



Hybrid Mesh Network Security

06 May 2026

CHECK POINT GATEWAY AND MANAGEMENT HARDENING

Administration Guide



Check Point Copyright Notice

© 2026 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



Check Point Gateway and Management Hardening Administration Guide



Latest Version of this Document in English

Open the latest version of this [document in a Web browser](#).
Download the latest version of this [document in PDF format](#).



Feedback

Check Point is engaged in a continuous effort to improve its documentation. [Please help us by sending your comments](#).

Revision History

| Date | Description |
|-------------|--|
| 06 May 2026 | Updated " Gaia OS Hardening " on page 21 - added recommendations for the LOM interface |
| 04 May 2026 | First release of this document |

Table of Contents

| | |
|--|-----------|
| Introduction | 6 |
| Decreasing Security Gateway Exposure with Policy | 7 |
| Security Gateway Stealth Rule | 7 |
| Limit and Log Implied Rules | 7 |
| Management Plane Protection | 10 |
| Protect the Management Server Behind a Firewall | 10 |
| Restrict Administrative Source IP Addresses | 10 |
| Administrator Identity and Access Control | 12 |
| Limit SmartConsole Trusted Client Access settings | 12 |
| MFA and Identity Provider Integration | 12 |
| Review and Remove Unused Administrator Accounts Regularly | 13 |
| Ensure administrator access, password policy, and idle timeout are set | 13 |
| Limiting Third-Party Integration Credentials | 15 |
| General Principle: Least Privilege for Integrations | 15 |
| Active Directory (AD) Integration Accounts | 15 |
| Cloud Controller Integrations (AWS, Azure, GCP) | 15 |
| Identity Provider and API Integrations | 16 |
| Updates, Health, and Ongoing Protection | 17 |
| Upgrade to Latest Recommended Jumbo Hotfix Accumulator | 17 |
| Enable Dynamic Updates (AutoUpdater Utility) | 19 |
| Enable Diagnostics and Telemetry (cpdiag) | 20 |
| Gaia OS Hardening | 21 |
| Gaia Default Hardening Overview | 21 |
| Gaia OS administrator settings | 21 |
| Password Policy Hardening (Complexity, Age, Reuse) | 22 |
| Dynamic Routing Hardening | 26 |
| SNMP Monitoring Hardening | 28 |

| | |
|---|-----------|
| Expert mode Governance | 29 |
| Enable Security Gateway system logging to the Management Server | 32 |
| Enable Management Server system logging to an external server | 34 |
| Restrict Access to Lights Out Management (LOM / Out of Band Management) | 35 |
| Advanced Hardening (High Security Environments Only) | 37 |
| Explicit Rules Instead of Implied Rules | 37 |
| Deployment Checklists | 38 |
| Quick Checklist (All Environments) | 38 |

Introduction

This document provides practical hardening recommendations for Check Point Security Gateways and Management Servers running supported Gaia OS releases. The recommendations apply to these versions:

- R82.10
- R82
- R81.20

Recent industry developments, including Anthropic's Mythos and related initiatives, reflect a fundamental shift in the cyber threat landscape. Advanced AI capabilities are expected to significantly accelerate the pace, scale, and automation of attacks, reducing the time and effort required to identify, adapt, and operationalize attack techniques. As a result, attackers are increasingly expected to focus on management planes, control planes, privileged access paths, trust relationships, and operational misconfigurations for assets that provide disproportionate leverage when abused.

This shift does not depend on weaknesses in specific products. Rather, it highlights a broader reality: highly trusted platforms and administrative systems must be continuously hardened to remain resilient as attack speed and sophistication increase.

Check Point is providing this guidance to help customers proactively strengthen their environments, reduce exposed attack surface, and limit the potential impact of control plane or identity-based abuse. These recommendations are part of a defense in depth approach designed to improve preparedness as AI accelerated attack techniques become more prevalent across the industry.

Each recommendation in this document includes:

- What to do
- Why it is recommended
- Default vs. recommended behavior
- An example where appropriate
- A direct reference to official Check Point documentation or SecureKnowledge for implementation

Decreasing Security Gateway Exposure with Policy

Security Gateway Stealth Rule

Recommendation: Configure a Stealth Rule to drop traffic that is directed to the Security Gateway itself, except for explicitly required management and control traffic.

Security Gateways are frequently scanned. A Stealth Rule reduces the Security Gateway's exposure and limits which hosts can reach Security Gateway services.

| Item | Default (Typical) | Recommended |
|--|-------------------|---|
| Security Gateway is reachable on data plane interfaces | Depends on policy | Allow only required traffic that is directed to the Security Gateway. Drop all other traffic directed to the Security Gateway. |
| Logging of stealth drops | Depends on policy | Enable during rollout, then tune to reduce noise. |

Example policy pattern (simplified):

- Allow & Log: Admin Jump Hosts and Specific Admin user groups -> Security Gateway (HTTPS / SSH / API as used)
- Drop & Log: Any -> Security Gateway (all other traffic directed to Security Gateway)

| No. | Name | Source | Destination | Services & Applications | Action | Track | Install On |
|------------------------------------|----------------------------------|--------|--------------|-------------------------|--------|-------|------------------|
| ▼ Security Gateways Access (1-2) ✓ | | | | | | | |
| 1 | Administrator Access to Gateways | Admins | Corporate-GW | Manage Services | Accept | Log | * Policy Targets |
| 2 | Stealth rule | * Any | Corporate-GW | * Any | Drop | Log | * Policy Targets |

Implementation reference:

[R82.10 Security Management Administration Guide](#) > Creating an Access Control Policy, Best Practices for Access Control Rules

Limit and Log Implied Rules

Recommendation: Review implied rules settings, only enable those that are necessary and ensure that logging for implied rules remain enabled.

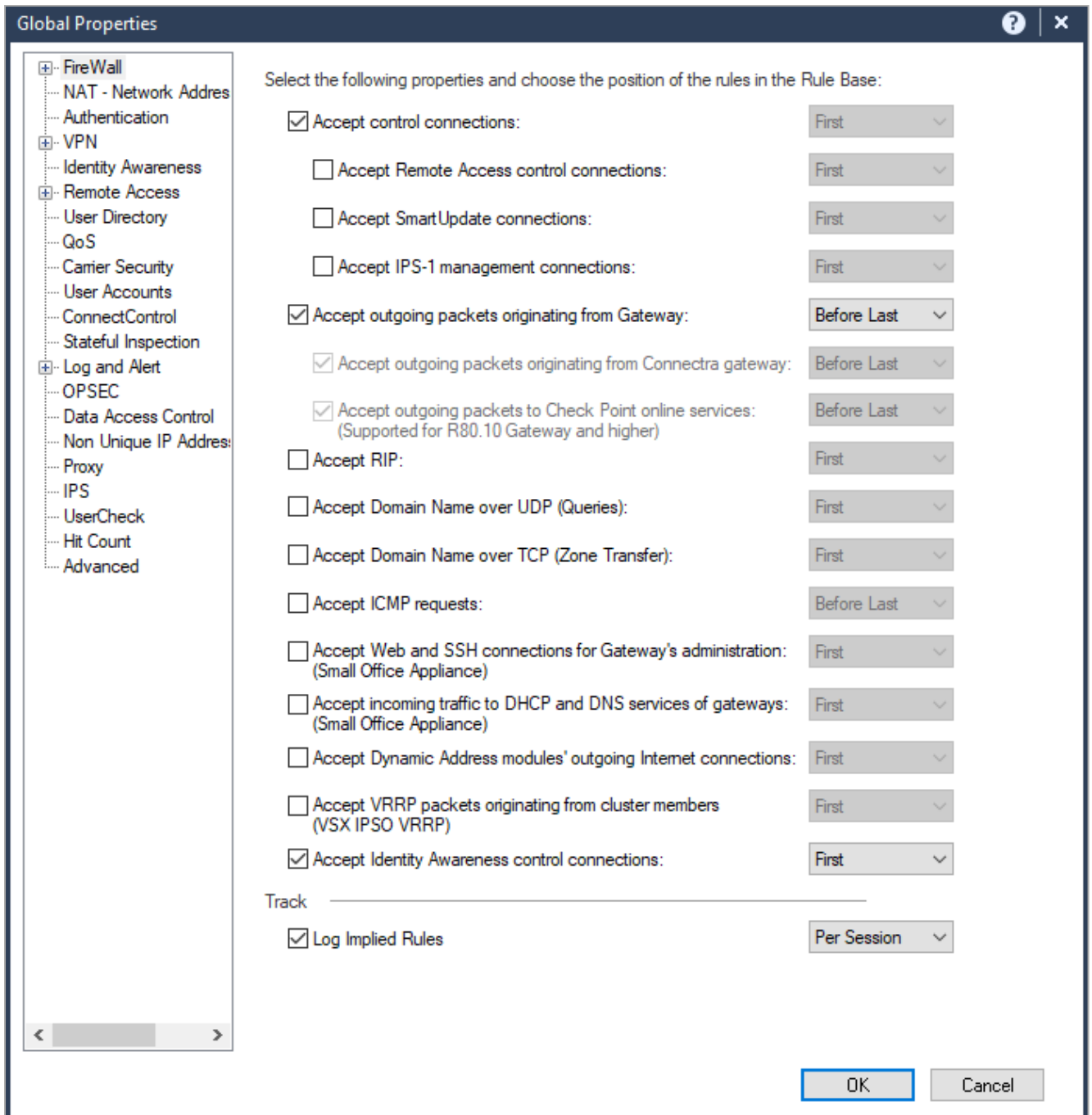
Implied Rules allow essential Check Point internal communication, connectivity for essential features (e.g. VPN & Remotes Access).

