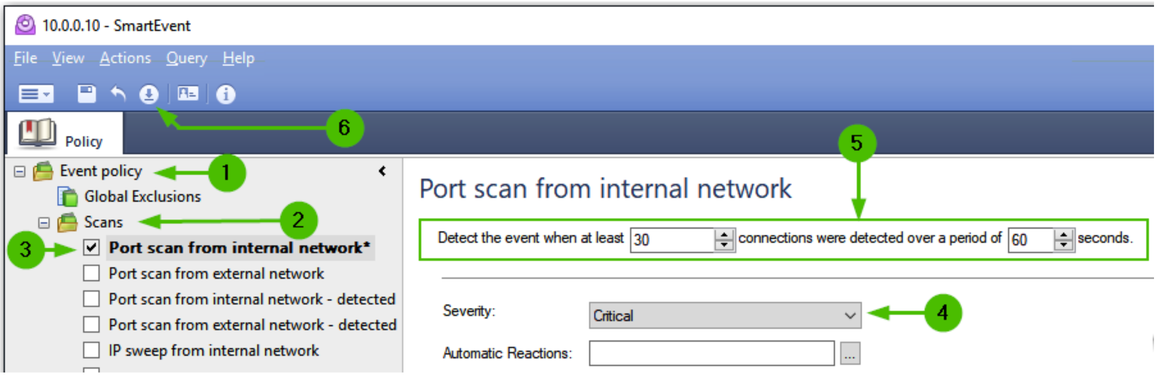
OS: Gaia

● Custom Threat Prevention
○ Autonomous Threat Prevention

SandBlast:
□ Threat Emulation
□ Threat Extraction

Threat Prevention:
☑ IPS
□ Anti-Bot
□ Anti-Virus





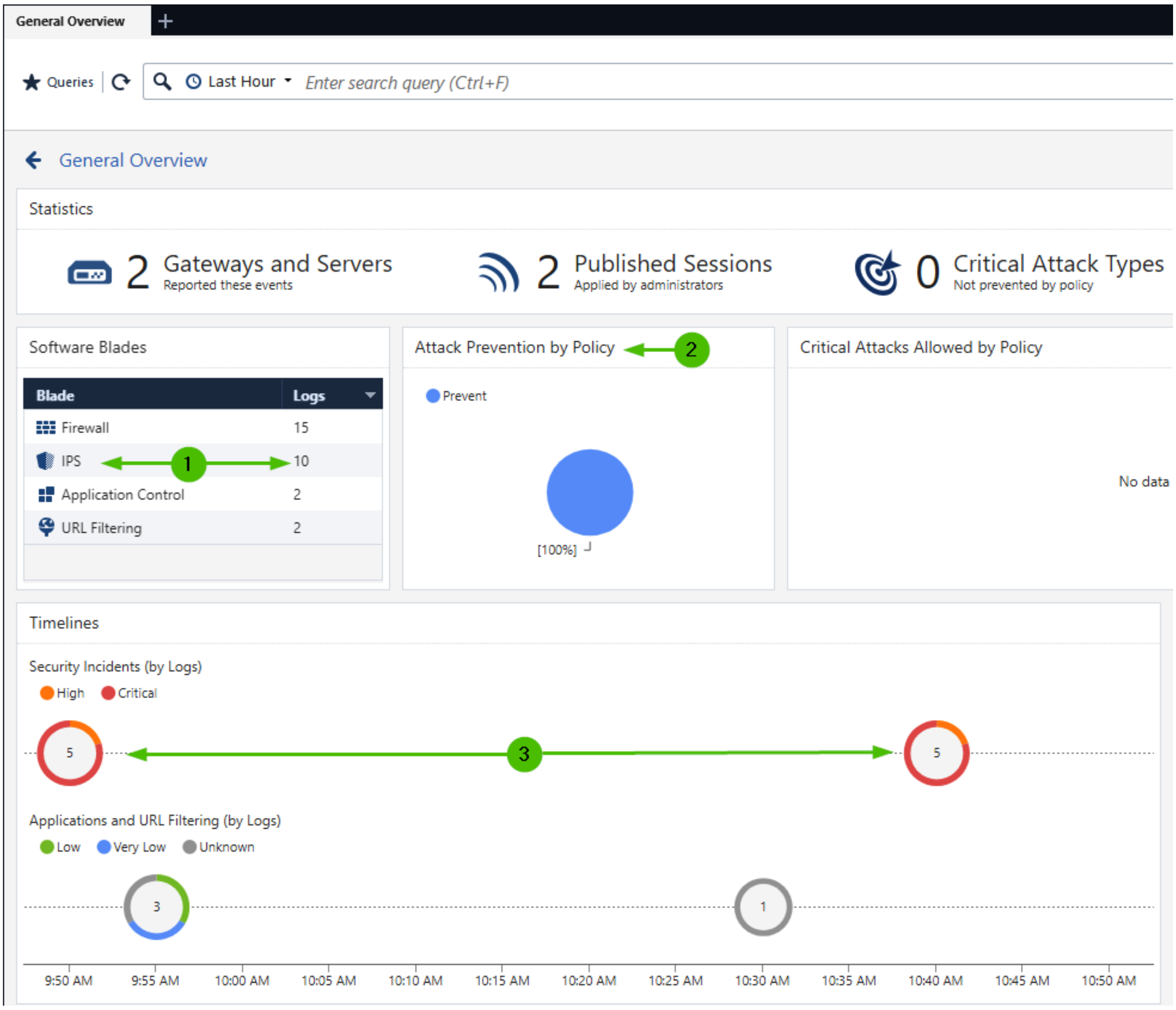
10.0.0.10 - SmartEvent
File View Actions Query Help
Policy
6
Event policy
1
Global Exclusions
Scans
2
3
☑ Port scan from internal network*
□ Port scan from external network
□ Port scan from internal network - detected
□ Port scan from external network - detected
□ IP sweep from internal network
5
4

Port scan from internal network

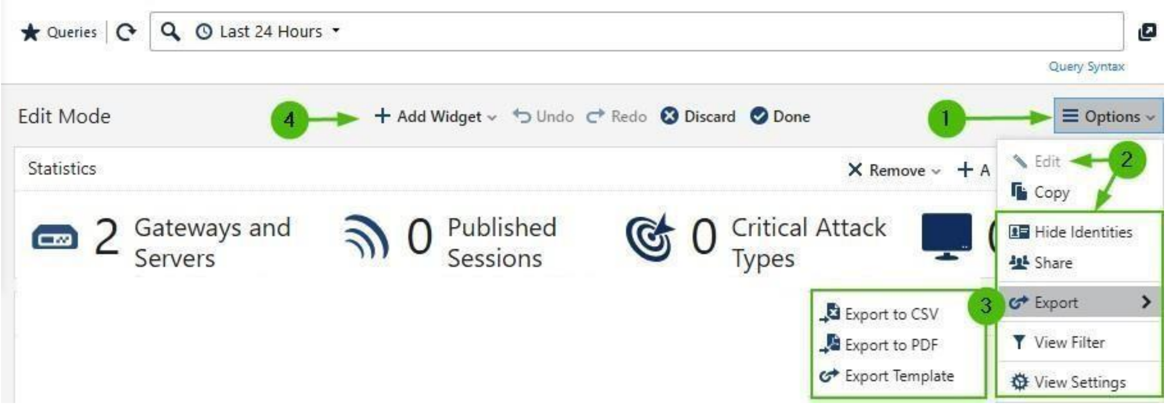
Detect the event when at least 30 connections were detected over a period of 60 seconds.

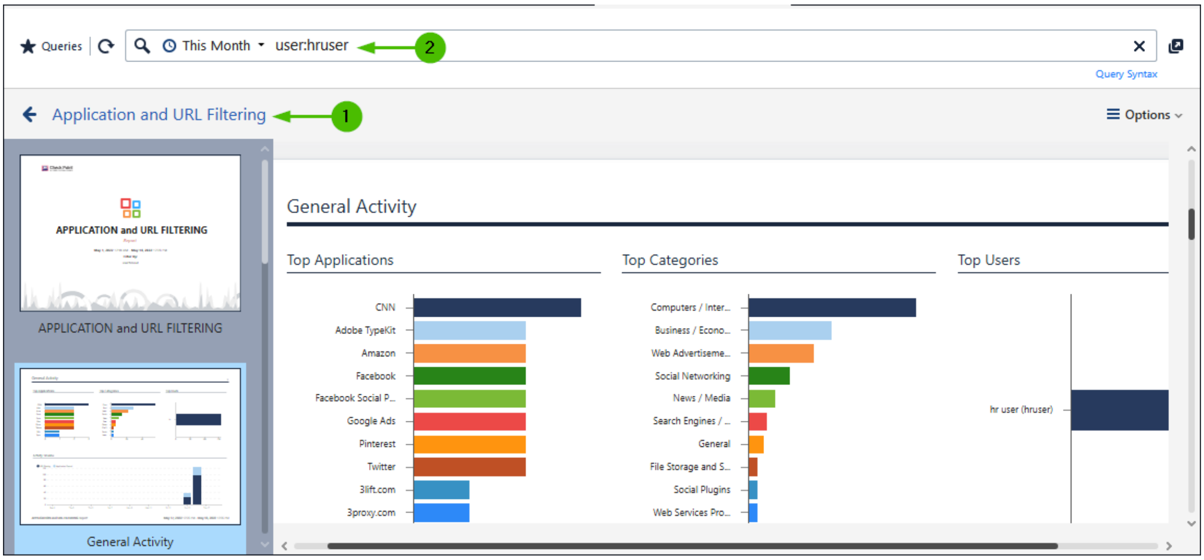
Severity: Critical

Automatic Reactions:

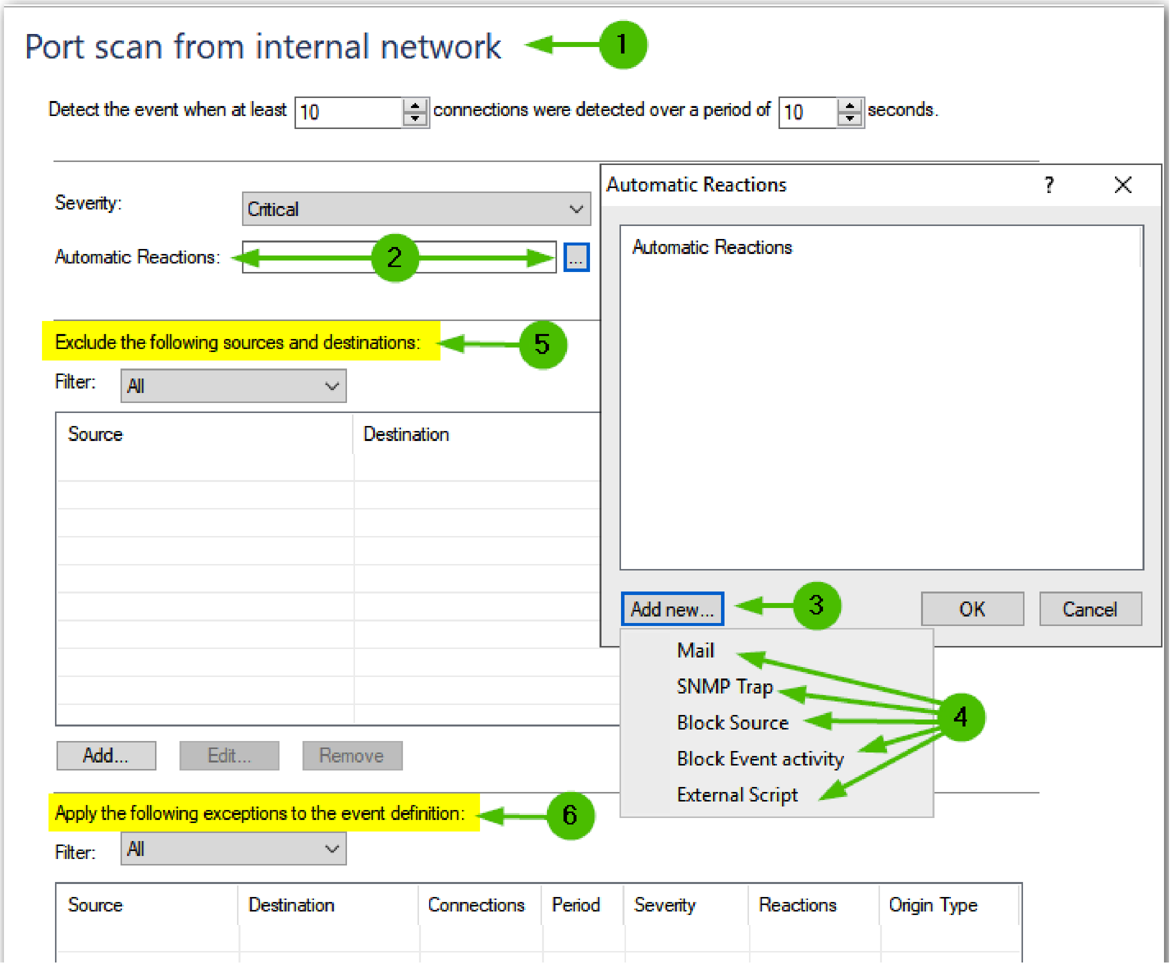


Blade	Logs
Firewall	15
IPS	10
Application Control	2
URL Filtering	2



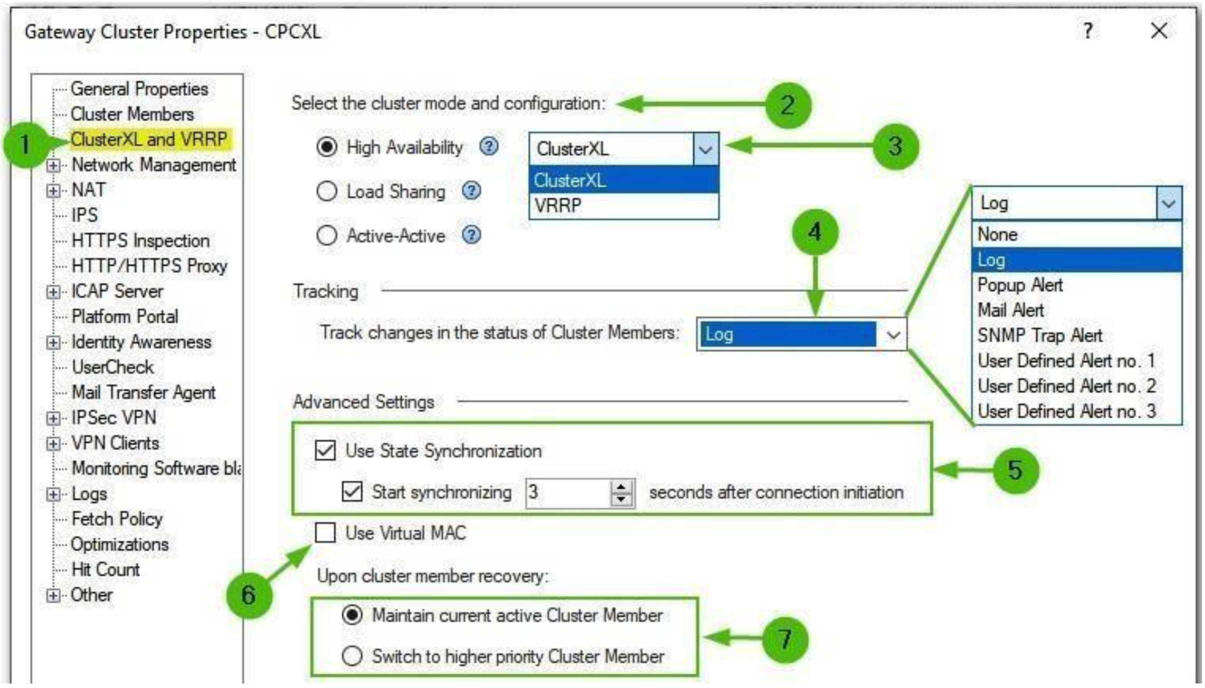


Queries
This Month
user:hruser
2
Query Syntax
Application and URL Filtering
1
Options
APPLICATION and URL FILTERING
General Activity
General Activity
Top Applications
Top Categories
Top Users
CNN
Adobe TypeKit
Amazon
Facebook
Facebook Social P...
Google Ads
Pinterest
Twitter
3lift.com
3proxy.com
Computers / Inter...
Business / Econo...
Web Advertiseme...
Social Networking
News / Media
Search Engines / ...
General
File Storage and S...
Social Plugins
Web Services Pro...
hr user (hruser)



Port scan from internal network
1
Detect the event when at least 10 connections were detected over a period of 10 seconds.
Severity: Critical
Automatic Reactions:
2
Exclude the following sources and destinations:
5
Filter: All
Source
Destination
Add...
Edit...
Remove
Apply the following exceptions to the event definition:
6
Filter: All
Source
Destination
Connections
Period
Severity
Reactions
Origin Type
Automatic Reactions
?
Automatic Reactions
Add new...
3
OK
Cancel
Mail
SNMP Trap
Block Source
Block Event activity
External Script
4

Chapter 14: Working with ClusterXL High Availability



Gateway Cluster Properties - CPCXL

Select the cluster mode and configuration:

● High Availability: ClusterXL

○ Load Sharing

○ Active-Active

Tracking

Track changes in the status of Cluster Members: Log

Advanced Settings

☑ Use State Synchronization

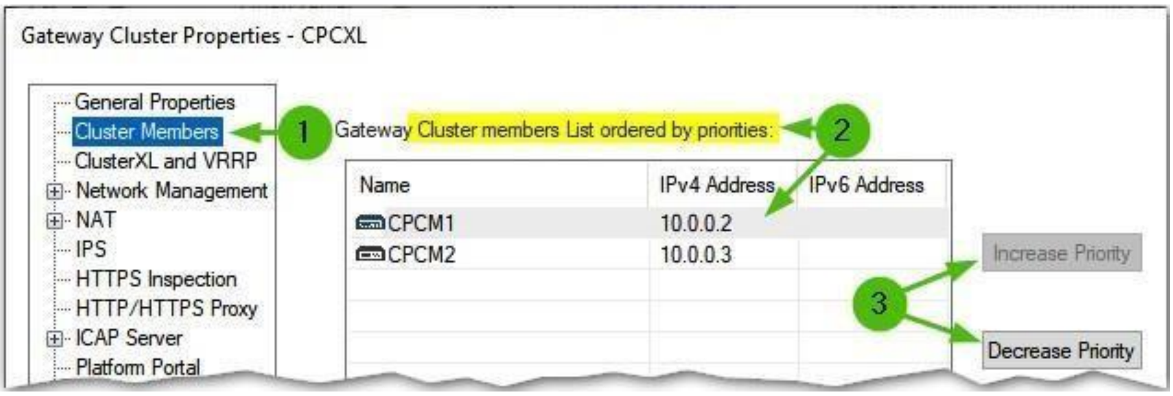
☑ Start synchronizing 3 seconds after connection initiation