Reducing these to the minimum will reduce the potential attack surface and logging them improves auditability and troubleshooting without breaking functionality.

| Item | Default (Typical) | Recommended |
|---------------------------|-------------------|--|
| Implied rules execution | Enabled | Keep enabled unless you implement full explicit replacement. |
| Logging for implied rules | Disabled | Enable logging for visibility and troubleshooting. |

Operational note: Disabling implied rules without correct explicit rules can cause policy install failures and loss of management / log connectivity.

Check Point Security Gateway clusters using static IP addresses, without remote access enabled, should be set up as follows:



Implementation reference:

[R82.10 Security Management Administration Guide](#) > Creating an Access Control Policy, Implied Rules.

Management Plane Protection

Protect the Management Server Behind a Firewall

Recommendation: Deploy the Security Management Server behind a firewall or protected network segment and restrict inbound access to required administrative sources only.

The Management Server controls policy installation, trust relationships (SIC), and administrator access. Segmentation reduces exposure and blast radius.

| Item | Default (Typical) | Recommended |
|------------------------------|----------------------|--|
| Management server exposure | Environment specific | Limit access to admin networks / jump hosts and required Security Gateways only. |
| Dedicated management network | Environment specific | Use a dedicated management VLAN / subnet where possible. |

Example allowed sources: Admin jump hosts, Security Gateways / Clusters (for SIC/policy/logs), and dedicated log servers (if used).

Restrict Administrative Source IP Addresses

Recommendation: Restrict SmartConsole / WebUI / SSH / API access to specific internal IP ranges or jump hosts.

Network-level restrictions stop broad scanning and brute force attempts before authentication is attempted.

| Item | Default (Typical) | Recommended |
|------------------------------|----------------------|--|
| Admin source restriction | Environment specific | Restricted to admin jump hosts / administrator subnets only. |
| Direct Internet admin access | Environment specific | Avoid. Require VPN. |

We recommend using Web SmartConsole to access the Management Server, as it only requires access to the TCP port 443.

The Desktop SmartConsole application needs access to these ports on the Management Server:

- TCP 18190
- TCP 18264
- TCP 19009

A complete list of ports used is listed in [sk52421](#).

Implementation reference:

[R82.10 Installation and Upgrade Guide](#) > Installing SmartConsole.

Administrator Identity and Access Control

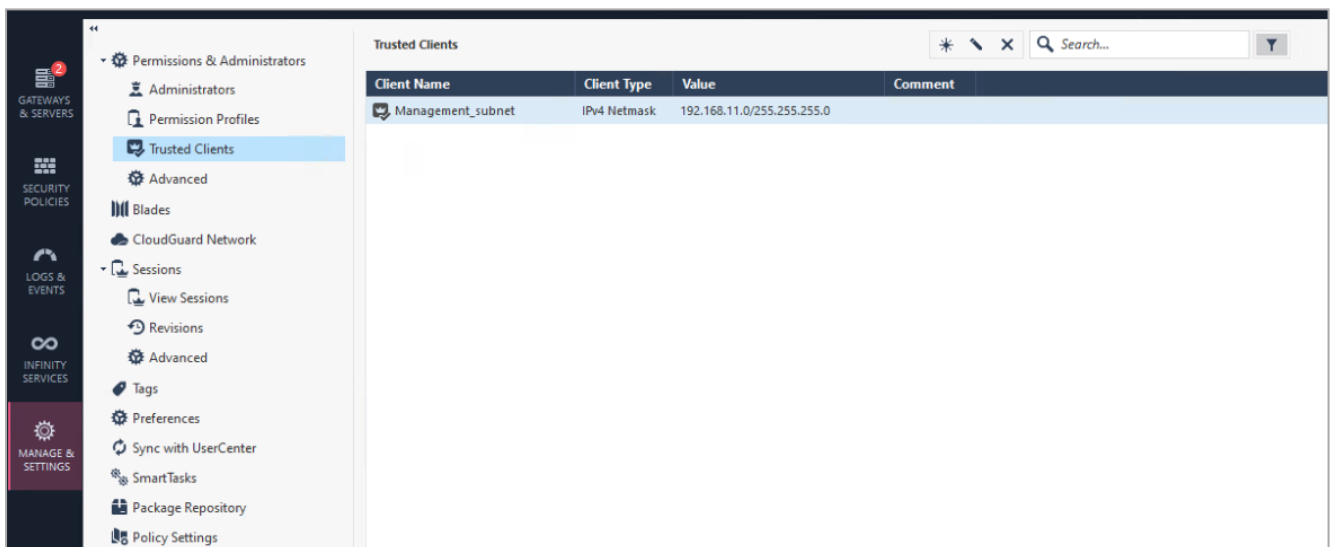
Limit SmartConsole Trusted Client Access settings

Recommendation: Restrict the IP addresses, subnets and ranges that can use a SmartConsole to the necessary minimum.

In addition to network controls that may be in place, the management server can be configured to limit access as well. It is an additional safeguard to ensure access is limited only to the required locations.

To validate and apply these settings:

SmartConsole > **Manage & Settings** view > **Permissions & Administrators** > **Trusted Clients**.



MFA and Identity Provider Integration

Recommendation: Enforce MFA for all administrative access using an external Identity Provider (for example, SAML-based administrator login or TACACS / RADIUS where applicable).

MFA reduces the risk of credential compromise and enables centralized identity lifecycle management (join / move / leave).

| Item | Default (Typical) | Recommended |
|---------------------------------|-------------------|--|
| MFA enforcement | Not guaranteed | Mandatory for all administrator roles |
| Local only admin authentication | Common | IdP + MFA for daily admin access; keep break glass accounts controlled |

Implementation reference:

[R82.10 Security Management Administration Guide](#) > Creating an Administrator Account with SAML Authentication Login.

Review and Remove Unused Administrator Accounts Regularly

Recommendation: Periodically review administrator accounts and disable / remove accounts that are no longer used.

Dormant accounts are a common entry point for attackers and are often overlooked.

| Item | Default (Typical) | Recommended |
|-----------------------|-------------------|--------------------------------|
| Admin account reviews | Ad hoc | Quarterly review as a minimum |
| Shared admin accounts | Sometimes exist | Avoid. Use named accounts only |

Ensure administrator access, password policy, and idle timeout are set

Recommendations:

- Administrator access should expire at a set interval of time.
- Administrator password length should be at least 10 characters long.
- SmartConsole should be disconnected after 10 minutes of idle time and an administrator account lockout setting should be applied.

Attackers may be able to take control of an administrator host or capture passwords using a keylogger. Restricting access, expiring accounts, and locking accounts after authentication failures will reduce the possibility of an attacker gaining control over the management server.

To validate and apply these settings:

SmartConsole > **Manage & Settings** view > **Permissions & Administrators** > **Advanced**.

The screenshot displays the 'Advanced' settings page for Administrator Identity and Access Control in the SmartConsole. The left sidebar shows the navigation menu with 'MANAGE & SETTINGS' selected. The main content area is divided into several sections:

- Administrator Settings**
 - Authentication Default Values**: Authentication method is set to 'Check Point Password'.
 - Default Expiration Date**:
 - Never expires
 - Expires at: 10/04/2026
 - Expires after: 2 Months
 - Expiration Notifications**:
 - Show 'about to expire' indication in administrators view 14 days in advance.
 - Notify administrator 30 days in advance.
- Check Point Password Settings**:
 - Minimum password length: 10
- My Check Point Password**:
 - Change my Check Point password on next login: [Change...](#)
- Idle Timeout**:
 - Perform logout after being idle
 - The SmartConsole will automatically logout after being idle for 10 minutes.
 - Updating the interval will take effect only on next login.
- Login Restrictions**:
 - Lockout Administrator's account after 3 failed authentication attempts
 - Unlock Administrator's account after 30 minutes
 - Display an informative message upon denying access

Limiting Third-Party Integration Credentials

General Principle: Least Privilege for Integrations

Recommendation: Configure third-party integration credentials (directory, cloud, IdP, API) with the minimum privileges required - prefer read-only roles - and separate these credentials from interactive administrator accounts.

Integration credentials are often long-lived and non-interactive. Over privileged integration accounts increase blast radius if compromised.

Active Directory (AD) Integration Accounts

Recommendation: Use a dedicated directory service account for AD / LDAP integrations with read only permissions for user / group lookup and authentication. Do not use Domain Admin or highly privileged accounts.

Directory integrations typically do not require write permissions. Read only accounts reduce lateral movement risk.

Implementation reference:

[sk93938 - Using Identity Awareness AD Query without Active Directory Administrator privileges](#)

Cloud Controller Integrations (AWS, Azure, GCP)

Recommendation: Use cloud native roles / service accounts with read only permissions for discovery; add write permissions only if automation use cases require them.

Cloud credentials can expose large parts of your infrastructure and metadata. Read only roles reduce impact of credential compromise.

Examples (minimum privilege approach):

- AWS: IAM role limited to Describe* APIs only (for discovery)
- Azure: Service Principal / Managed Identity with Reader role
- GCP: Service Account with Viewer role

Implementation reference:

[R82.10 CloudGuard Controller Administration Guide](#) > Configuring Permissions for Amazon Web Services.

Identity Provider and API Integrations

Recommendation: Scope API credentials / tokens to the minimum required roles and APIs. Avoid using full administrative API tokens for integrations that only need authentication or limited identity attributes. Use certificates for authentication where possible, create API keys for a duration of two months and do not store these in clear-text file repositories.

Broad API permissions can allow unintended configuration changes if the token is exposed.

Implementation reference:

[R82.10 Security Management Administration Guide](#) > Managing Security through API, Creating an Administrator Account with API Key Authentication.

Updates, Health, and Ongoing Protection

Upgrade to Latest Recommended Jumbo Hotfix Accumulator

Check Point periodically releases Jumbo Hotfix Accumulators (JHFs) for each supported version. These releases consolidate stability fixes, reliability improvements, performance enhancements, and security related corrections into a tested and supported package.

Running the recommended Jumbo Hotfix Accumulator is a foundational hardening step and should be treated as a baseline requirement for production Security Gateways and Management Servers.

Recommendation: Always run Check Point Security Gateways and Management Servers on:

- A supported major release, and
- The currently recommended Jumbo Hotfix Accumulator for that release

Delaying adoption of recommended Jumbo Hotfix Accumulators increases operational risk, reduces platform resilience, and limits the effectiveness of other hardening controls described in this document.

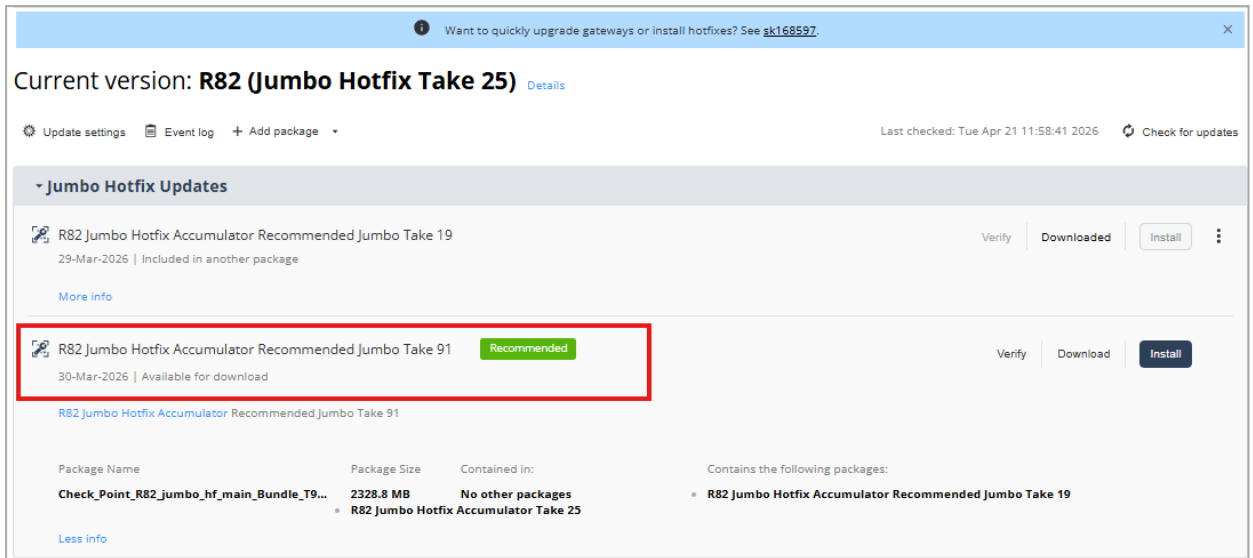
Recommended Jumbo Hotfix Accumulator Takes include important security and stability fixes that reduce exposure to known issues.