☐ Use Virtual MAC

Upon cluster member recovery:

● Maintain current active Cluster Member

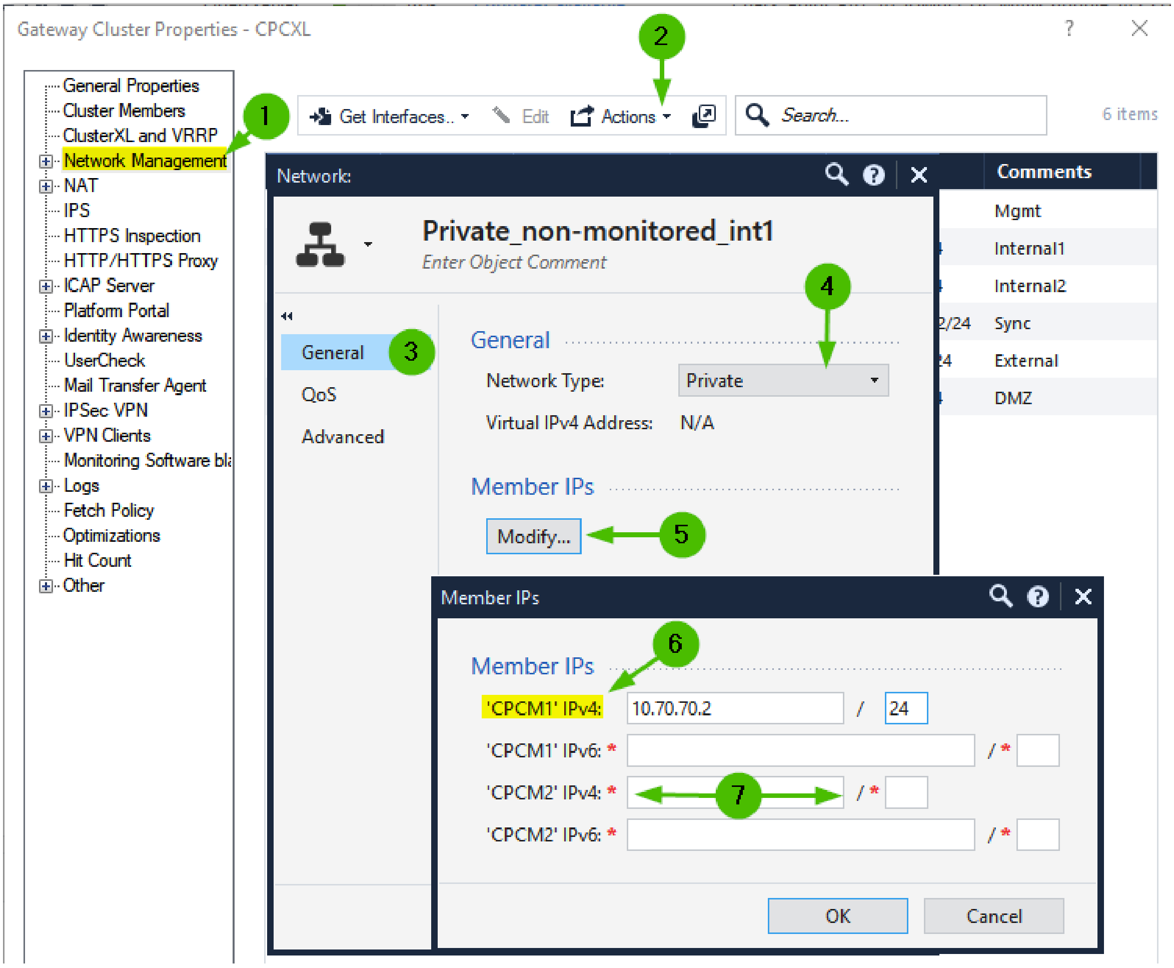
○ Switch to higher priority Cluster Member



Gateway Cluster Properties - CPCXL

Gateway Cluster members List ordered by priorities:

Name	IPv4 Address	IPv6 Address
CPCM1	10.0.0.2	
CPCM2	10.0.0.3	



Private_non-monitored_int1

Network Type: Private

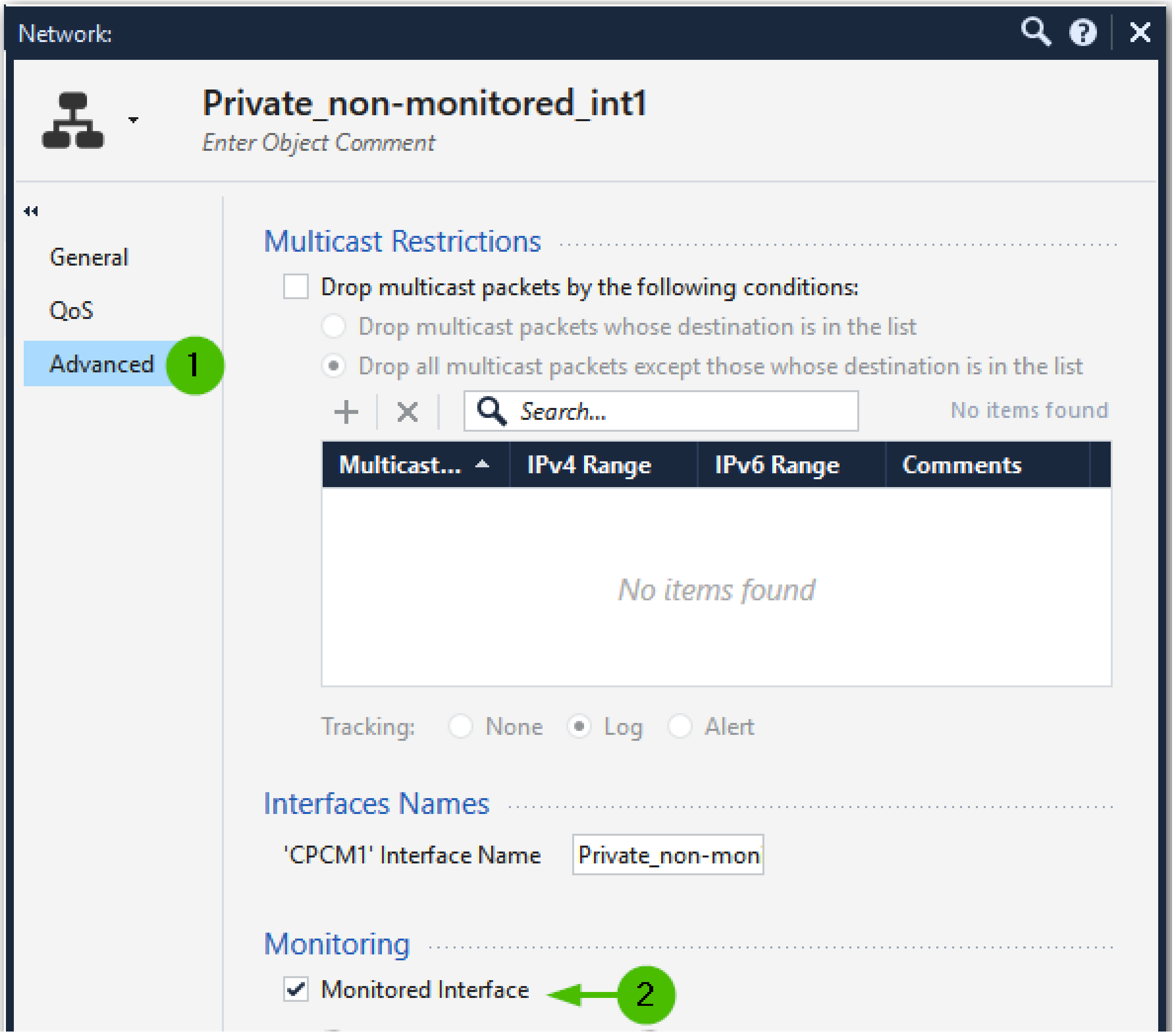
Virtual IPv4 Address: N/A

'CPCM1' IPv4: 10.70.70.2 / 24

'CPCM1' IPv6: * / *

'CPCM2' IPv4: * / *

'CPCM2' IPv6: * / *



Network:

Private_non-monitored_int1

Enter Object Comment

General

QoS

Advanced

Multicast Restrictions

☐ Drop multicast packets by the following conditions:

○ Drop multicast packets whose destination is in the list

● Drop all multicast packets except those whose destination is in the list

Multicast...	IPv4 Range	IPv6 Range	Comments

No items found

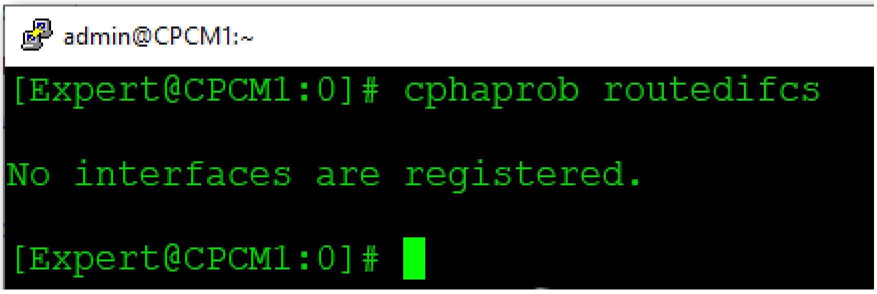
Tracking: ○ None ● Log ○ Alert

Interfaces Names

'CPCM1' Interface Name: Private_non-mon

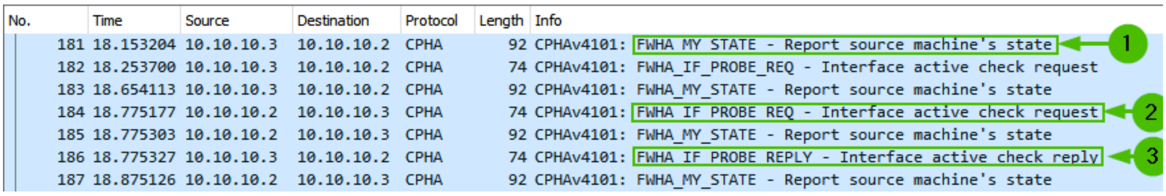
Monitoring

☑ Monitored Interface

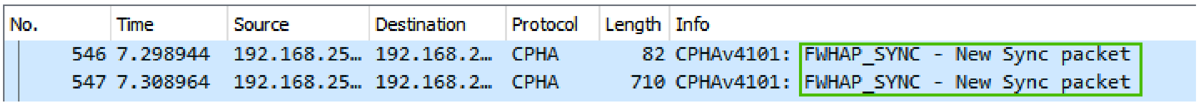


admin@CPCM1:~

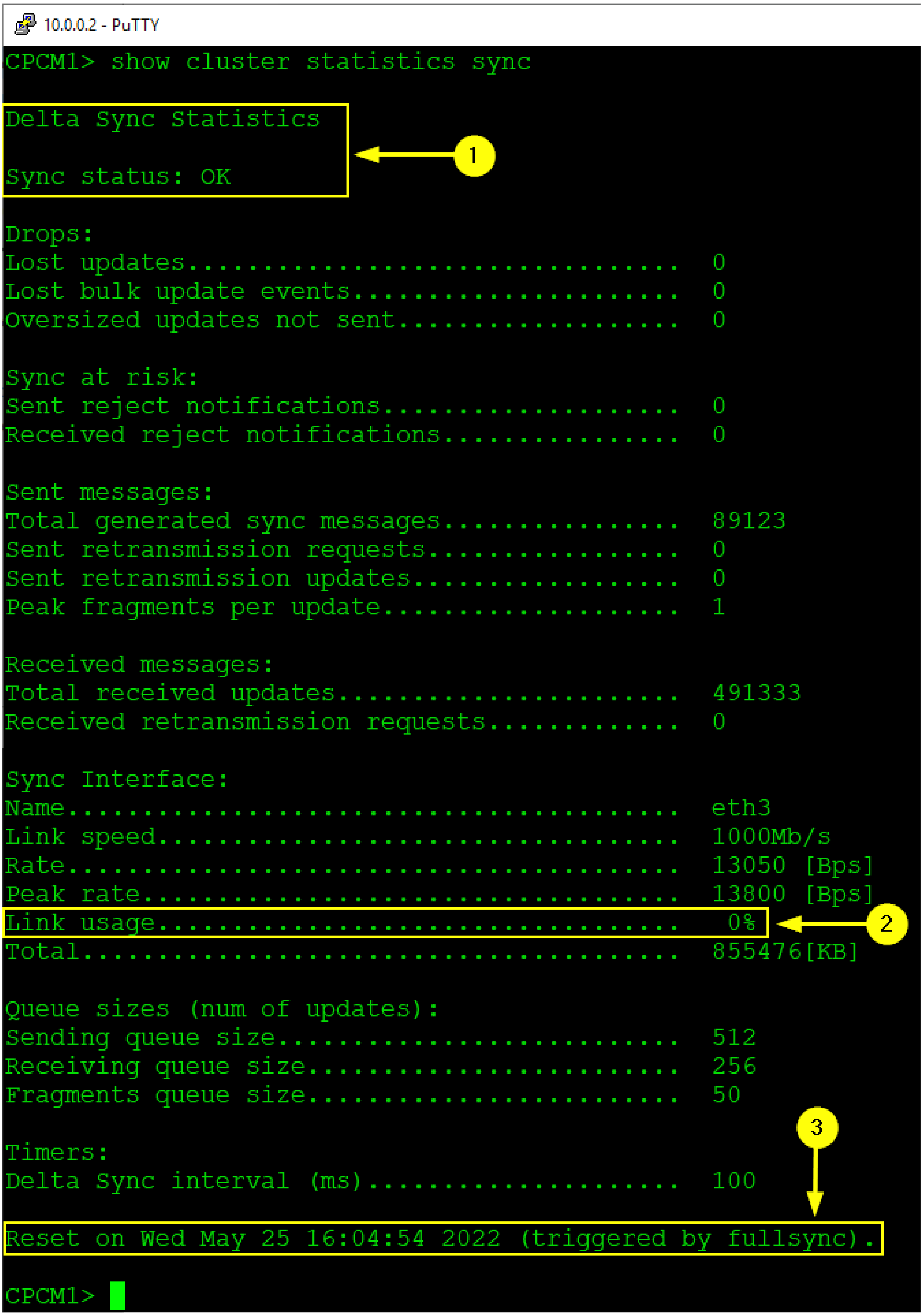
```
[Expert@CPCM1:0]# cphaprob routedifcs

No interfaces are registered.

[Expert@CPCM1:0]#
```



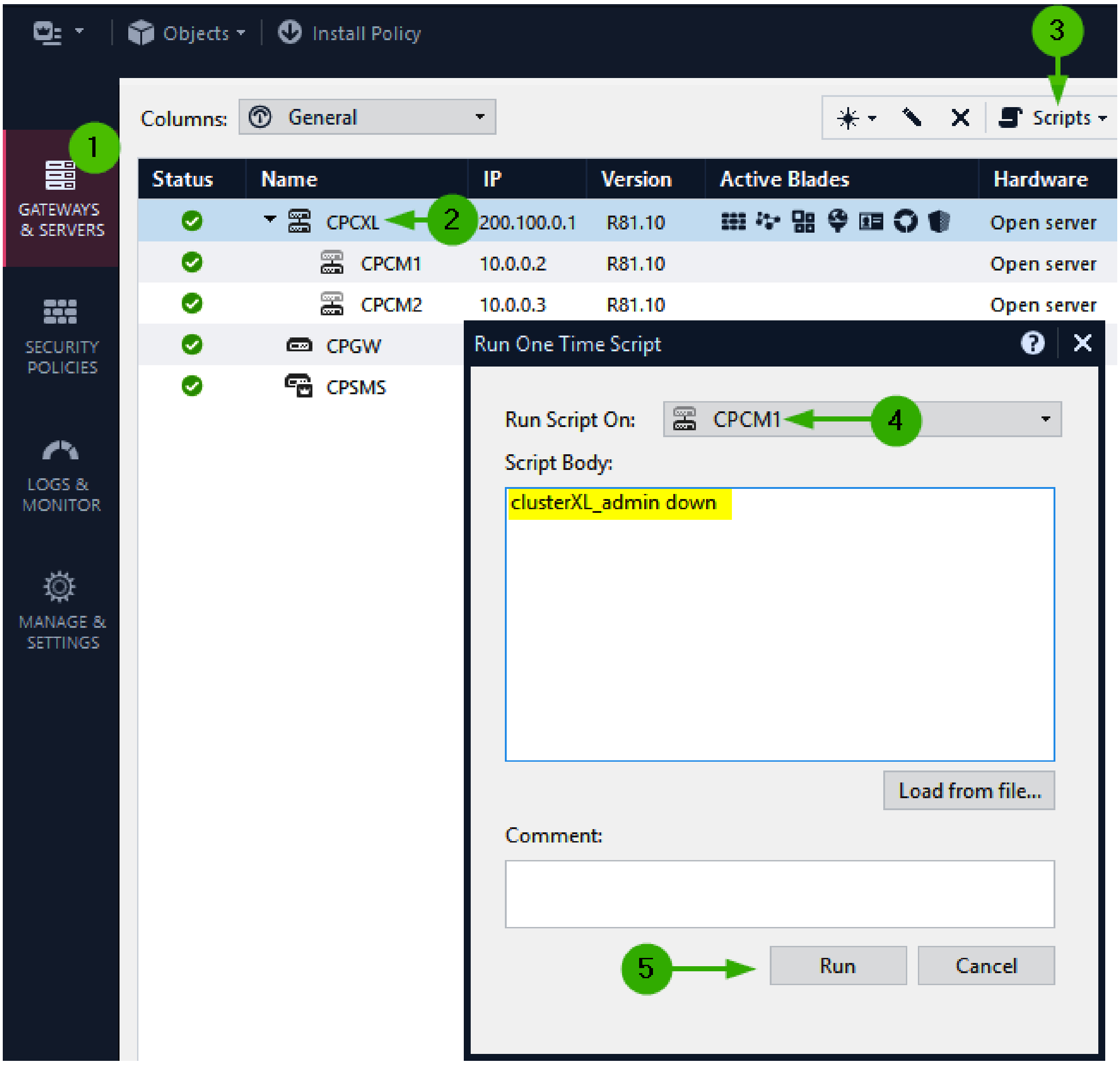
```
No.  Time      Source      Destination  Protocol  Length  Info
  181 18.153204 10.10.10.3  10.10.10.2   CPHA        92 CPHAv4101: FWHA_MY_STATE - Report source machine's state
  182 18.253700 10.10.10.3  10.10.10.2   CPHA        74 CPHAv4101: FWHA_IF_PROBE_REQ - Interface active check request
  183 18.654113 10.10.10.3  10.10.10.2   CPHA        92 CPHAv4101: FWHA_MY_STATE - Report source machine's state
  184 18.775177 10.10.10.2  10.10.10.3   CPHA        74 CPHAv4101: FWHA_IF_PROBE_REQ - Interface active check request
  185 18.775303 10.10.10.2  10.10.10.3   CPHA        92 CPHAv4101: FWHA_MY_STATE - Report source machine's state
  186 18.775327 10.10.10.3  10.10.10.2   CPHA        74 CPHAv4101: FWHA_IF_PROBE_REPLY - Interface active check reply
  187 18.875126 10.10.10.2  10.10.10.3   CPHA        92 CPHAv4101: FWHA_MY_STATE - Report source machine's state
```