Implementation reference:

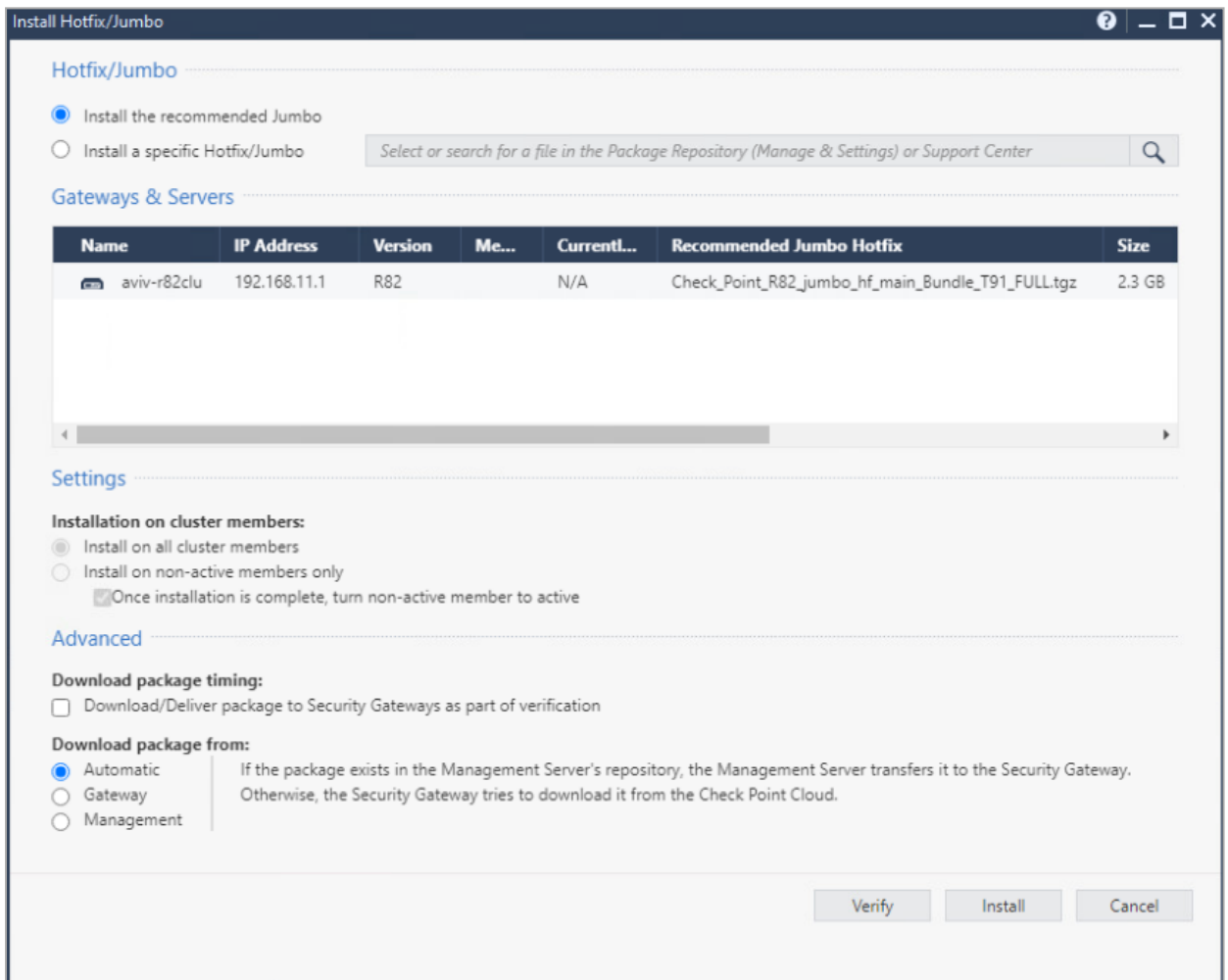
[sk95746 - Check Point Recommended Version and Release Terminology.](#)

Upgrades are available:

■ From the local Gaia Portal:



■ From SmartConsole:



Enable Dynamic Updates (AutoUpdater Utility)

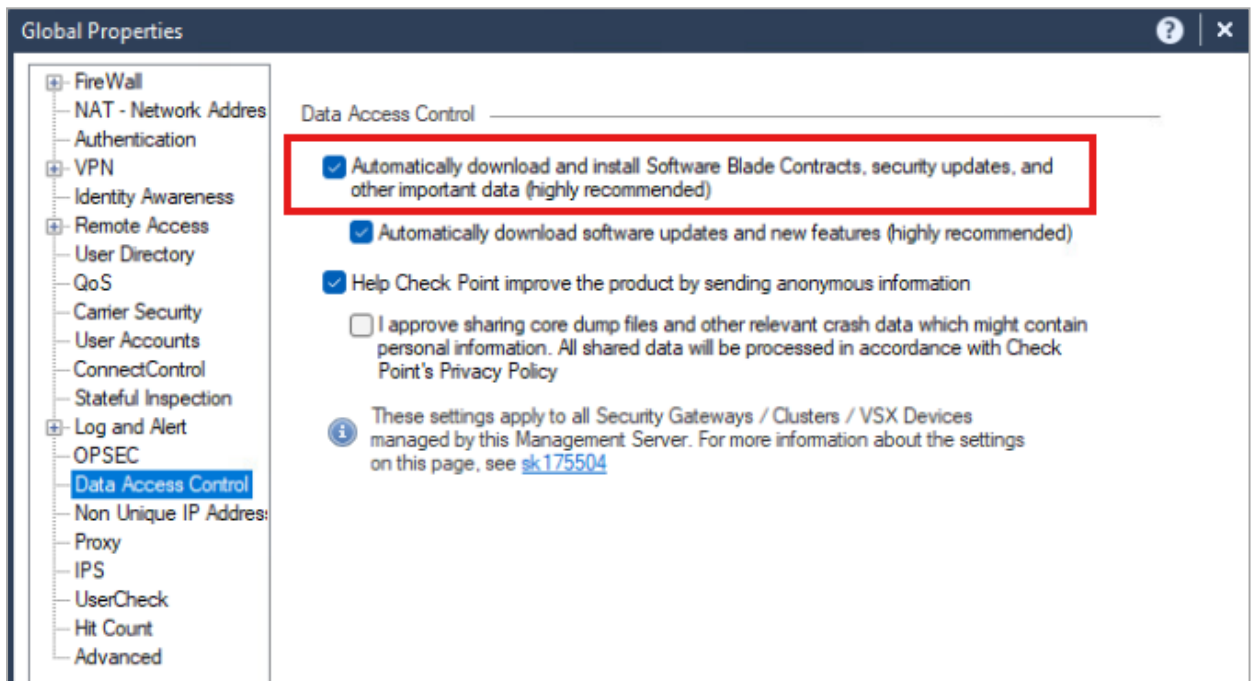
Recommendation: This utility enables dynamic security updates including IPS updates and security fixes.

Dynamic updates keep protections current without requiring disruptive upgrades or reboots.

Ensure that you provide consent for Check Point to install security updates as following the instructions in [sk175504](#):

1. In SmartConsole top-left corner, click the **Menu** button > click **Global properties**.
2. In the **Data Access Control** pane, select this checkbox:

Automatically download and install Software Blade Contracts, security updates, and other important data (highly recommended)



3. Click **OK**.
4. Install the Access Control policy.

This will ensure only security updates will be installed and no other unnecessary updates.

Check Point uses this mechanism to mitigate vulnerability as interim preventative measure that helped protect many customers before they were even aware.