No.	Time	Source	Destination	Protocol	Length	Info
546	7.298944	192.168.25…	192.168.2…	CPHA	82	CPHAv4101: FWHAP_SYNC - New Sync packet
547	7.308964	192.168.25…	192.168.2…	CPHA	710	CPHAv4101: FWHAP_SYNC - New Sync packet



```
CPCM1> show cluster statistics sync

Delta Sync Statistics

Sync status: OK

Drops:
Lost updates.................................  0
Lost bulk update events......................  0
Oversized updates not sent...................  0

Sync at risk:
Sent reject notifications....................  0
Received reject notifications................  0

Sent messages:
Total generated sync messages................  89123
Sent retransmission requests.................  0
Sent retransmission updates..................  0
Peak fragments per update....................  1

Received messages:
Total received updates.......................  491333
Received retransmission requests.............  0

Sync Interface:
Name.........................................  eth3
Link speed...................................  1000Mb/s
Rate.........................................  13050 [Bps]
Peak rate....................................  13800 [Bps]
Link usage...................................   0%
Total........................................  855476[KB]

Queue sizes (num of updates):
Sending queue size...........................  512
Receiving queue size.........................  256
Fragments queue size.........................  50

Timers:
Delta Sync interval (ms).....................  100

Reset on Wed May 25 16:04:54 2022 (triggered by fullsync).

CPCM1>
```



Status	Name	IP	Version	Active Blades	Hardware
✓	CPCXL	200.100.0.1	R81.10		Open server
✓	CPCM1	10.0.0.2	R81.10		Open server
✓	CPCM2	10.0.0.3	R81.10		Open server
✓	CPGW				
✓	CPSMS				

Run One Time Script

Run Script On: CPCM1

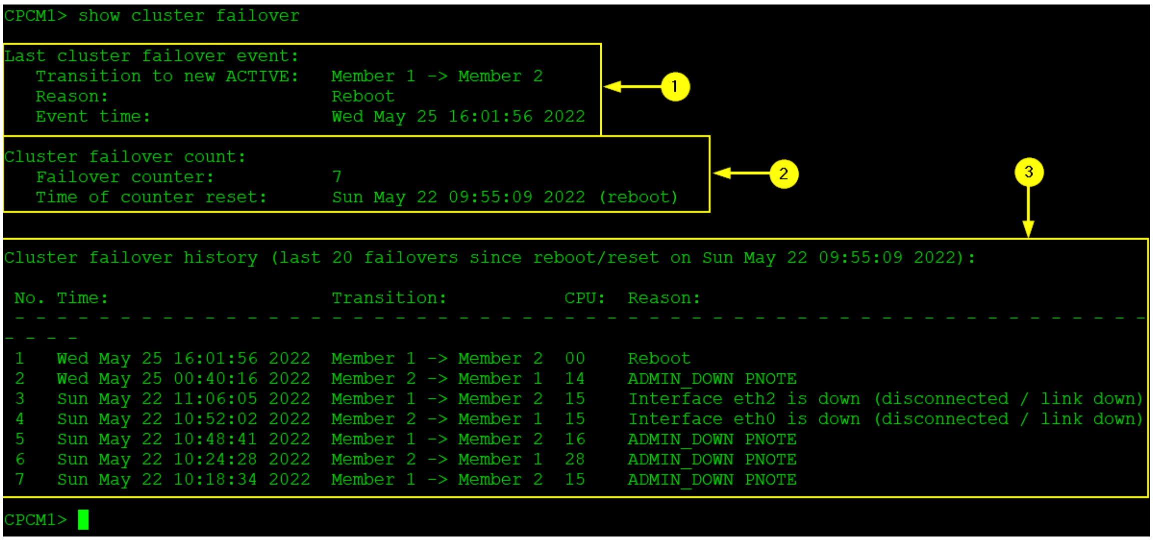
Script Body:

```
clusterXL_admin down
```

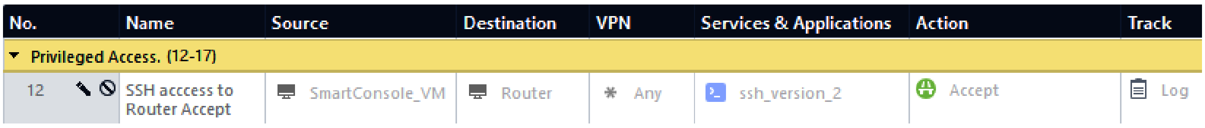
Load from file...

Comment:

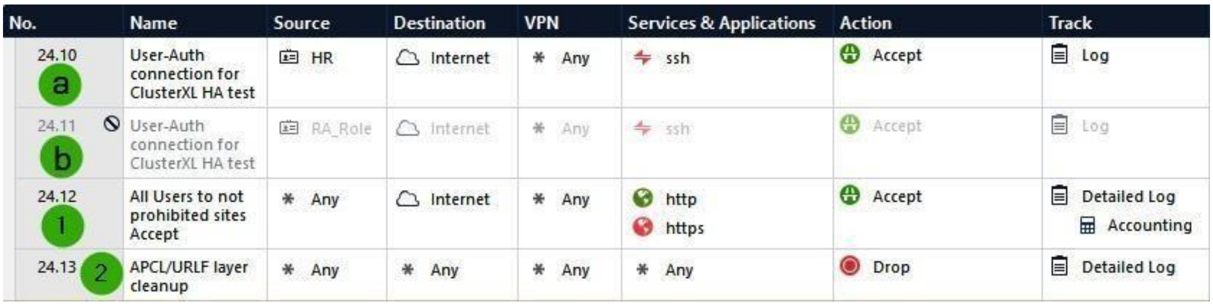
Run | Cancel



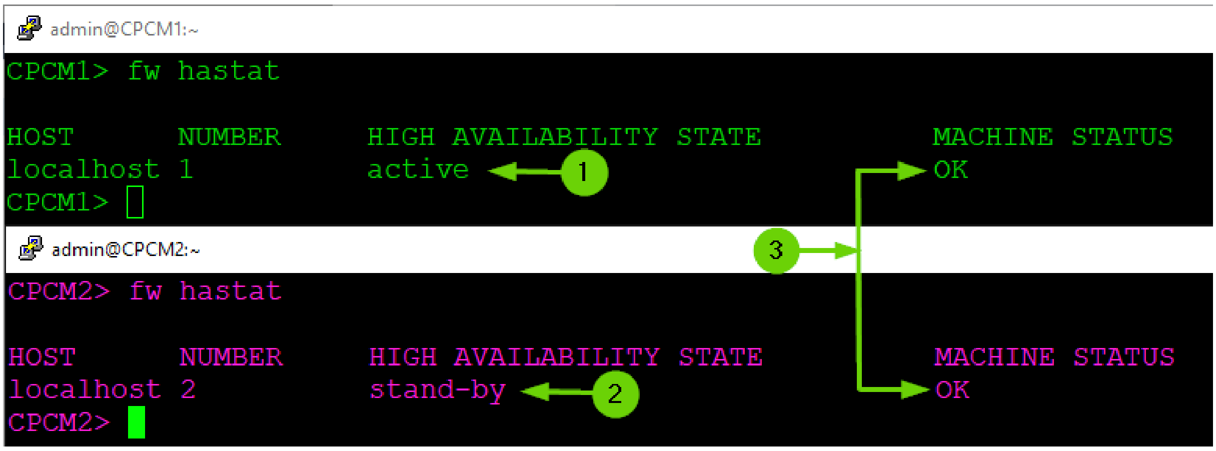
```
CPCM1> show cluster failover

Last cluster failover event:
   Transition to new ACTIVE:   Member 1 -> Member 2
   Reason:                     Reboot
   Event time:                 Wed May 25 16:01:56 2022

Cluster failover count:
   Failover counter:           7
   Time of counter reset:      Sun May 22 09:55:09 2022 (reboot)

Cluster failover history (last 20 failovers since reboot/reset on Sun May 22 09:55:09 2022):

 No. Time:                     Transition:           CPU:  Reason:
 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - -
 1   Wed May 25 16:01:56 2022  Member 1 -> Member 2  00    Reboot
 2   Wed May 25 00:40:16 2022  Member 2 -> Member 1  14    ADMIN_DOWN PNOTE
 3   Sun May 22 11:06:05 2022  Member 1 -> Member 2  15    Interface eth2 is down (disconnected / link down)
 4   Sun May 22 10:52:02 2022  Member 2 -> Member 1  15    Interface eth0 is down (disconnected / link down)
 5   Sun May 22 10:48:41 2022  Member 1 -> Member 2  16    ADMIN_DOWN PNOTE
 6   Sun May 22 10:24:28 2022  Member 2 -> Member 1  28    ADMIN_DOWN PNOTE
 7   Sun May 22 10:18:34 2022  Member 1 -> Member 2  15    ADMIN_DOWN PNOTE

CPCM1>
```



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
Privileged Access. (12-17)							
12	SSH acccess to Router Accept	SmartConsole_VM	Router	Any	ssh_version_2	Accept	Log



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
24.10	User-Auth connection for ClusterXL HA test	HR	Internet	Any	ssh	Accept	Log
24.11	User-Auth connection for ClusterXL HA test	RA_Role	Internet	Any	ssh	Accept	Log
24.12	All Users to not prohibited sites Accept	Any	Internet	Any	http https	Accept	Detailed Log Accounting
24.13	APCL/URLF layer cleanup	Any	Any	Any	Any	Drop	Detailed Log

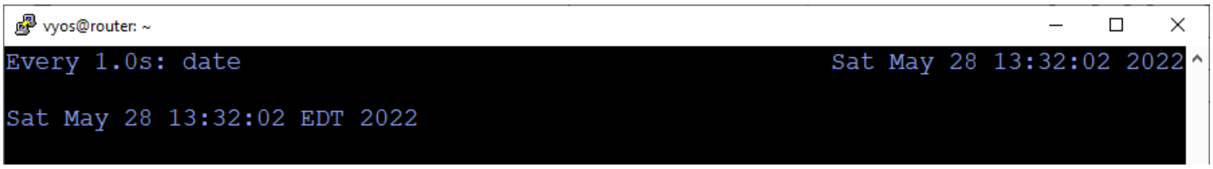


admin@CPCM1:~

```
CPCM1> fw hastat

HOST      NUMBER     HIGH AVAILABILITY STATE          MACHINE STATUS
localhost 1          active                           OK
CPCM1>
```

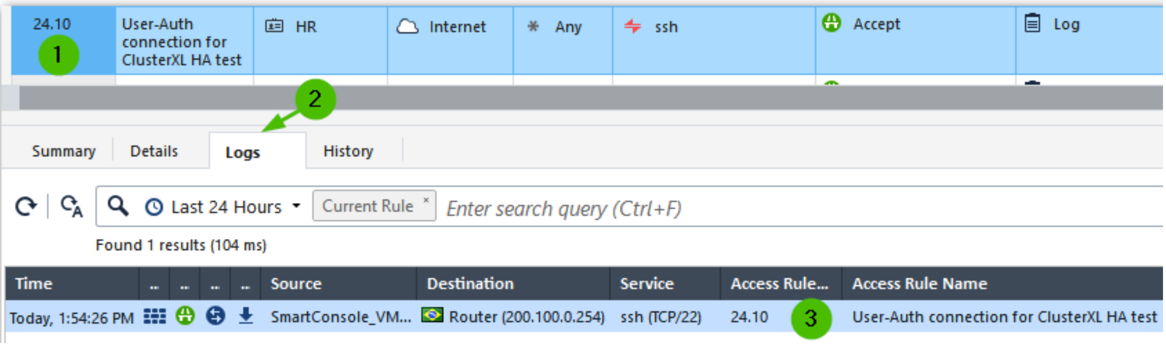
admin@CPCM2:~

```
CPCM2> fw hastat

HOST      NUMBER     HIGH AVAILABILITY STATE          MACHINE STATUS
localhost 2          stand-by                         OK
CPCM2>
```



vyos@router: ~

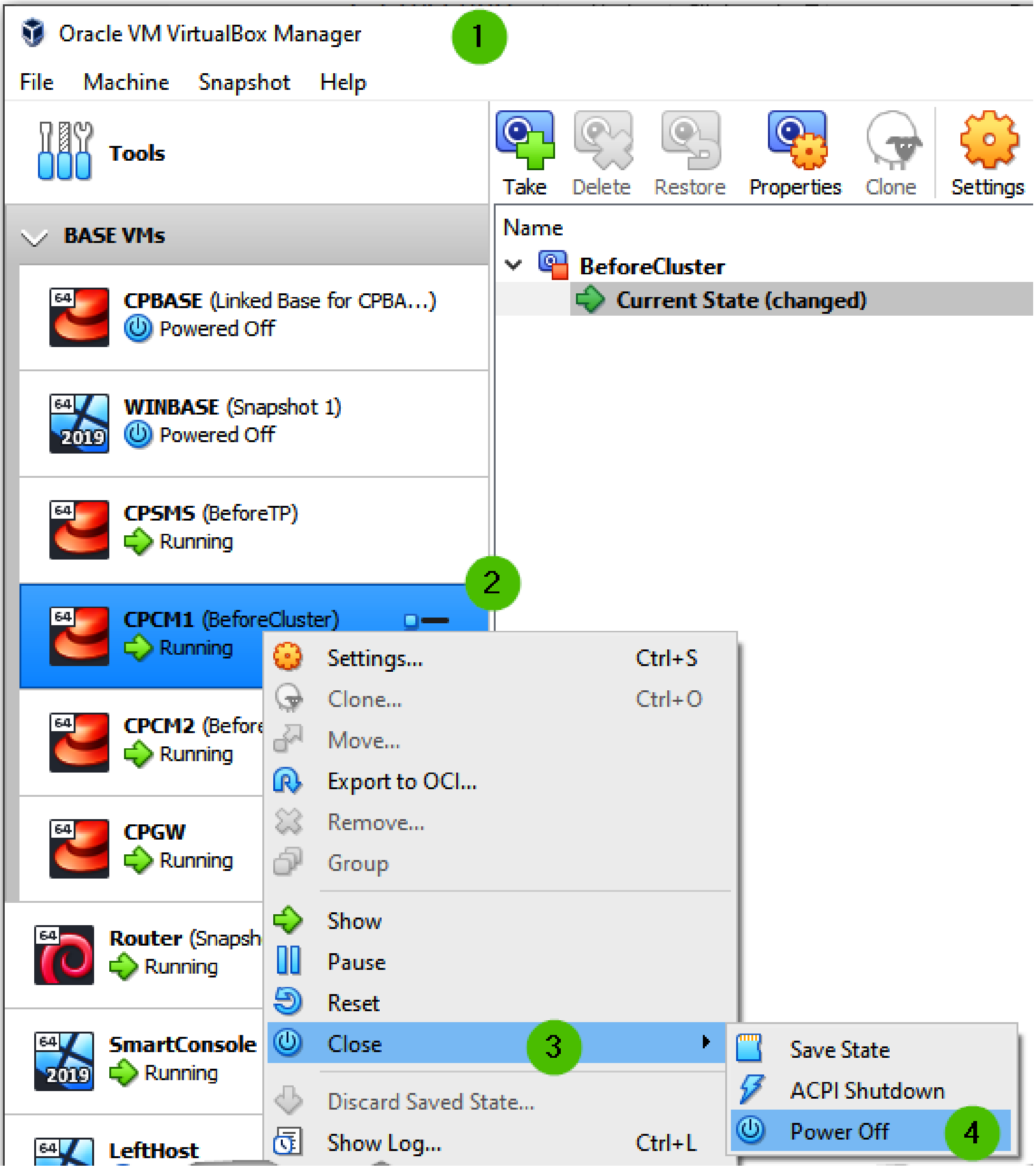
```
Every 1.0s: date                                    Sat May 28 13:32:02 2022

Sat May 28 13:32:02 EDT 2022
```

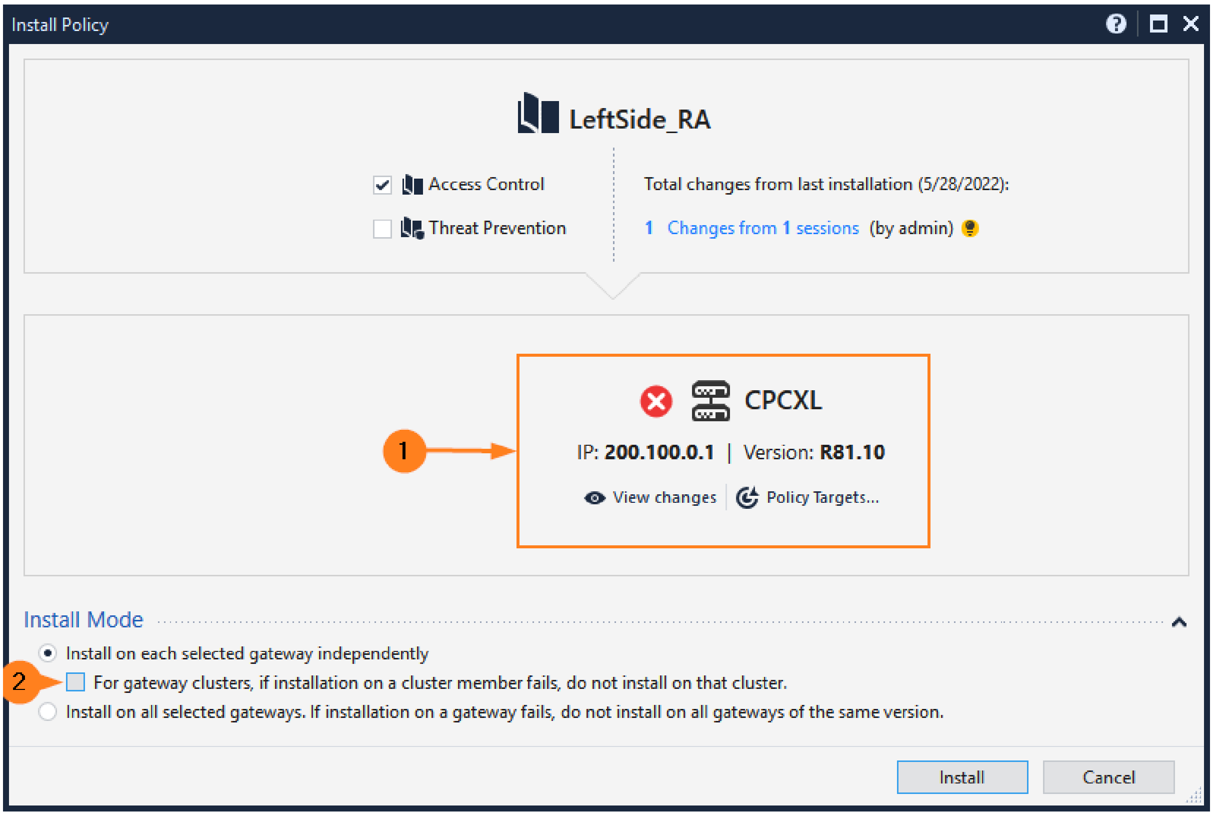


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
24.10	User-Auth connection for ClusterXL HA test	HR	Internet	Any	ssh	Accept	Log

Found 1 results (104 ms)

Time	..	..	..	..	Source	Destination	Service	Access Rule...	Access Rule Name
Today, 1:54:26 PM					SmartConsole_VM...	Router (200.100.0.254)	ssh (TCP/22)	24.10	User-Auth connection for ClusterXL HA test


Oracle VM VirtualBox Manager
1
File
Machine
Snapshot
Help
Tools
Take
Delete
Restore
Properties
Clone
Settings
Name
BeforeCluster
Current State (changed)
BASE VMs
CPBASE (Linked Base for CPBA…)
Powered Off
WINBASE (Snapshot 1)
Powered Off
CPSMS (BeforeTP)
Running
2
CPCM1 (BeforeCluster)
Running
CPCM2 (Before
Running
CPGW
Running
Router (Snapsh
Running
SmartConsole
Running
LeftHost
Settings... Ctrl+S
Clone... Ctrl+O
Move...
Export to OCI...
Remove...
Group
Show
Pause
Reset
Close
3
Discard Saved State...
Show Log... Ctrl+L
Save State
ACPI Shutdown
Power Off
4



☑ Access Control

□ Threat Prevention

Total changes from last installation (5/28/2022):

1 Changes from 1 sessions (by admin)

CPCXL

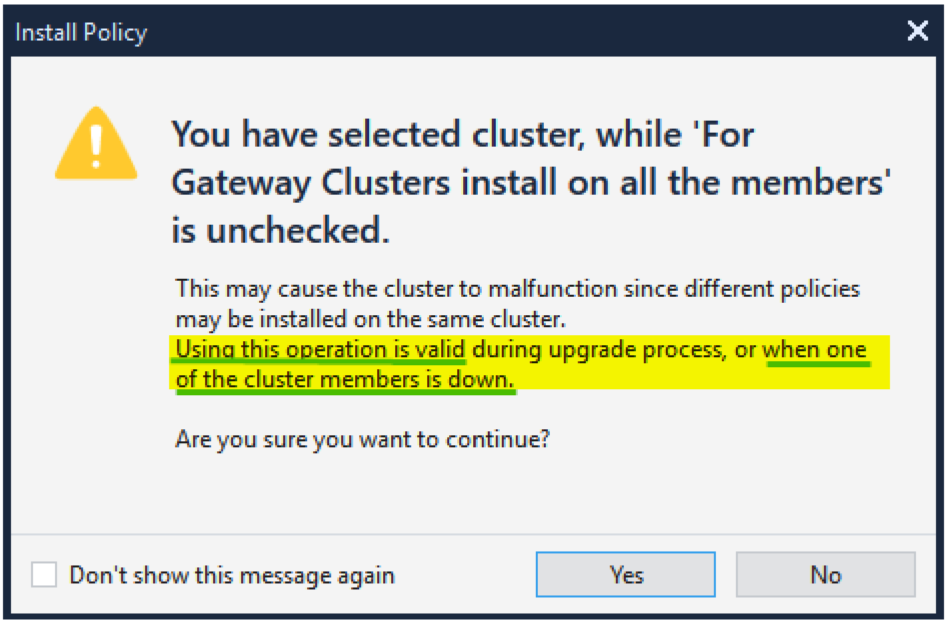
IP: **200.100.0.1** | Version: **R81.10**

Install Mode

● Install on each selected gateway independently

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

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

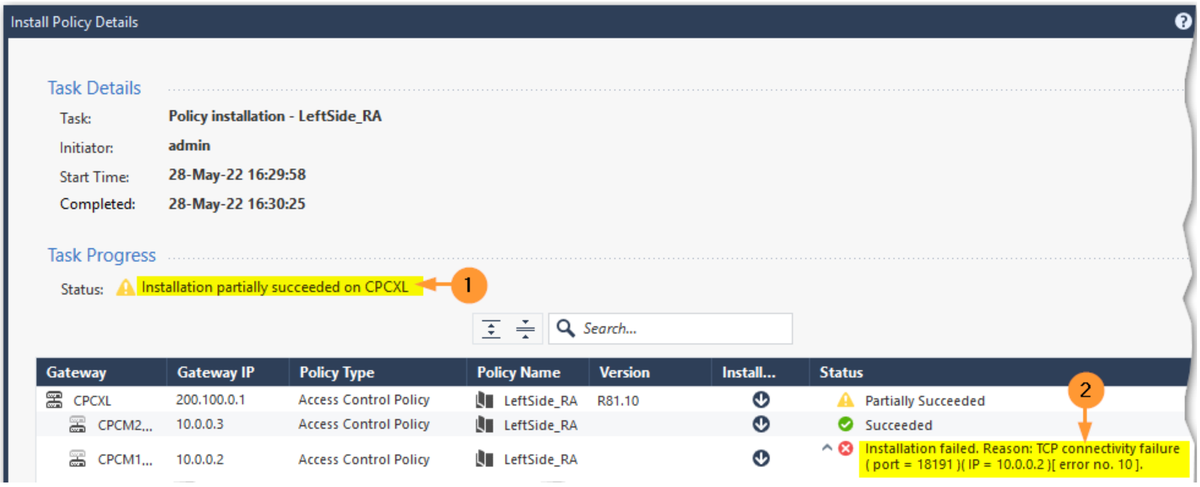


You have selected cluster, while 'For Gateway Clusters install on all the members' is unchecked.

This may cause the cluster to malfunction since different policies may be installed on the same cluster.
Using this operation is valid during upgrade process, or when one of the cluster members is down.

Are you sure you want to continue?

□ Don't show this message again



Install Policy Details

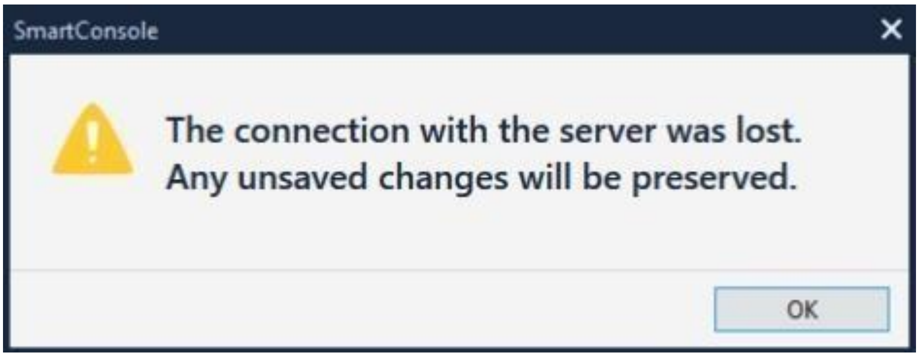
Task Details

Task:	Policy installation - LeftSide_RA
Initiator:	admin
Start Time:	28-May-22 16:29:58
Completed:	28-May-22 16:30:25

Task Progress

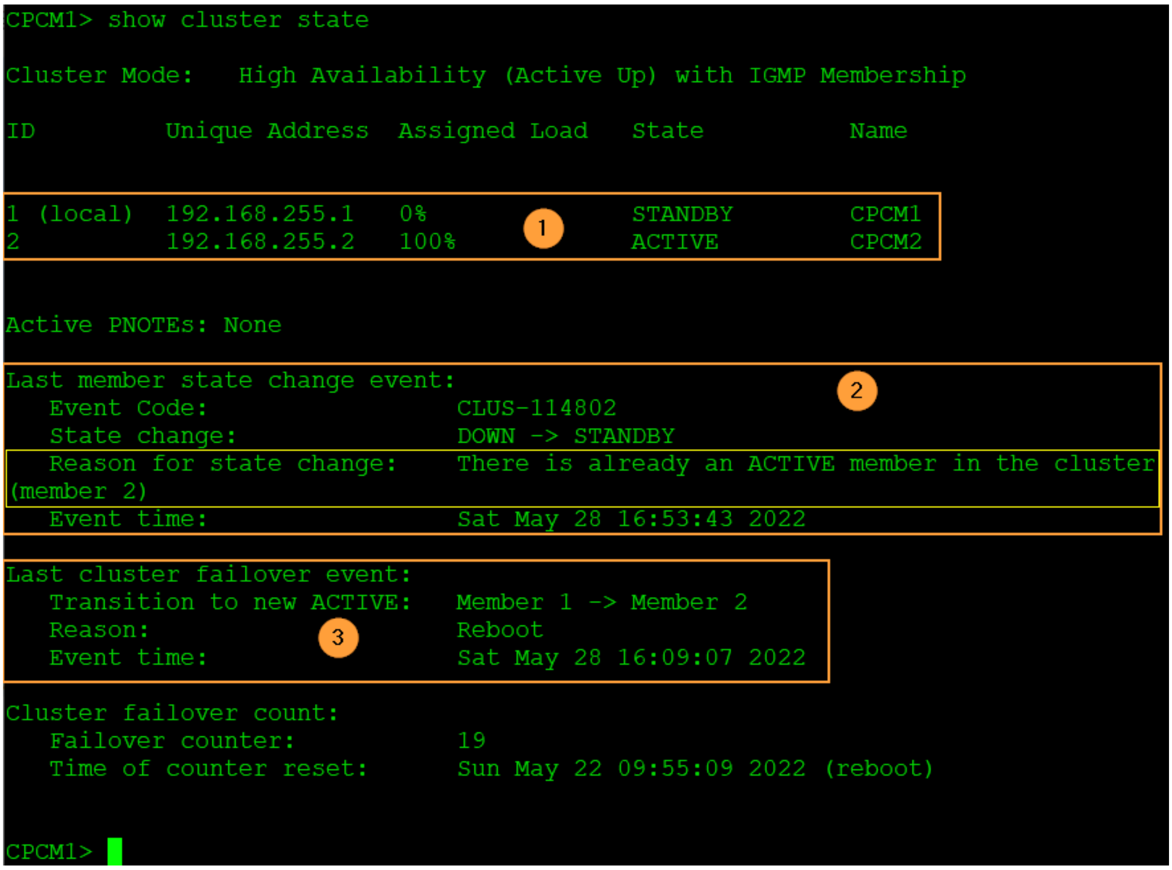
Status: ⚠ Installation partially succeeded on CPCXL

Gateway	Gateway IP	Policy Type	Policy Name	Version	Install...	Status
CPCXL	200.100.0.1	Access Control Policy	LeftSide_RA	R81.10	⬇	⚠ Partially Succeeded
CPCM2,...	10.0.0.3	Access Control Policy	LeftSide_RA		⬇	✓ Succeeded
CPCM1,...	10.0.0.2	Access Control Policy	LeftSide_RA		⬇	✖ Installation failed. Reason: TCP connectivity failure (port = 18191)(IP = 10.0.0.2)[error no. 10].

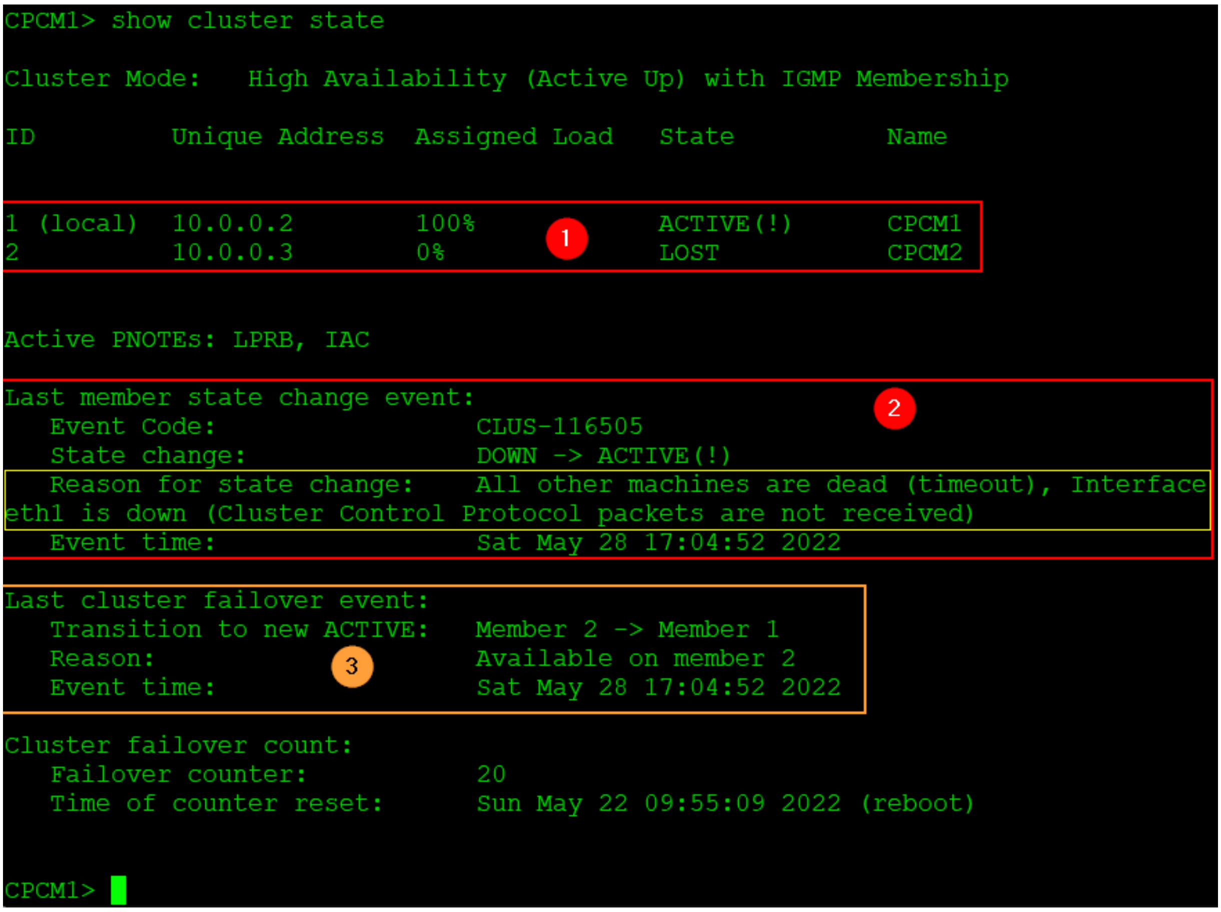


SmartConsole

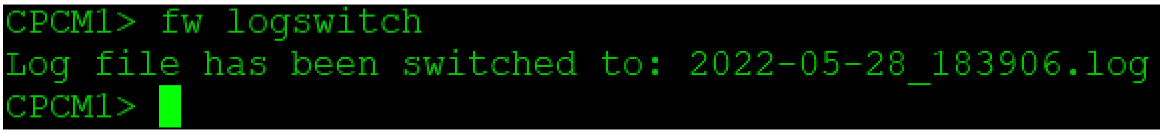
The connection with the server was lost.
Any unsaved changes will be preserved.