Implementation reference:

- [sk175504 - How to configure Check Point software to upload data to Check Point / download data from Check Point in versions R81.20 and higher.](#)
- [sk182376 - Interim preventative measure \(VPNF\) for CVE-2024-24919.](#)

Enable Diagnostics and Telemetry (cpdiag)

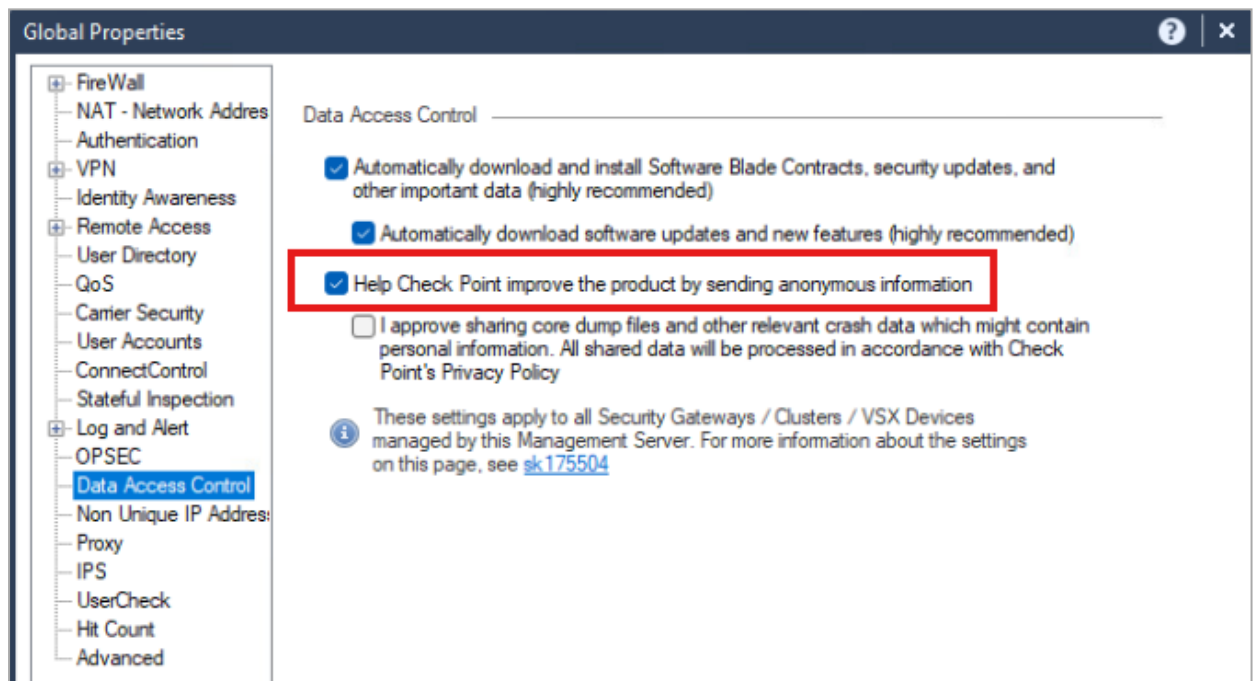
Recommendation: Enable your Check Point Management Servers and Security Gateways to share essential non-PII, diagnostics data with Check Point cloud.

Check Point Diagnostics collects usage information and status telemetry of the product operation. This helps improve supportability and enable proactive identification of issues (without replacing your logging strategy). This is essential for Check Point to identify and proactively alert if your products are exposed to a known vulnerability. The collection and transmission of the data is not CPU-intensive and is shared every 24 hours.

Ensure that you provide consent for Check Point to install security updates by following the instructions in [sk175504](#):

1. In SmartConsole top-left corner, click the **Menu** button > click **Global properties**.
2. In the **Data Access Control** pane, select this checkbox:

Help Check Point improve the product by sending anonymous information



3. Click **OK**.
4. Install the Access Control policy.

Implementation reference:

[sk184778 - CPDiag \(Check Point Diagnostics\) Release Updates.](#)

Gaia OS Hardening

Gaia Default Hardening Overview

Gaia OS is delivered in a hardened baseline state. After the Gaia OS installation, the only network services on Gaia OS are OpenSSH (TCP 22), Gaia Portal secure web server (HTTPS TCP 443), cpid (TCP 18208), and Gaia REST API server (HTTPS via TCP 443).

Restrict access to these ports to internal trusted networks.



Gaia OS administrator settings

Review all users with access to the Gaia OS and ensure all users are authorized, use strong passwords, configure the access role to allow the minimal access required per user role, ensure the shell is set to Gaia Clish and force users to use MFA for access

1. In Gaia Portal, navigate to **User Management > Users**:

User Management ▸ Users

Users

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

2. Select each user and click **Edit**.
3. Make sure the **Shell** is set to **/etc/cli.sh**:

The screenshot shows the 'Add User' configuration window. The 'Shell' dropdown menu is selected and highlighted with a red border, showing the value '/etc/cli.sh'. To the right, the 'Available Roles' list contains 'adminRole' and the 'Assigned Roles' list contains 'monitorRole'. The password strength indicator shows a green bar and the word 'Strong'. The 'Access Mechanisms' section has three checkboxes: 'Web' (checked), 'Clish Access' (checked), and 'Gaia API' (unchecked). At the bottom right, there are 'OK' and 'Cancel' buttons.

4. Click OK.

Implementation reference:

[R82.10 Gaia Administration Guide](#) > User Management > Authentication.

Password Policy Hardening (Complexity, Age, Reuse)

Recommendation: Enforce password complexity, multi-factor authentication (R82 or higher), password history (reuse prevention), password aging, auto lock out of admins with multiple authentication failures or with long inactivity periods.

Strong password policy reduces brute force and credential reuse risk. Automatically disabling dormant administrator accounts significantly reduces the attack surface by preventing access from accounts associated with former employees.

1. In Gaia Portal, navigate to **User Management > Password Policy**.
2. In the section **Password Strength**:

| Item | Default | Recommended |
|-------------------------|--------------|---------------|
| Minimum Password Length | 6 characters | 10 characters |

| Item | Default | Recommended |
|----------------------|---------------------------------|----------------------------------|
| Disallow Palindromes | Enabled | Enabled |
| Password Complexity | 2 - Require two character types | 4 - require four character types |

User Management ▶ Password Policy

Password Strength

Minimum Password Length:

Disallow Palindromes:

i A palindrome is a word that can be read the same way in either direction

Password Complexity: 1 - Don't check
 2 - Require two character types
 3 - Require three character types
 4 - Require four character types

3. In the section **Password History**:

| Item | Default | Recommended |
|--------------------------|---------|-------------|
| Check for Password Reuse | Enabled | Enabled |

Password History

Check for Password Reuse:

History Length:

4. In the section **Mandatory Password Change**:

| Item | Default | Recommended |
|---|--|--------------------------------|
| Password Expiration | Passwords never expire | Passwords expire after 90 days |
| Lockout users after password expiration | Never lockout users after password expires | Lockout user after 1 days |

Mandatory Password Change

Password Expiration: Passwords never expire

Passwords expire after days

Warn users before password expiration: days

Lockout users after password expiration: Never lockout users after password expires

Lockout user after days

Force users to change password at first login after password was changed from [Users](#) page:

5. In the section **Deny Access to Unused Accounts**:

| Item | Default | Recommended |
|--------------------------------|----------|-------------|
| Deny access to unused accounts | Disabled | Enabled |
| Days non-use before lock-out | 365 days | 30 days |

Deny Access to Unused Accounts

Deny access to unused accounts:

Days of non-use before lock-out:

6. In the section **Deny Access After Failed Login Attempts**:

| Item | Default | Recommended |
|---|-----------------------|------------------------|
| Deny access after failed login attempts | Disabled | Enabled |
| Block admin user | Disabled | Enabled |
| Maximum number of failed attempts allowed | 10 | 5 |
| Allow access again after | 1200 seconds (20 min) | 7200 seconds (2 hours) |

Deny Access After Failed Login Attempts

Deny access after failed login attempts:

Block admin user:

Maximum number of failed attempts allowed:

Allow access again after time: seconds

7. In the section **Password hashing algorithm**:

| Item | Default | Recommended |
|------------------|---------|-------------|
| Password Hashing | SHA512 | SHA512 |

Important: If the Gaia server has been through multiple upgrades, you should reset the passwords to force them to be re-hashed with a stronger hashing function.

Password hashing algorithm

Hashing Algorithm: SHA256 SHA512


8. In the section **Two-Factor Authentication** (available in R82 and higher):

| Item | Default | Recommended |
|--|----------|-------------|
| Force all users to use Two-Factor Authentication | Disabled | Enabled |

Two-Factor Authentication

For an added layer of security, you can require users to use [Two-Factor Authentication \(2FA\)](#) when they sign in to Gaia.