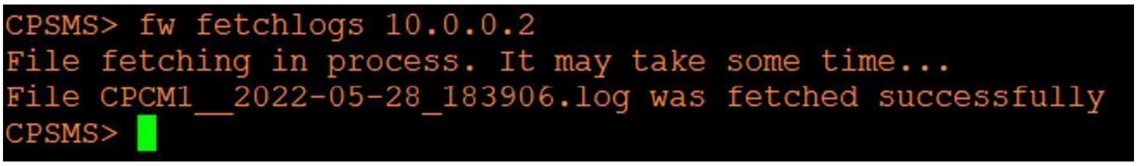
```
CPCM1> show cluster state

Cluster Mode:   High Availability (Active Up) with IGMP Membership

ID          Unique Address  Assigned Load   State          Name


1 (local)   192.168.255.1   0%              STANDBY        CPCM1
2           192.168.255.2   100%            ACTIVE         CPCM2


Active PNOTEs: None

Last member state change event:
   Event Code:                  CLUS-114802
   State change:                DOWN -> STANDBY
   Reason for state change:     There is already an ACTIVE member in the cluster
(member 2)
   Event time:                  Sat May 28 16:53:43 2022

Last cluster failover event:
   Transition to new ACTIVE:    Member 1 -> Member 2
   Reason:                      Reboot
   Event time:                  Sat May 28 16:09:07 2022

Cluster failover count:
   Failover counter:            19
   Time of counter reset:       Sun May 22 09:55:09 2022 (reboot)


CPCM1>
```



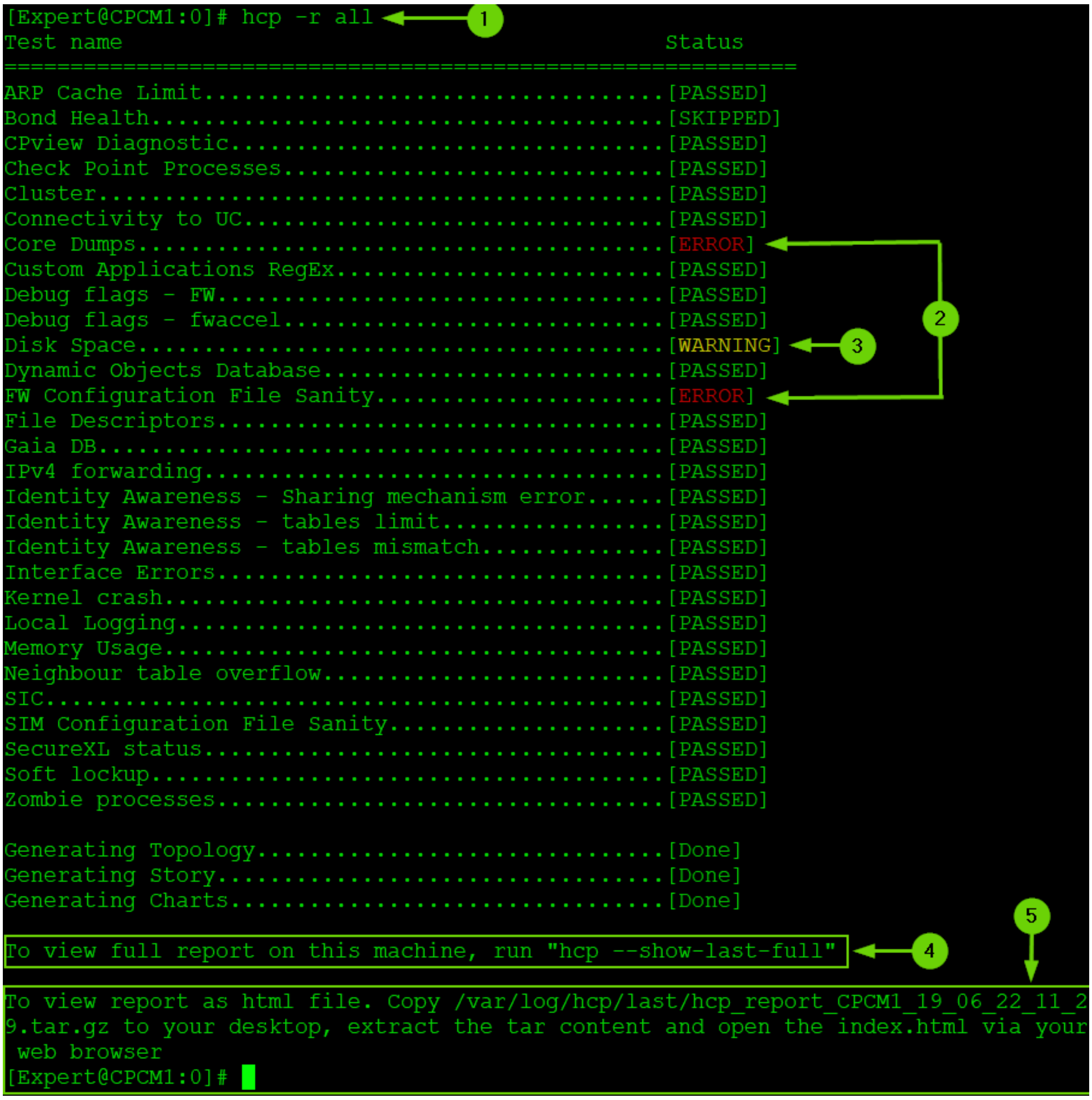
```
CPCM1> show cluster state

Cluster Mode:   High Availability (Active Up) with IGMP Membership

ID          Unique Address  Assigned Load   State          Name


1 (local)   10.0.0.2        100%            ACTIVE(!)      CPCM1
2           10.0.0.3        0%              LOST           CPCM2


Active PNOTEs: LPRB, IAC

Last member state change event:
   Event Code:                CLUS-116505
   State change:              DOWN -> ACTIVE(!)
   Reason for state change:   All other machines are dead (timeout), Interface
eth1 is down (Cluster Control Protocol packets are not received)
   Event time:                Sat May 28 17:04:52 2022

Last cluster failover event:
   Transition to new ACTIVE:  Member 2 -> Member 1
   Reason:                    Available on member 2
   Event time:                Sat May 28 17:04:52 2022

Cluster failover count:
   Failover counter:          20
   Time of counter reset:     Sun May 22 09:55:09 2022 (reboot)


CPCM1>
```



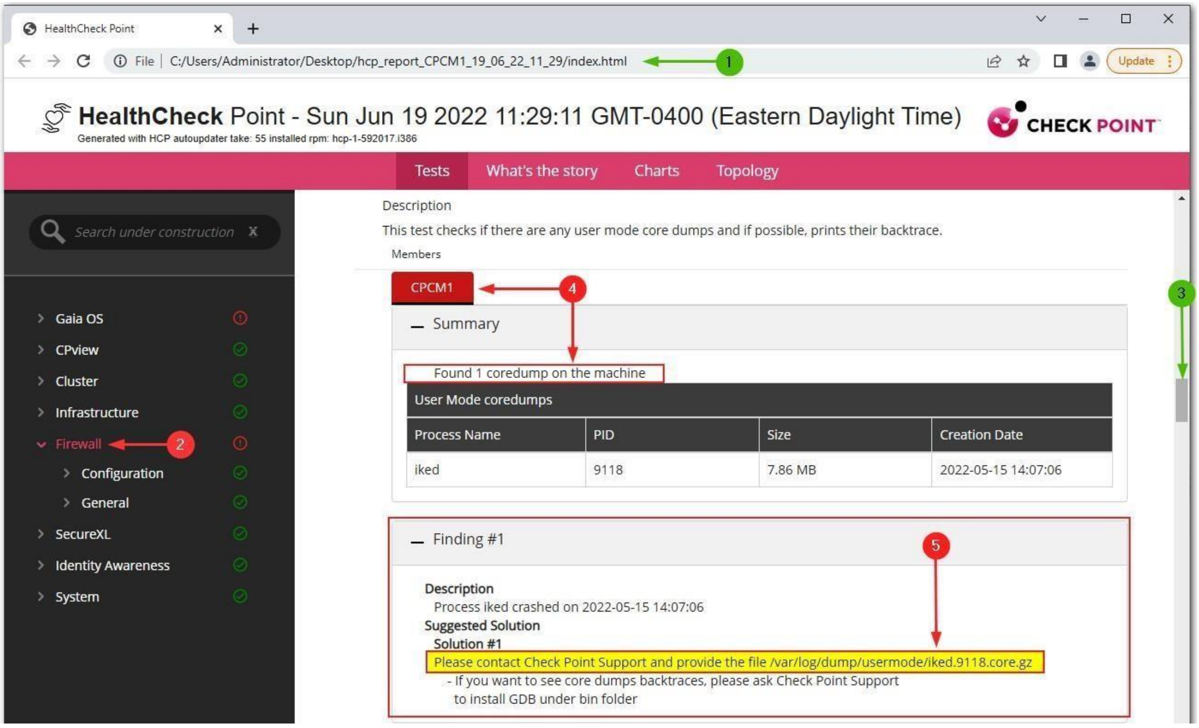
```
CPCM1> fw logswitch
Log file has been switched to: 2022-05-28_183906.log
CPCM1>
```



```
CPSMS> fw fetchlogs 10.0.0.2
File fetching in process. It may take some time...
File CPCM1__2022-05-28_183906.log was fetched successfully
CPSMS>
```



```
[Expert@CPCM1:0]# hcp -r all
Test name                                                 Status
============================================================
ARP Cache Limit..................................[PASSED]
Bond Health......................................[SKIPPED]
CPview Diagnostic................................[PASSED]
Check Point Processes............................[PASSED]
Cluster..........................................[PASSED]
Connectivity to UC...............................[PASSED]
Core Dumps.......................................[ERROR]
Custom Applications RegEx........................[PASSED]
Debug flags - FW.................................[PASSED]
Debug flags - fwaccel............................[PASSED]
Disk Space.......................................[WARNING]
Dynamic Objects Database.........................[PASSED]
FW Configuration File Sanity.....................[ERROR]
File Descriptors.................................[PASSED]
Gaia DB..........................................[PASSED]
IPv4 forwarding..................................[PASSED]
Identity Awareness - Sharing mechanism error.....[PASSED]
Identity Awareness - tables limit................[PASSED]
Identity Awareness - tables mismatch.............[PASSED]
Interface Errors.................................[PASSED]
Kernel crash.....................................[PASSED]
Local Logging....................................[PASSED]
Memory Usage.....................................[PASSED]
Neighbour table overflow.........................[PASSED]
SIC..............................................[PASSED]
SIM Configuration File Sanity....................[PASSED]
SecureXL status..................................[PASSED]
Soft lockup......................................[PASSED]
Zombie processes.................................[PASSED]

Generating Topology..............................[Done]
Generating Story.................................[Done]
Generating Charts................................[Done]

To view full report on this machine, run "hcp --show-last-full"

To view report as html file. Copy /var/log/hcp/last/hcp_report_CPCM1_19_06_22_11_2
9.tar.gz to your desktop, extract the tar content and open the index.html via your
 web browser
[Expert@CPCM1:0]#
```



HealthCheck Point - Sun Jun 19 2022 11:29:11 GMT-0400 (Eastern Daylight Time)

Generated with HCP autoupdater take: 55 installed rpm: hcp-1-592017.i386

Description

This test checks if there are any user mode core dumps and if possible, prints their backtrace.

Members

CPCM1

— Summary

Found 1 coredump on the machine

User Mode coredumps

Process Name	PID	Size	Creation Date
iked	9118	7.86 MB	2022-05-15 14:07:06

— Finding #1

Description

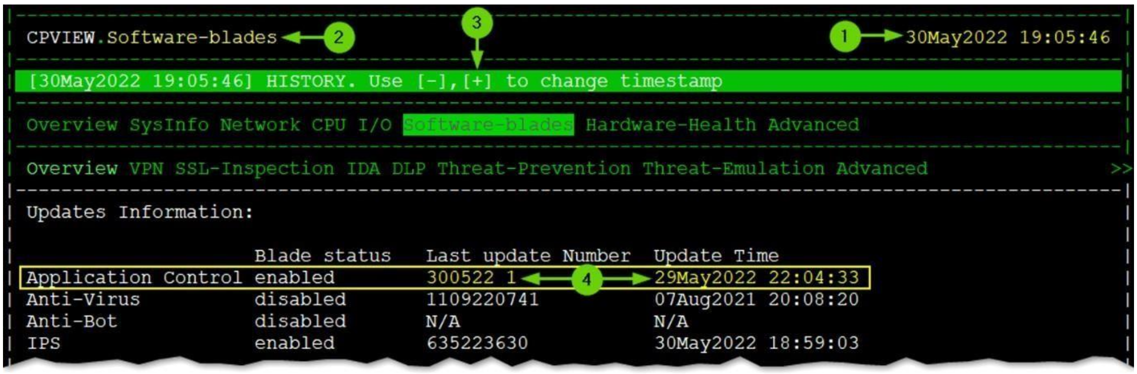
Process iked crashed on 2022-05-15 14:07:06

Suggested Solution

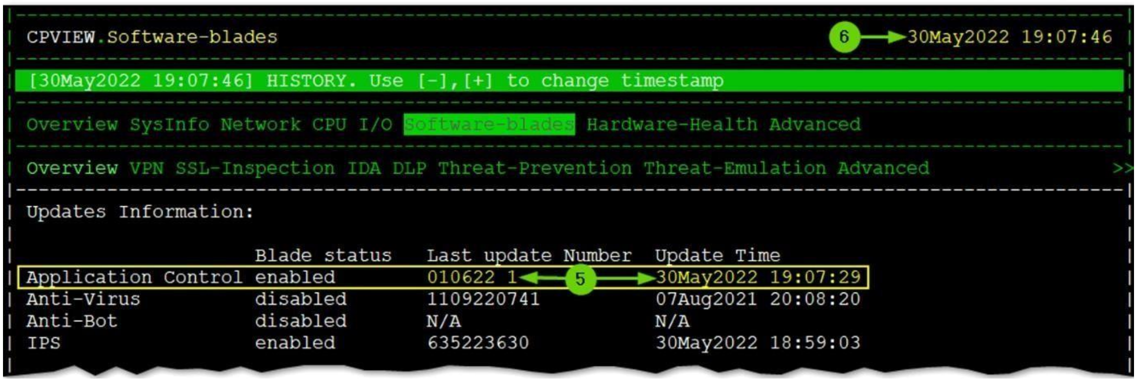
Solution #1

Please contact Check Point Support and provide the file /var/log/dump/usermode/iked.9118.core.gz

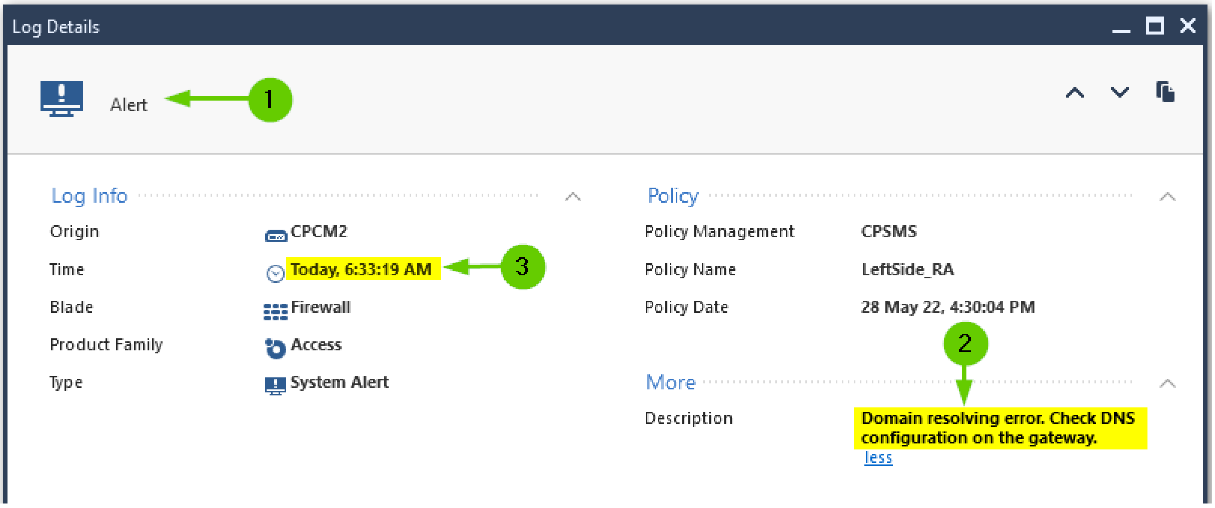
- If you want to see core dumps backtraces, please ask Check Point Support to install GDB under bin folder



```
|-------------------------------------------------------------------------------------|
| CPVIEW.Software-blades                                          30May2022 19:05:46 |
|-------------------------------------------------------------------------------------|
| [30May2022 19:05:46] HISTORY. Use [-],[+] to change timestamp                       |
|-------------------------------------------------------------------------------------|
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced           |
|-------------------------------------------------------------------------------------|
| Overview VPN SSL-Inspection IDA DLP Threat-Prevention Threat-Emulation Advanced   >>
|-------------------------------------------------------------------------------------|
| Updates Information:                                                                |
|                                                                                     |
|                     Blade status  Last update Number  Update Time                   |
| Application Control enabled       300522 1            29May2022 22:04:33            |
| Anti-Virus          disabled      1109220741          07Aug2021 20:08:20            |
| Anti-Bot            disabled      N/A                 N/A                           |
| IPS                 enabled       635223630           30May2022 18:59:03            |
```



```
|-------------------------------------------------------------------------------------|
| CPVIEW.Software-blades                                          30May2022 19:07:46 |
|-------------------------------------------------------------------------------------|
| [30May2022 19:07:46] HISTORY. Use [-],[+] to change timestamp                       |
|-------------------------------------------------------------------------------------|
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced           |
|-------------------------------------------------------------------------------------|
| Overview VPN SSL-Inspection IDA DLP Threat-Prevention Threat-Emulation Advanced   >>
|-------------------------------------------------------------------------------------|
| Updates Information:                                                                |
|                                                                                     |
|                     Blade status  Last update Number  Update Time                   |
| Application Control enabled       010622 1            30May2022 19:07:29            |
| Anti-Virus          disabled      1109220741          07Aug2021 20:08:20            |
| Anti-Bot            disabled      N/A                 N/A                           |
| IPS                 enabled       635223630           30May2022 18:59:03            |
|
```