Force all users to use Two-Factor Authentication:

 This applies to Gaia Portal, Gaia Clish, and Gaia API access.

Implementation reference:

- [R82.10 Gaia Administration Guide](#) > User Management > Password Policy in Gaia Portal.
- [sk181854 - Two-Factor Authentication for Gaia OS login.](#)

Dynamic Routing Hardening

Recommendation: Enable only routing protocols required, accept routing protocols only from predefined list or routing peers, apply authentication (e.g., BGP MD5), use route filters to restrict learned routes impact.

Dynamic routing protocols require the Security Gateway to listen on specific ports to exchange routing information. Routing peers may be outside your organization, which increases risk. To reduce attack surface and prevent abuse or misconfiguration that could lead to security issues, allow routing updates only from approved peers, use authentication, and apply route filtering.

Start with disabling the implied rules relating to dynamic routing as mentioned in ["Decreasing Security Gateway Exposure with Policy" on page 7](#). Instead use an explicit access rule that will let only routing peers connect to the Security Gateway.

In the example below, the group "BGP_routing_peers" contains the relevant IP address of the routing peers that it must communicate with, with a destination set to be the Security Gateway itself. Use the BGP protocol from application control as it will verify the protocol is indeed BGP and not an attempt to tunnel other traffic over a well known port.

| No. | Name | Source | Destination | VPN | Services & Applications | Action | Track |
|-----|---------------------------------|-------------------|-------------|-------|-------------------------|--------|-------------------|
| 1 | explicit dynamic routing access | BGP_routing_peers | aviv-r82clu | * Any | BGP Protocol | Accept | Log Accounting |

To find the list of configured peers in Gaia Portal, navigate to **Advanced Routing > BGP**.

Example (it is for BGP, but should be repeated for other dynamic routing protocols):

VMware aviv-r82mgmt

Advanced Routing > BGP

View mode: Advanced

Border Gateway Protocol (BGP) is an inter-AS protocol, meaning that it can be deployed within and between autonomous systems (AS).

BGP Global Settings

Router ID: 192.168.11.2

Cluster ID for Route Reflectors:

Local Autonomous System Number: 65000

Change Global Settings

Miscellaneous Settings

Default MED: [Dropdown] Default Gateway: [Text Field]

Enable IGP Synchronization: Enable Communities:

Enable ECMP:

Graceful Restart Time: Default: 360 Graceful Restart Selection Deferral Time: Default: 360

Enable Weighted Route Dampening:

Ping Interval: Default: 2 Ping Count: Default: 3

Apply

Peer Groups

Add Edit Delete Restart Restart All

| Peer Group | Group Type | Local Address | Peers | Description |
|------------|------------|---------------|---------------|-------------|
| 65001 | External | | 141.226.36.36 | |

Configure MD5 authentication for BGP to improve the level of trust with peer routers:

1. In Gaia Portal, navigate to **Advanced Routing > BGP**.
2. Select the peer group and click **Edit**.
3. Select the specific peer and click **Edit**.
4. Click **Show Advanced Settings**.
5. Scroll down to the **Authentication** section.
 - a. In the **Authentication Type** field, select **MD5**.
 - b. In the **Password** field, enter the applicable password.

Recommendation: Rotate this password every 90 days.

Example:

The screenshot shows the configuration window for a BGP peer. The 'Authentication' section is highlighted with a red box. It contains the following fields:

- Authentication Type:** MD5 (selected from a dropdown menu)
- Password:** A text input field containing masked characters (dots).

Other visible settings include:

- Routes:** Accept Routes Received From the Peer: All (dropdown)
- Allows Accept TCP Sessions from your Peer:** Passive:
- Limit BGP Updates Send to a Peer:** Throttle Count: (empty input field)

Buttons for 'Save' and 'Cancel' are located at the bottom right of the window.

6. Click **Save**.

Configure inbound route filters to ensure only desired routes are learned from peers.

For example, do not allow external routers to advertize routes for internal networks.

Implementation reference:

- [R82.10 Gaia Advanced Routing Administration Guide](#) > Configuring BGP Remote Peers in Gaia Portal.
- [sk95967 - BGP on Gaia OS](#).
- [sk98936 - How to configure route redistribution and inbound route filters in Gaia Portal](#).

SNMP Monitoring Hardening

Recommendation: Disable SNMP if not needed. If SNMP is required, use SNMPv3 with SHA512 authentication and AES256 encryption (do not use SNMPv1 or SNMPv2). Run the SNMP agent only on internal interfaces and only allow specific IPs to send requests to these interfaces. For monitoring of Check Point Security Gateways and Management Server, a read-only permission is sufficient.

SNMP can expose operational details. Secure configuration reduces information disclosure risk.

1. In Gaia Portal, navigate to **System Management > SNMP**.
2. In the section **SNMP Genera Settings**:

- a. In the **Version** field, select **v3-Only**.
 - b. Click **Apply**.
3. In the section **Agent Interfaces**:
 - Select only the relevant **internal** interfaces.
 4. In the section **V3 - User-Based Security Model (USM)**:
 - a. Add a new USM user.
 - b. Configure the **Privacy Protocol** level to **AES256**.
 - c. Configure the **Authentication Protocol** level to **SHA512**.

The screenshot displays the Gaia OS System Management interface for SNMP configuration. The left sidebar shows the navigation menu with 'SNMP' selected. The main content area is divided into three sections:

- SNMP General Settings:** 'Enable SNMP Agent' is checked. The 'Version' dropdown is set to 'v3-Only'. There are empty input fields for 'SNMP Location String' and 'SNMP Contact String', and an 'Apply' button.
- Agent Interfaces:** A table lists interfaces with checkboxes. 'eth0 [192.168.11.2, fc01:0:0:1::2]' and 'lo [127.0.0.1, ::1]' are checked.
- V3 - User-Based Security Model (USM):** Includes 'Add', 'Edit', and 'Remove' buttons. A table shows the configuration for the 'snmp_admin' user:

| User Name | Security Level | Privacy Protocol | Authentication Protocol |
|------------|----------------|------------------|-------------------------|
| snmp_admin | authPriv | AES256 | SHA512 |

Implementation reference:

[R82.10 Gaia Administration Guide](#) > System Management > SNMP > Configuring SNMP in Gaia Portal.