Log Details

Alert

Log Info

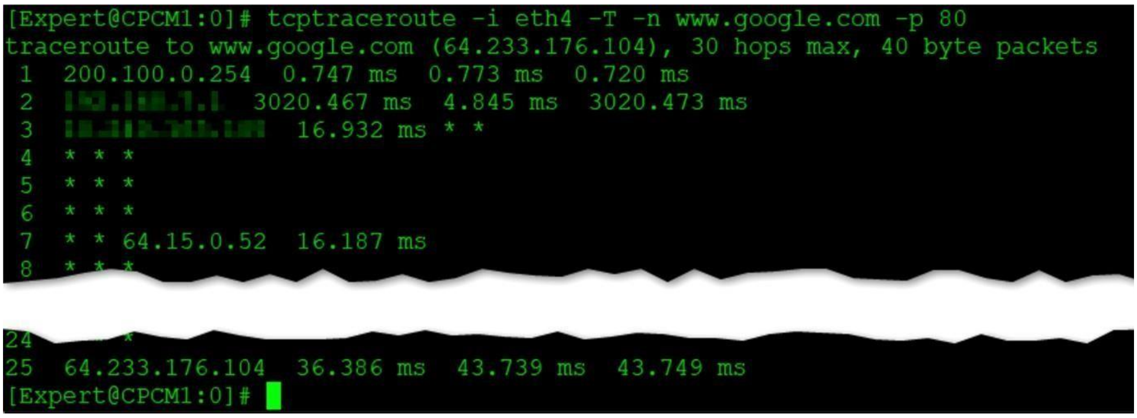
Origin	CPCM2
Time	Today, 6:33:19 AM
Blade	Firewall
Product Family	Access
Type	System Alert

Policy

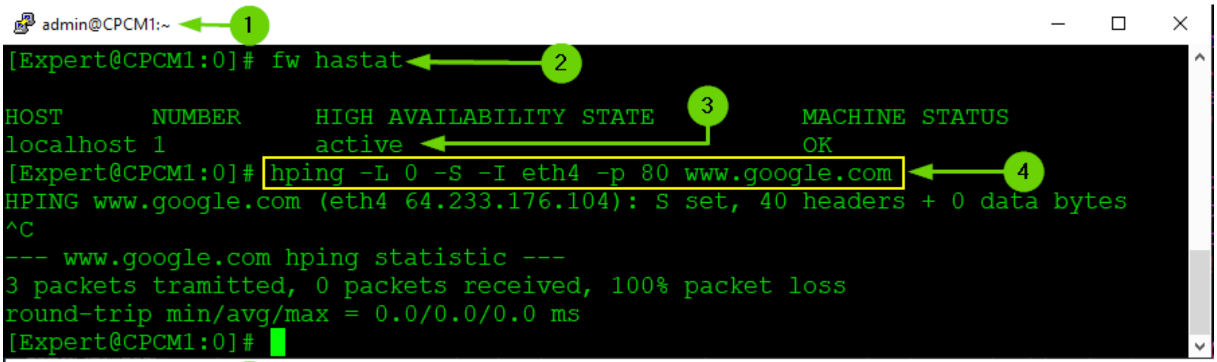
Policy Management	CPSMS
Policy Name	LeftSide_RA
Policy Date	28 May 22, 4:30:04 PM

More

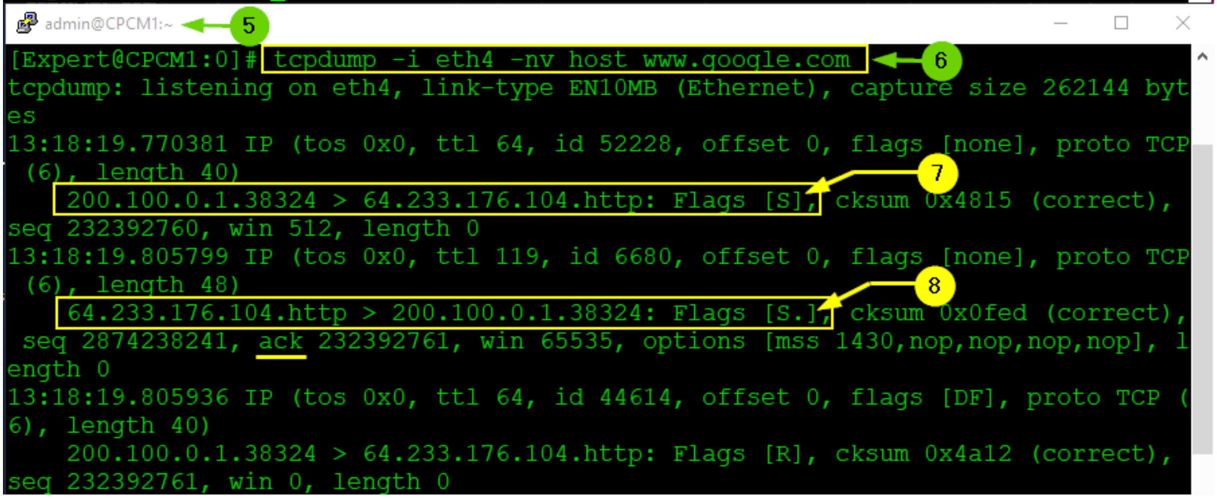
Description: Domain resolving error. Check DNS configuration on the gateway.
less



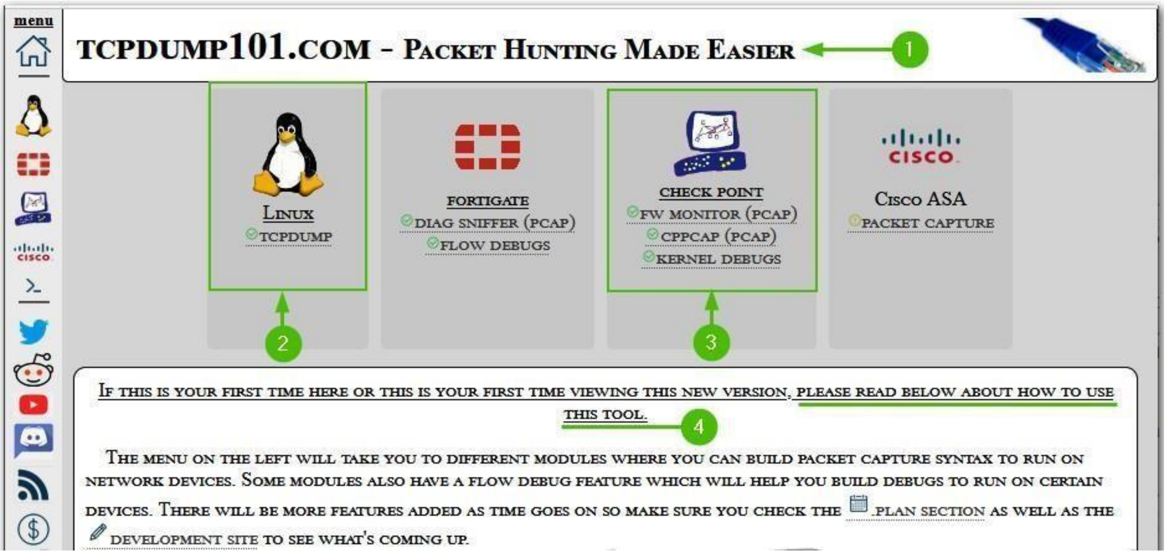
```
[Expert@CPCM1:0]# tcptraceroute -i eth4 -T -n www.google.com -p 80
traceroute to www.google.com (64.233.176.104), 30 hops max, 40 byte packets
 1  200.100.0.254  0.747 ms  0.773 ms  0.720 ms
 2  [redacted]  3020.467 ms  4.845 ms  3020.473 ms
 3  [redacted]  16.932 ms * *
 4  * * *
 5  * * *
 6  * * *
 7  * * 64.15.0.52  16.187 ms
 8  * * *
24    *
25  64.233.176.104  36.386 ms  43.739 ms  43.749 ms
[Expert@CPCM1:0]# 
```



```
[Expert@CPCM1:0]# fw hastat

HOST       NUMBER      HIGH AVAILABILITY STATE       MACHINE STATUS
localhost 1            active                        OK
[Expert@CPCM1:0]# hping -L 0 -S -I eth4 -p 80 www.google.com
HPING www.google.com (eth4 64.233.176.104): S set, 40 headers + 0 data bytes
^C
--- www.google.com hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[Expert@CPCM1:0]#
```

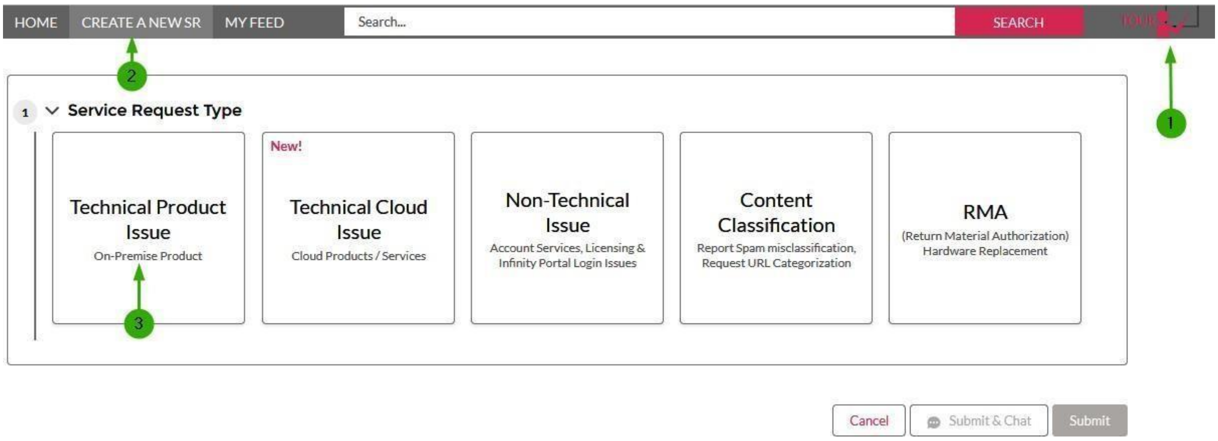


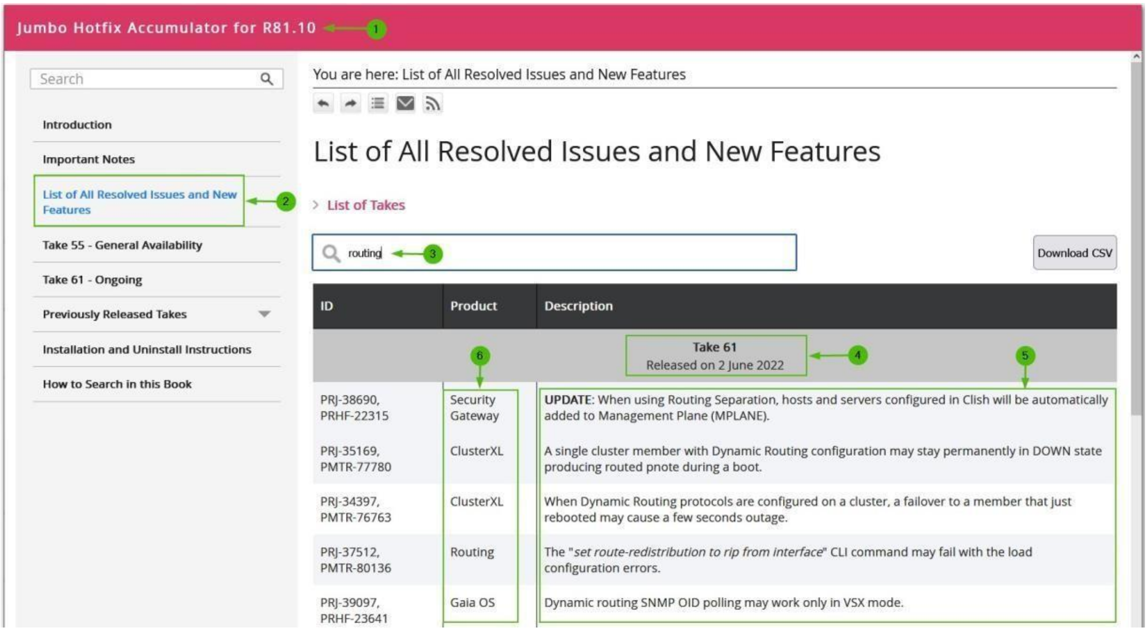
```
[Expert@CPCM1:0]# tcpdump -i eth4 -nv host www.google.com
tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture size 262144 byt
es
13:18:19.770381 IP (tos 0x0, ttl 64, id 52228, offset 0, flags [none], proto TCP
 (6), length 40)
    200.100.0.1.38324 > 64.233.176.104.http: Flags [S], cksum 0x4815 (correct),
seq 232392760, win 512, length 0
13:18:19.805799 IP (tos 0x0, ttl 119, id 6680, offset 0, flags [none], proto TCP
 (6), length 48)
    64.233.176.104.http > 200.100.0.1.38324: Flags [S.], cksum 0x0fed (correct),
 seq 2874238241, ack 232392761, win 65535, options [mss 1430,nop,nop,nop,nop], l
ength 0
13:18:19.805936 IP (tos 0x0, ttl 64, id 44614, offset 0, flags [DF], proto TCP (
6), length 40)
    200.100.0.1.38324 > 64.233.176.104.http: Flags [R], cksum 0x4a12 (correct),
seq 232392761, win 0, length 0
```



If this is your first time here or this is your first time viewing this new version, please read below about how to use this tool.

The menu on the left will take you to different modules where you can build packet capture syntax to run on network devices. Some modules also have a flow debug feature which will help you build debugs to run on certain devices. There will be more features added as time goes on so make sure you check the plan section as well as the development site to see what's coming up.



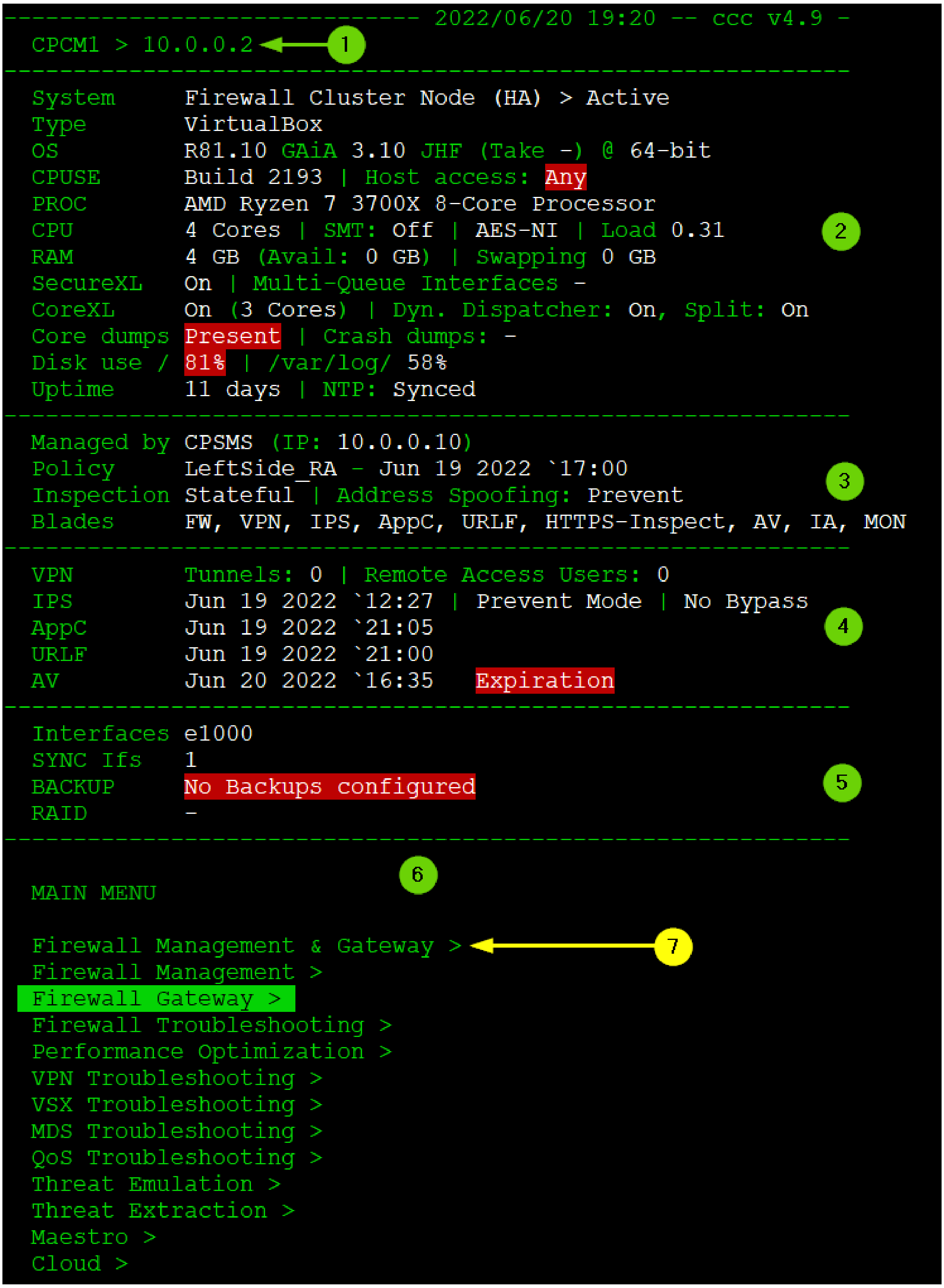

Jumbo Hotfix Accumulator for R81.10
1
Search
Introduction
Important Notes
List of All Resolved Issues and New Features
2
Take 55 - General Availability
Take 61 - Ongoing
Previously Released Takes
Installation and Uninstall Instructions
How to Search in this Book
routing
3
Download CSV
4
5
6

You are here: List of All Resolved Issues and New Features

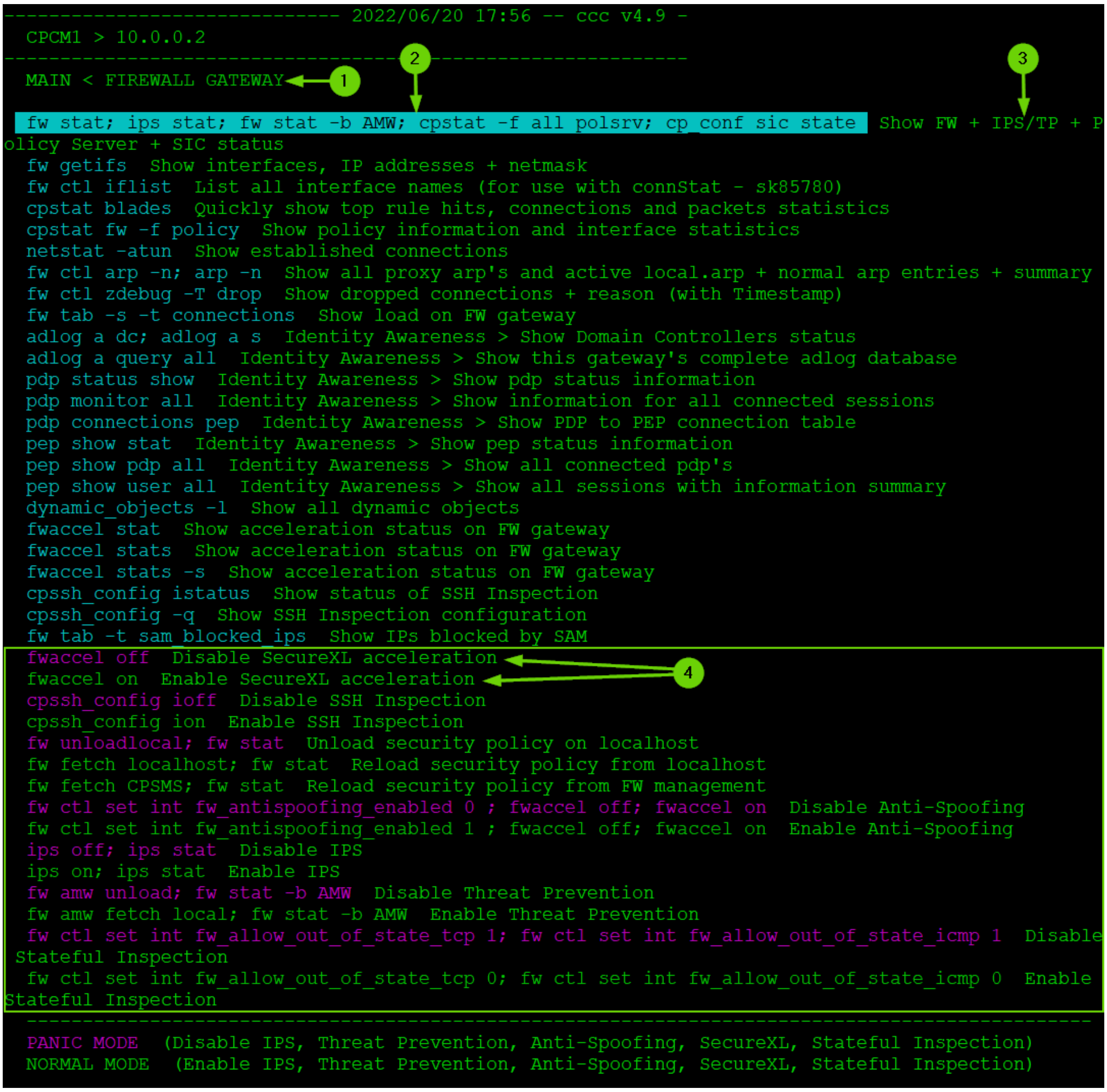
List of All Resolved Issues and New Features

> List of Takes

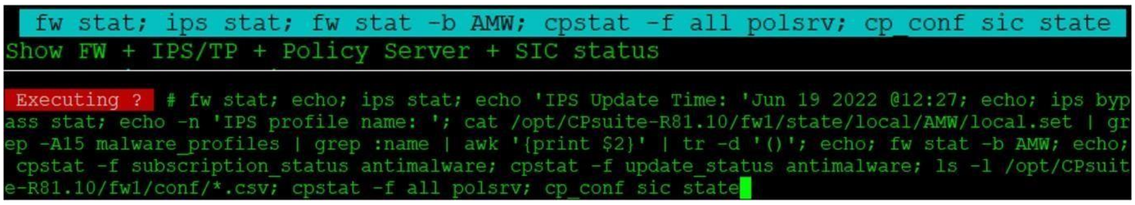
ID	Product	Description
		Take 61 Released on 2 June 2022
PRJ-38690, PRHF-22315	Security Gateway	**UPDATE**: When using Routing Separation, hosts and servers configured in Clish will be automatically added to Management Plane (MPLANE).
PRJ-35169, PMTR-77780	ClusterXL	A single cluster member with Dynamic Routing configuration may stay permanently in DOWN state producing routed pnote during a boot.
PRJ-34397, PMTR-76763	ClusterXL	When Dynamic Routing protocols are configured on a cluster, a failover to a member that just rebooted may cause a few seconds outage.
PRJ-37512, PMTR-80136	Routing	The "*set route-redistribution to rip from interface*" CLI command may fail with the load configuration errors.
PRJ-39097, PRHF-23641	Gaia OS	Dynamic routing SNMP OID polling may work only in VSX mode.



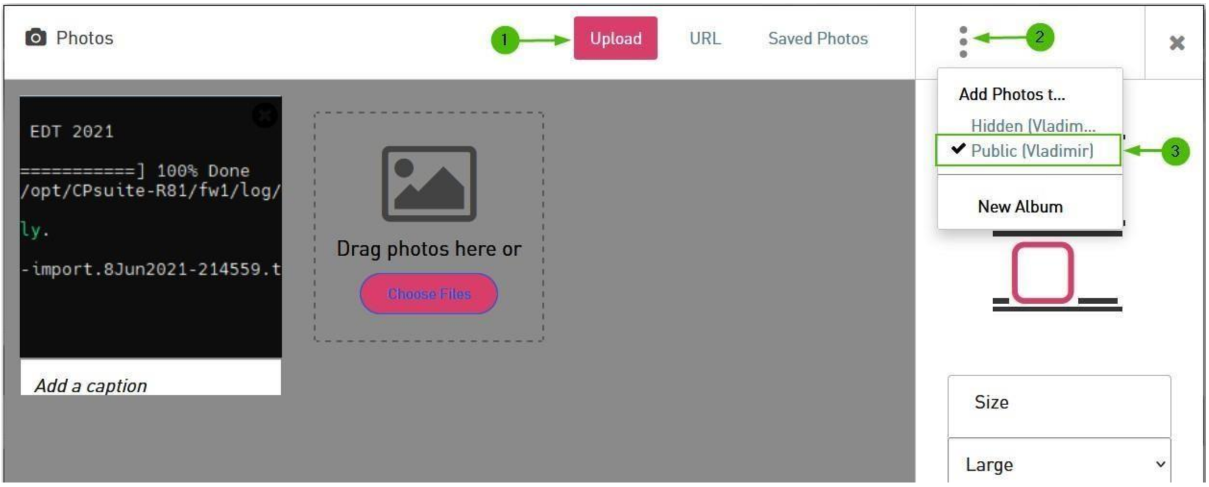
```
------------------------------ 2022/06/20 19:20 -- ccc v4.9 -
  CPCM1 > 10.0.0.2
-------------------------------------------------------------
  System      Firewall Cluster Node (HA) > Active
  Type        VirtualBox
  OS          R81.10 GAiA 3.10 JHF (Take -) @ 64-bit
  CPUSE       Build 2193 | Host access: Any
  PROC        AMD Ryzen 7 3700X 8-Core Processor
  CPU         4 Cores | SMT: Off | AES-NI | Load 0.31
  RAM         4 GB (Avail: 0 GB) | Swapping 0 GB
  SecureXL    On | Multi-Queue Interfaces -
  CoreXL      On (3 Cores) | Dyn. Dispatcher: On, Split: On
  Core dumps  Present | Crash dumps: -
  Disk use /  81% | /var/log/ 58%
  Uptime      11 days | NTP: Synced
-------------------------------------------------------------
  Managed by  CPSMS (IP: 10.0.0.10)
  Policy      LeftSide_RA - Jun 19 2022 `17:00
  Inspection  Stateful | Address Spoofing: Prevent
  Blades      FW, VPN, IPS, AppC, URLF, HTTPS-Inspect, AV, IA, MON
-------------------------------------------------------------
  VPN         Tunnels: 0 | Remote Access Users: 0
  IPS         Jun 19 2022 `12:27 | Prevent Mode | No Bypass
  AppC        Jun 19 2022 `21:05
  URLF        Jun 19 2022 `21:00
  AV          Jun 20 2022 `16:35   Expiration
-------------------------------------------------------------
  Interfaces  e1000
  SYNC Ifs    1
  BACKUP      No Backups configured
  RAID        -
-------------------------------------------------------------

  MAIN MENU

  Firewall Management & Gateway >
  Firewall Management >
  Firewall Gateway >
  Firewall Troubleshooting >
  Performance Optimization >
  VPN Troubleshooting >
  VSX Troubleshooting >
  MDS Troubleshooting >
  QoS Troubleshooting >
  Threat Emulation >
  Threat Extraction >
  Maestro >
  Cloud >
```



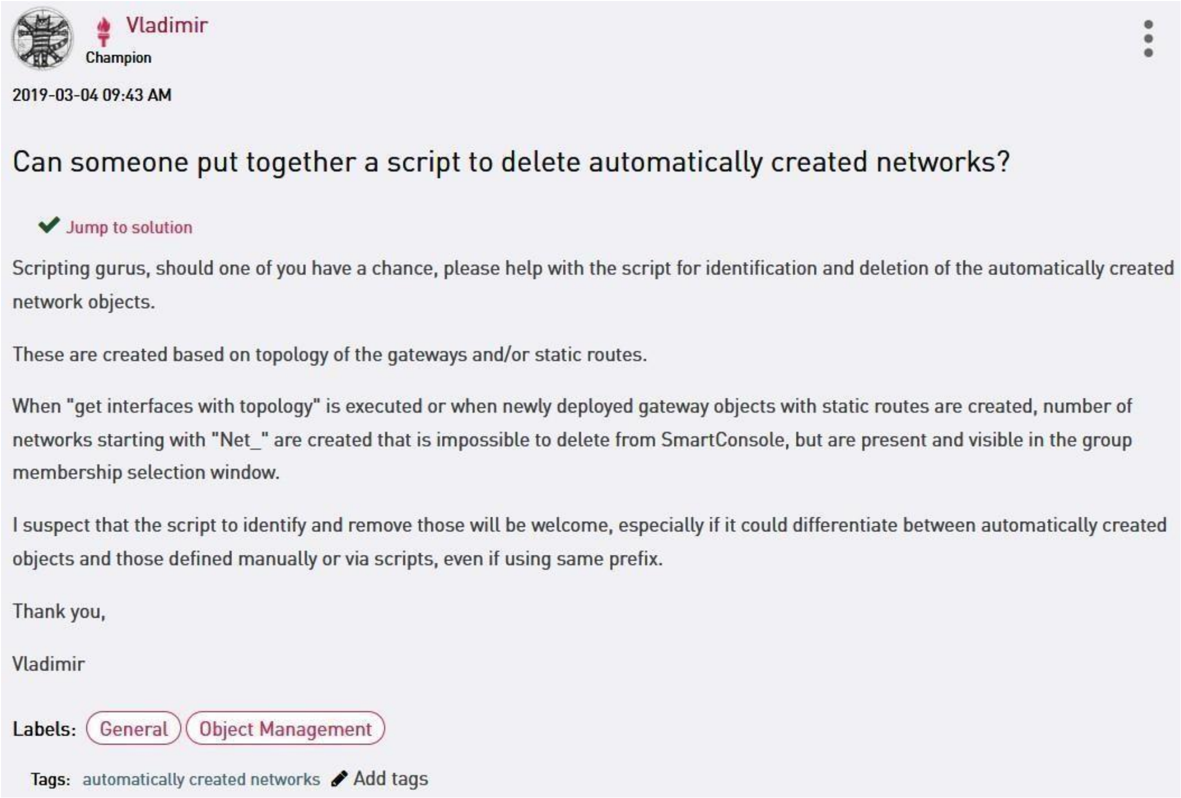
```
------------------------------ 2022/06/20 17:56 -- ccc v4.9 -
  CPCM1 > 10.0.0.2
-------------------------------------------------------------
  MAIN < FIREWALL GATEWAY

  fw stat; ips stat; fw stat -b AMW; cpstat -f all polsrv; cp_conf sic state  Show FW + IPS/TP + P
olicy Server + SIC status
  fw getifs  Show interfaces, IP addresses + netmask
  fw ctl iflist  List all interface names (for use with connStat - sk85780)
  cpstat blades  Quickly show top rule hits, connections and packets statistics
  cpstat fw -f policy  Show policy information and interface statistics
  netstat -atun  Show established connections
  fw ctl arp -n; arp -n  Show all proxy arp's and active local.arp + normal arp entries + summary
  fw ctl zdebug -T drop  Show dropped connections + reason (with Timestamp)
  fw tab -s -t connections  Show load on FW gateway
  adlog a dc; adlog a s  Identity Awareness > Show Domain Controllers status
  adlog a query all  Identity Awareness > Show this gateway's complete adlog database
  pdp status show  Identity Awareness > Show pdp status information
  pdp monitor all  Identity Awareness > Show information for all connected sessions
  pdp connections pep  Identity Awareness > Show PDP to PEP connection table
  pep show stat  Identity Awareness > Show pep status information
  pep show pdp all  Identity Awareness > Show all connected pdp's
  pep show user all  Identity Awareness > Show all sessions with information summary
  dynamic_objects -l  Show all dynamic objects
  fwaccel stat  Show acceleration status on FW gateway
  fwaccel stats  Show acceleration status on FW gateway
  fwaccel stats -s  Show acceleration status on FW gateway
  cpssh_config istatus  Show status of SSH Inspection
  cpssh_config -q  Show SSH Inspection configuration
  fw tab -t sam_blocked_ips  Show IPs blocked by SAM
  fwaccel off  Disable SecureXL acceleration
  fwaccel on  Enable SecureXL acceleration
  cpssh_config ioff  Disable SSH Inspection
  cpssh_config ion  Enable SSH Inspection
  fw unloadlocal; fw stat  Unload security policy on localhost
  fw fetch localhost; fw stat  Reload security policy from localhost
  fw fetch CPSMS; fw stat  Reload security policy from FW management
  fw ctl set int fw_antispoofing_enabled 0 ; fwaccel off; fwaccel on  Disable Anti-Spoofing
  fw ctl set int fw_antispoofing_enabled 1 ; fwaccel off; fwaccel on  Enable Anti-Spoofing
  ips off; ips stat  Disable IPS
  ips on; ips stat  Enable IPS
  fw amw unload; fw stat -b AMW  Disable Threat Prevention
  fw amw fetch local; fw stat -b AMW  Enable Threat Prevention
  fw ctl set int fw_allow_out_of_state_tcp 1; fw ctl set int fw_allow_out_of_state_icmp 1  Disable
 Stateful Inspection
  fw ctl set int fw_allow_out_of_state_tcp 0; fw ctl set int fw_allow_out_of_state_icmp 0  Enable
Stateful Inspection
  ------------------------------------------------------------------------------------------------

  PANIC MODE  (Disable IPS, Threat Prevention, Anti-Spoofing, SecureXL, Stateful Inspection)
  NORMAL MODE  (Enable IPS, Threat Prevention, Anti-Spoofing, SecureXL, Stateful Inspection)
```



```
  fw stat; ips stat; fw stat -b AMW; cpstat -f all polsrv; cp_conf sic state
Show FW + IPS/TP + Policy Server + SIC status

 Executing ?  # fw stat; echo; ips stat; echo 'IPS Update Time: 'Jun 19 2022 @12:27; echo; ips byp
ass stat; echo -n 'IPS profile name: '; cat /opt/CPsuite-R81.10/fw1/state/local/AMW/local.set | gr
ep -A15 malware_profiles | grep :name | awk '{print $2}' | tr -d '()'; echo; fw stat -b AMW; echo;
 cpstat -f subscription_status antimalware; cpstat -f update_status antimalware; ls -l /opt/CPsuit
e-R81.10/fw1/conf/*.csv; cpstat -f all polsrv; cp_conf sic state
```



```
 EDT 2021

===========] 100% Done
/opt/CPsuite-R81/fw1/log/

ly.

-import.8Jun2021-214559.t
```



Vladimir
Champion

2019-03-04 09:43 AM

Can someone put together a script to delete automatically created networks?

✓ Jump to solution

Scripting gurus, should one of you have a chance, please help with the script for identification and deletion of the automatically created network objects.

These are created based on topology of the gateways and/or static routes.

When "get interfaces with topology" is executed or when newly deployed gateway objects with static routes are created, number of networks starting with "Net_" are created that is impossible to delete from SmartConsole, but are present and visible in the group membership selection window.

I suspect that the script to identify and remove those will be welcome, especially if it could differentiate between automatically created objects and those defined manually or via scripts, even if using same prefix.