Expert mode Governance

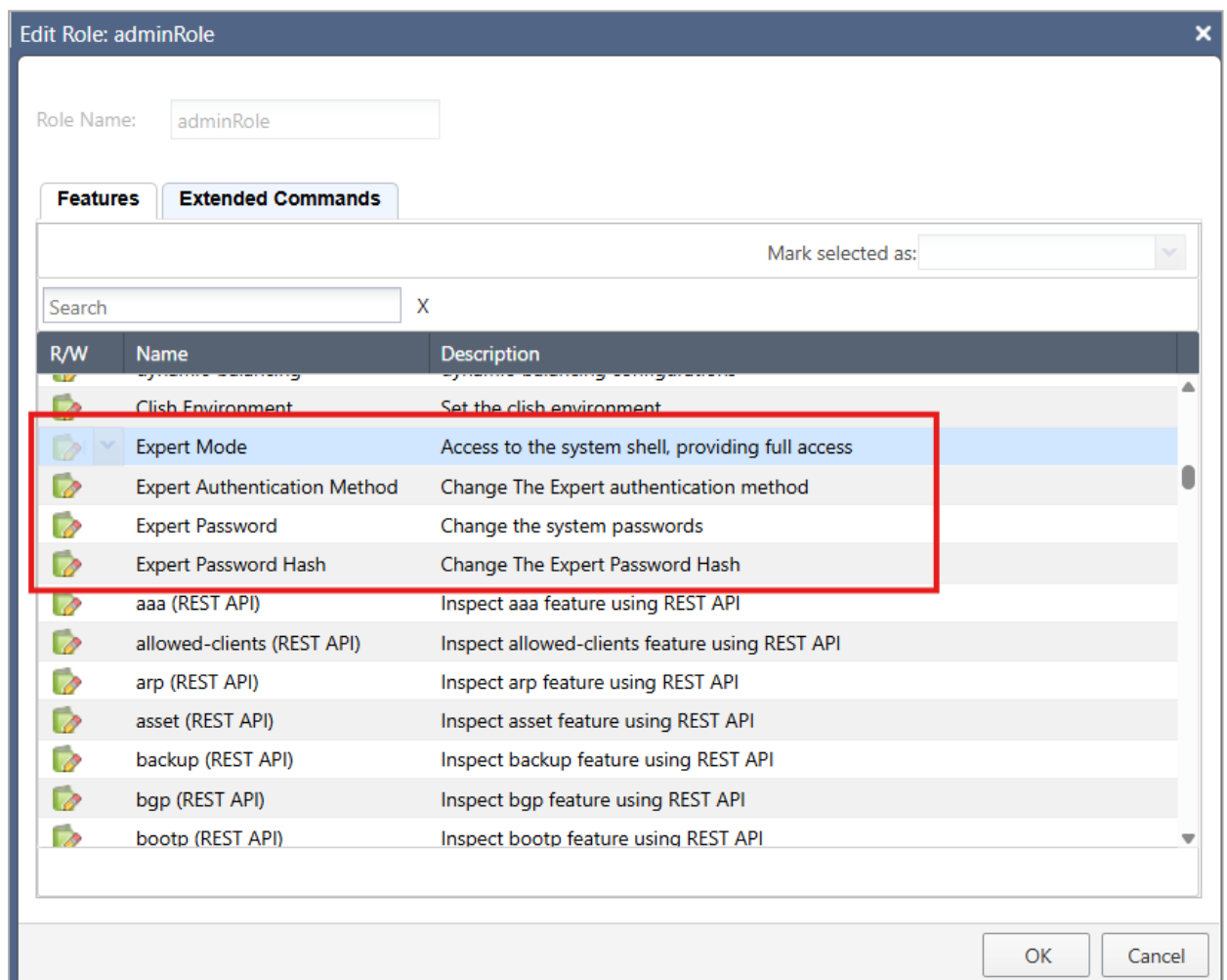
Recommendation: Restrict the Expert mode access to a limited, authorized set of administrators. Use integration with Check Point Playblocks to alert every time the Expert mode is activated (this Playblocks automation does **not** require a subscription to Playblocks).

The Expert mode provides full OS access as root user and should be tightly controlled.

1. In Gaia Portal, navigate to **User Management > Roles**.
2. Click **Add** to create a new role for administrators.

In this role, in the leftmost column **R/W**, set the following features to **None** or **Read Only**:

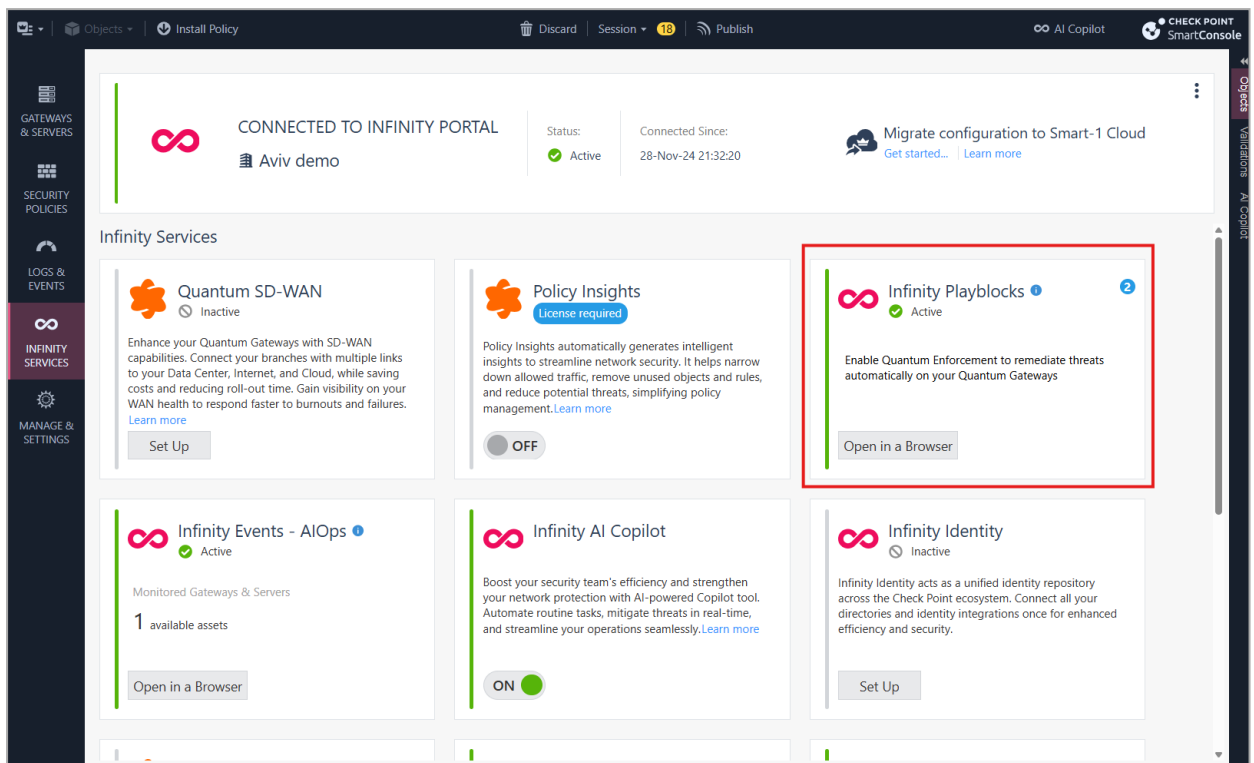
- **Clish Environment**
- **Expert Mode**
- **Expert Authentication Method**
- **Expert Password**
- **Expert Password Hash**



3. Click **OK**.
4. In Gaia Portal, navigate to **User Management > Users**.
5. Create new administrator users - in the **Available Roles** list, select the above limited administrator role.

6. In SmartConsole, connect your Management Server to Check Point cloud services.
7. Activate the Playblocks service.

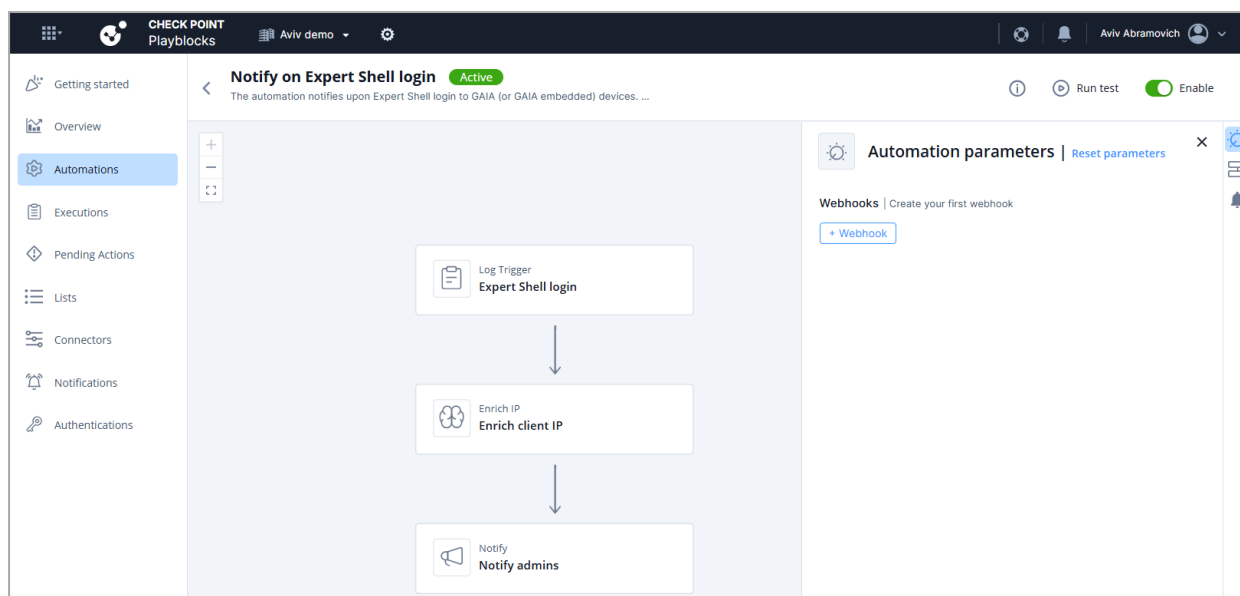
Note: This is supported for both on-premises servers and Smart-1 Cloud.