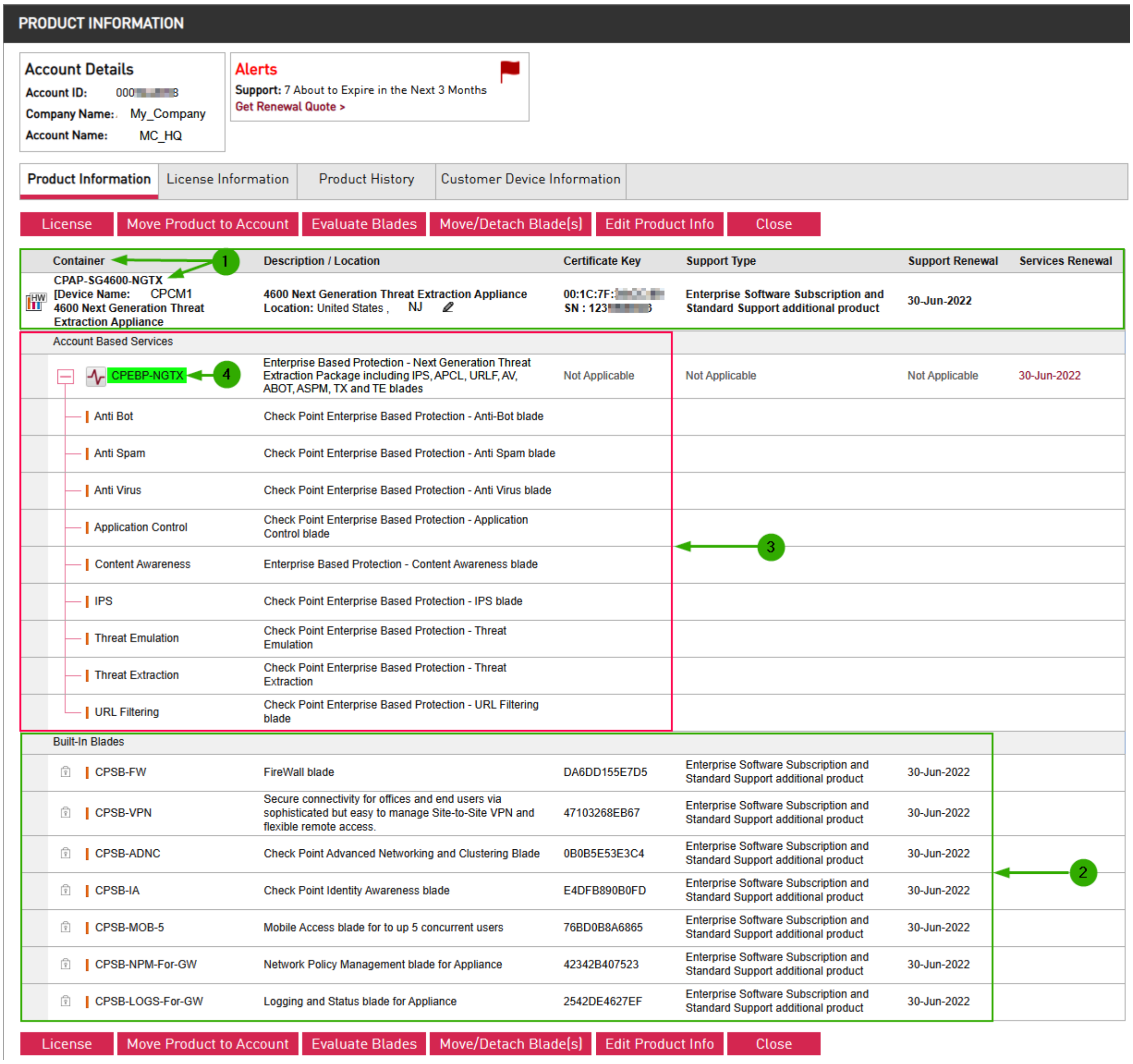
Thank you,

Vladimir

Labels: General Object Management

Tags: automatically created networks Add tags

Appendix



Account Details

Account ID: 000[redacted]3

Company Name: My_Company

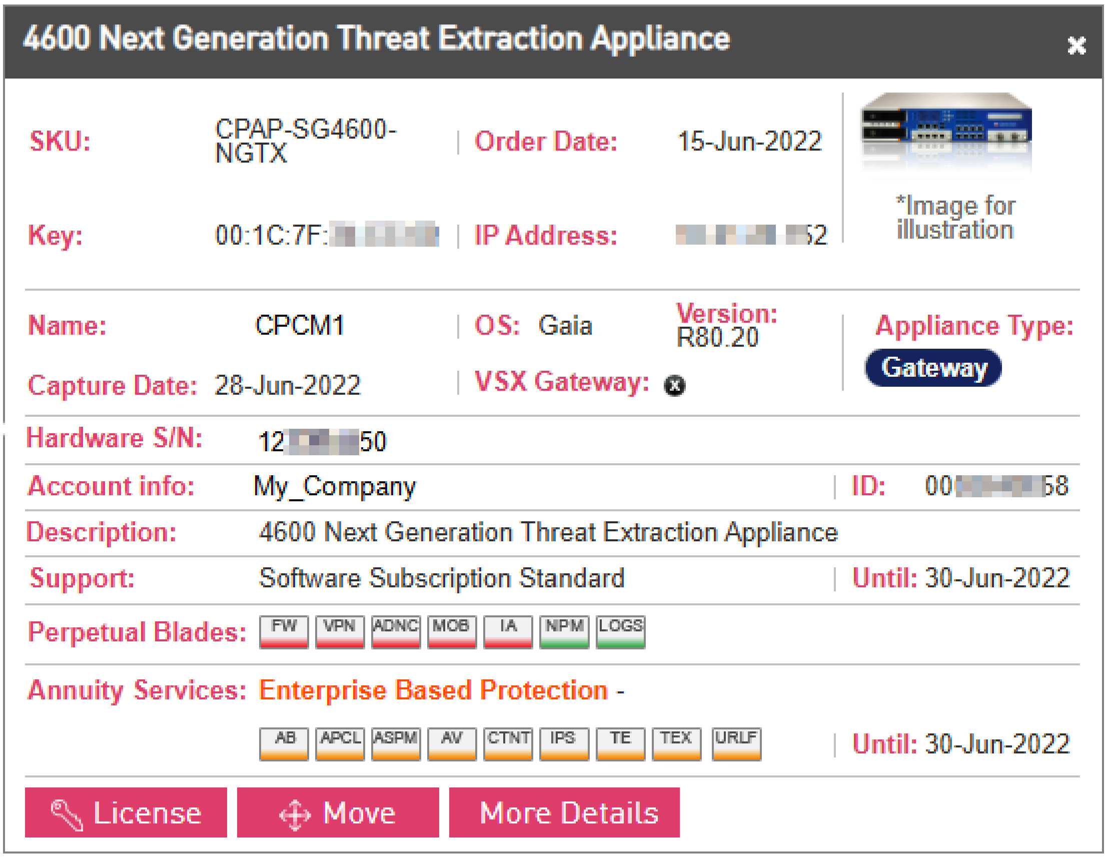
Account Name: MC_HQ

Alerts

Support: 7 About to Expire in the Next 3 Months

Get Renewal Quote >

Container	Description / Location	Certificate Key	Support Type	Support Renewal	Services Renewal
CPAP-SG4600-NGTX [Device Name: CPCM1 4600 Next Generation Threat Extraction Appliance	**4600 Next Generation Threat Extraction Appliance** **Location:** United States , NJ	**00:1C:7F:[redacted]** **SN : 123[redacted]3**	**Enterprise Software Subscription and Standard Support additional product**	**30-Jun-2022**	
Account Based Services					
CPEBP-NGTX	Enterprise Based Protection - Next Generation Threat Extraction Package including IPS, APCL, URLF, AV, ABOT, ASPM, TX and TE blades	Not Applicable	Not Applicable	Not Applicable	30-Jun-2022
Anti Bot	Check Point Enterprise Based Protection - Anti-Bot blade				
Anti Spam	Check Point Enterprise Based Protection - Anti Spam blade				
Anti Virus	Check Point Enterprise Based Protection - Anti Virus blade				
Application Control	Check Point Enterprise Based Protection - Application Control blade				
Content Awareness	Enterprise Based Protection - Content Awareness blade				
IPS	Check Point Enterprise Based Protection - IPS blade				
Threat Emulation	Check Point Enterprise Based Protection - Threat Emulation				
Threat Extraction	Check Point Enterprise Based Protection - Threat Extraction				
URL Filtering	Check Point Enterprise Based Protection - URL Filtering blade				
Built-In Blades					
CPSB-FW	FireWall blade	DA6DD155E7D5	Enterprise Software Subscription and Standard Support additional product	30-Jun-2022	
CPSB-VPN	Secure connectivity for offices and end users via sophisticated but easy to manage Site-to-Site VPN and flexible remote access.	47103268EB67	Enterprise Software Subscription and Standard Support additional product	30-Jun-2022	
CPSB-ADNC	Check Point Advanced Networking and Clustering Blade	0B0B5E53E3C4	Enterprise Software Subscription and Standard Support additional product	30-Jun-2022	
CPSB-IA	Check Point Identity Awareness blade	E4DFB890B0FD	Enterprise Software Subscription and Standard Support additional product	30-Jun-2022	
CPSB-MOB-5	Mobile Access blade for to up 5 concurrent users	76BD0B8A6865	Enterprise Software Subscription and Standard Support additional product	30-Jun-2022	
CPSB-NPM-For-GW	Network Policy Management blade for Appliance	42342B407523	Enterprise Software Subscription and Standard Support additional product	30-Jun-2022	
CPSB-LOGS-For-GW	Logging and Status blade for Appliance	2542DE4627EF	Enterprise Software Subscription and Standard Support additional product	30-Jun-2022	



4600 Next Generation Threat Extraction Appliance

SKU: CPAP-SG4600-NGTX | Order Date: 15-Jun-2022

Key: 00:1C:7F:[redacted] | IP Address: [redacted]52

*Image for illustration

Name: CPCM1 | OS: Gaia Version: R80.20 | Appliance Type: Gateway

Capture Date: 28-Jun-2022 | VSX Gateway: ⊗

Hardware S/N: 12[redacted]50

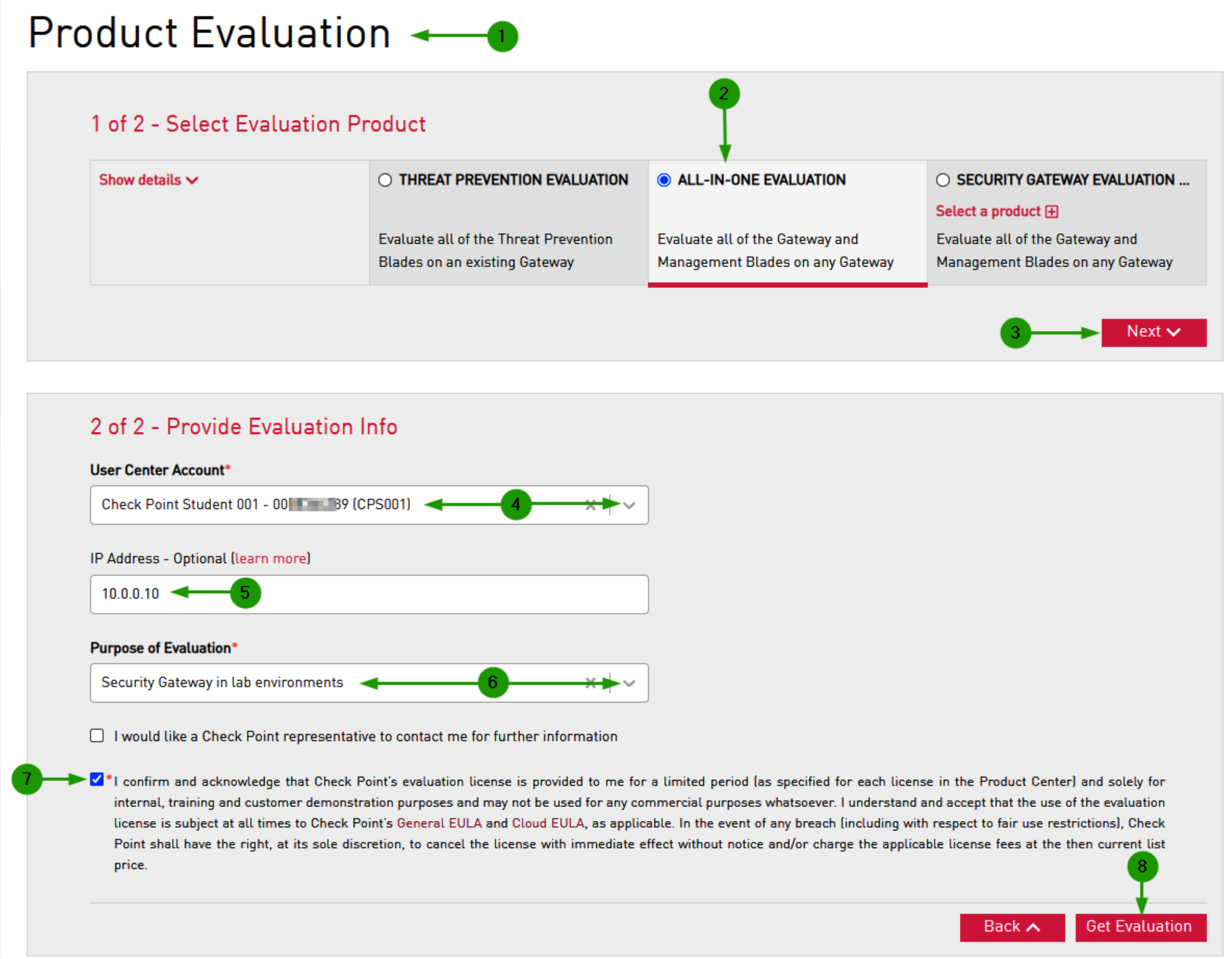
Account info: My_Company | ID: 00[redacted]58

Description: 4600 Next Generation Threat Extraction Appliance

Support: Software Subscription Standard | Until: 30-Jun-2022

Perpetual Blades: FW VPN ADNC MOB IA NPM LOGS

Annuity Services: Enterprise Based Protection - AB APCL ASPM AV CTNT IPS TE TEX URLF | Until: 30-Jun-2022



Product Evaluation

1 of 2 - Select Evaluation Product

Show details

○ THREAT PREVENTION EVALUATION
Evaluate all of the Threat Prevention Blades on an existing Gateway

● ALL-IN-ONE EVALUATION
Evaluate all of the Gateway and Management Blades on any Gateway

○ SECURITY GATEWAY EVALUATION ...
Select a product ⊞
Evaluate all of the Gateway and Management Blades on any Gateway

2 of 2 - Provide Evaluation Info

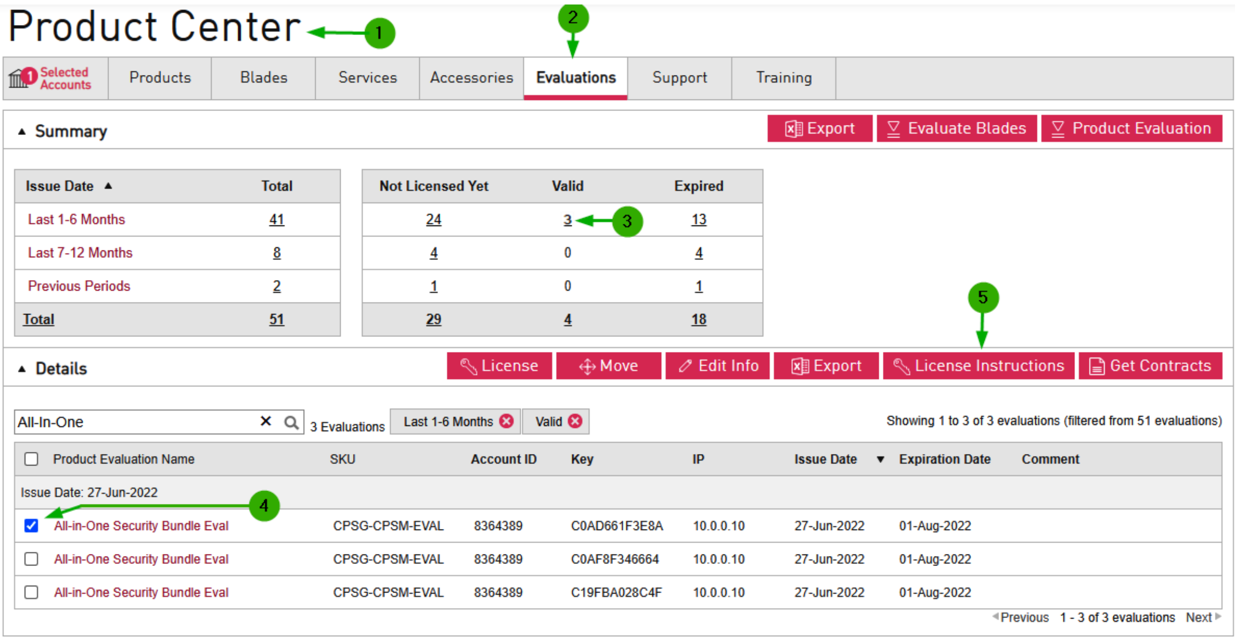
User Center Account*: Check Point Student 001 - 00[redacted]39 (CPS001)

IP Address - Optional (learn more): 10.0.0.10

Purpose of Evaluation*: Security Gateway in lab environments

☐ I would like a Check Point representative to contact me for further information

☑ *I confirm and acknowledge that Check Point's evaluation license is provided to me for a limited period (as specified for each license in the Product Center) and solely for internal, training and customer demonstration purposes and may not be used for any commercial purposes whatsoever. I understand and accept that the use of the evaluation license is subject at all times to Check Point's General EULA and Cloud EULA, as applicable. In the event of any breach (including with respect to fair use restrictions), Check Point shall have the right, at its sole discretion, to cancel the license with immediate effect without notice and/or charge the applicable license fees at the then current list price.



Product Center

▲ Summary

Issue Date ▲	Total
Last 1-6 Months	41
Last 7-12 Months	8
Previous Periods	2
Total	51

Not Licensed Yet	Valid	Expired
24	3	13
4	0	4
1	0	1
29	4	18

▲ Details

All-In-One ✕ 3 Evaluations Last 1-6 Months Valid

Showing 1 to 3 of 3 evaluations (filtered from 51 evaluations)

☐	Product Evaluation Name	SKU	Account ID	Key	IP	Issue Date ▼	Expiration Date	Comment
Issue Date: 27-Jun-2022								
☑	All-in-One Security Bundle Eval	CPSG-CPSM-EVAL	8364389	C0AD661F3E8A	10.0.0.10	27-Jun-2022	01-Aug-2022	
☐	All-in-One Security Bundle Eval	CPSG-CPSM-EVAL	8364389	C0AF8F346664	10.0.0.10	27-Jun-2022	01-Aug-2022	
☐	All-in-One Security Bundle Eval	CPSG-CPSM-EVAL	8364389	C19FBA028C4F	10.0.0.10	27-Jun-2022	01-Aug-2022	

◂Previous 1 - 3 of 3 evaluations Next▸