8. In the Playblocks card, click the button **Open in a Browser** to sign in to [Check Point Portal](#) and to go to the correct tenant.
9. In the left panel, click the **Automations** page.

Search for: expert.

Enable **Notify** for **Expert Shell** login.



This setting will generate a notification as configured in Playblocks upon each attempt to log in to the Expert mode.

Use these notifications to identify any unauthorized access to Expert mode.

Implementation reference:

- [R82.10 Gaia Administration Guide](#) > User Management > Roles > Configuring Roles in Gaia Portal.
- [Check Point Playblocks Administration Guide](#) > Automations > Predefined Automations > Notify on Expert Shell Login.

Enable Security Gateway system logging to the Management Server

Recommendation: Configure each Security Gateway to forward its Gaia OS system logs (syslog) to the Management Server and avoid relying solely on local log files on the Security Gateway.

Local syslog retention on the Security Gateway should be treated as a temporary buffer only, not as the primary source of system level visibility, for these reasons:

- **Centralized operational visibility:** Forwarding syslog to the Management Server allows administrators to review the Security Gateway's Gaia OS events alongside management plane activity.
- **Improved troubleshooting:** Many platform issues (for example routing daemon events, authentication failures, or service restarts) are visible only in system logs.

- Ability to audit. Central retention of system logs supports forensic analysis and operational audits.
- Resilience: Security Gateway local logs may be lost during reboot, disk issues, or hardware failure; central collection reduces this risk.

System logs complement - but do not replace - Security Gateway and traffic logging.

1. In Gaia Portal, navigate to **System Management > System Logging**.
2. In the **System Logging** section, select the checkbox **Send Syslog messages to management server**.

| Item | Default | Recommended |
|---|----------|-------------|
| Send syslog messages to management server | Disabled | Enabled |

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

Apply

System TLS Configuration

Import Delete

Location of uploaded TLS certificate files: /var/log/upload

| File Type | File Path |
|-----------|-----------|
| | |

Remote System Logging

Add Edit Delete

| IP Address | Send Logs from Priority Level | Port | Protocol | TLS Encryption | Authentication Mode | Permitted Peers | Queuing-Mechanism |
|----------------|-------------------------------|------|----------|----------------|--------------------------|-----------------|-------------------|
| 192.168.11.251 | All | 514 | tcp | on | certification validation | - | on |

3. Click **Apply**.

This allows the Security Gateway to send its syslog messages to the Management Server / Log Server.

You can later use these syslog messages for forensics in case of suspicious activity.

Example:

Card

Syslog Apr 23, 2026 3:59:19 PM

DETAILS

Origin: 192.0.2.1 Confidence Level: N/A

Time: Apr 23, 2026 3:59:19 PM Severity: Informational

Blade: Syslog

Product Family: Network

Type: Log

Log Server Origin: aviv-r82mgmt (192.168.11.2)

Log Server IP: 192.168.11.2

More

```
default_device_message: <46>Apr 23 15:59:19 aviv-r82gw1-s01-01
rsyslogd: [origin software="rsyslogd"
swVersion="8.24.0-53.el7.cp998000133"
x-pid="30848" x-
info="http://www.rsyslog.com"] start
```

Implementation reference:

[R82.10 Gaia Administration Guide](#) > System Management > System Logging > Configuring System Logging in Gaia Portal > Configuring the System Logging.

Enable Management Server system logging to an external server

Recommendation: Configure the Management Server to forward its Gaia OS system logs (syslog) to an external centralized log server, in addition to retaining a local copy for short term operational troubleshooting.

System logs generated by the Management Server should not be retained only locally.

Centralized retention supports investigations, regulatory audits, and compliance evidence requirements.

1. In Gaia Portal, navigate to **System Management > System Logging**.
2. In the **Remote System Logging** section, add the applicable remote syslog server.

Example:

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

Apply

System TLS Configuration

Import Delete

Location of uploaded TLS certificate files: /var/log/upload

| File Type | File Path |
|-----------|-----------|
| | |

Remote System Logging

Add Edit Delete

| IP Address | Send Logs from Priority Level | Port | Protocol | TLS Encryption | Authentication Mode | Permitted Peers | Queuing-Mechanism |
|----------------|-------------------------------|------|----------|----------------|--------------------------|-----------------|-------------------|
| 192.168.11.251 | All | 514 | tcp | on | certification validation | - | on |

Implementation reference:

[R82.10 Gaia Administration Guide](#) > System Management > System Logging > Configuring System Logging in Gaia Portal > Configuring the Remote System Logging.

Restrict Access to Lights Out Management (LOM / Out of Band Management)

Many Check Point Appliances include a Lights Out Management (LOM) or out of band management interface that provides direct, low level access to the system, including remote console, power control, and hardware monitoring capabilities.

This interface operates independently of the Gaia OS and security policy, and therefore must be treated as highly privileged infrastructure access.

Recommendation:

Ensure that the LOM interface is:

- Not directly exposed to the Internet.
- Connected only to a dedicated, secured management network.
- Accessible only from explicitly authorized source IP addresses.

Access to the LOM interface must be tightly restricted and monitored.

Why:

- LOM provides direct hardware level control, bypassing operating system and security policy enforcement.
- Unauthorized access to LOM can allow:
 - Full system control (including reboot and console access).
 - Modification of boot behavior.
 - Access to sensitive system information.
- As attackers increasingly target management and control planes, out of band interfaces represent a high impact entry point if not properly isolated.
- Improper exposure (for example, direct Internet connectivity) significantly increases the risk of unauthorized access.

Advanced Hardening (High Security Environments Only)

Explicit Rules Instead of Implied Rules

Recommendation: Replace implied rules with explicit Access Control rules only in high security environments, following the Check Point guidance exactly.

Explicit rules increase visibility and auditability, but incorrect rules can break policy installation and management/log connectivity.

Implementation reference:

[sk179346 - Configuring an Explicit Rule instead of Implied Rules.](#)

Deployment Checklists

Use these checklists during deployment and periodic security reviews.

Quick Checklist (All Environments)

- Implement a Stealth Rule for a Security Gateway (drop non-required traffic directed to the Security Gateway).
- Review and (where needed) enable logging for Implied Rules.
- Place Management Server in a protected segment behind a firewall.
- Restrict admin access by source IP (jump hosts / admin networks only).
- Enforce MFA for administrators via Identity Provider.
- Remove / disable unused administrator accounts.
- Apply latest recommended Hotfix / Jumbo Hotfix Accumulator Take and confirm update health.
- Harden Gaia OS: password policy, SNMP, routing (only if needed), restrict Expert mode.
- Use least privilege credentials for AD / Cloud / API integrations and maintain an inventory.