Check Point R81.10 for Gateway and Maestro Configurations

INSTALLATION AND CONFIGURATION

Administration Guide

Revision 002
20 October 2022

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 https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Check Point R81.10 CC Installation and Configuration Admin Guide

For more about this release, see sk173465 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk173465.

Document History

Revision	Date	Description
001	18 October 2022	First release of this document
002	20 October 2022	Minor correction

CHECK POINT
YOU DESERVE THE BEST SECURITY

Contents

Introduction

This document describes the delivery and operation procedures that must be implemented by Check Point Software Technologies Ltd. customers and/or resellers to ensure the secure delivery, installation, generation, and start-up of Check Point Security Gateway Appliances in accordance with the Common Criteria evaluated configuration, as defined in the Check Point R81.10 for Gateway and Maestro Configurations Security Target.

The guidelines provided in this document explain how to use the existing Check Point Installation process to set up Check Point Gateway and Maestro Appliances in a manner that is consistent with the evaluated configuration. This guidance must be read in conjunction with the referenced installation and configuration guides, and is written to take into account the specific details and settings that are required to conform with the evaluated configuration.

These guidelines and requirements are most often exceptions to the instructions written in the referenced documentation. If a feature or service is listed below, you must configure the mentioned item as described here. If a feature or service is not listed below, configure it as written in the referenced documentation.

If you follow the requirements in this document when setting up and using the system, your configuration will match the evaluated configuration.

Note - Legitimate reasons may exist to modify the system setup in ways not described here, if that is necessary for the system to fulfill its intended purpose. However, the evaluation results may not apply to such a configuration.

Who Should Use This Guide?

This guide is for IT staff who are installing *Check Point R81.10 for Gateway and Maestro Configurations*.

Note - In the Target of Evaluation (TOE), one type of security administrator (with full privileges) is in the evaluated configuration.

Related Documentation

The evaluated configuration is described in:

- Check Point Software Technologies Ltd. R81.10 for Gateway and Maestro Configurations Security Target

The Check Point Management REST API provides the only supported interface for administration of the Security Management Server. It is documented in the Management API Reference https://sc1.checkpoint.com/documents/latest/APIs/index.html. This communication is protected over a TLS v1.3 connection.

The subset of REST API allowed in the evaluated configuration is provided at REST API Allowed Calls (on page 81).

The Orchestrator appliance is administered through the Maestro Gaia portal (webUI). This is also protected over a TLS v1.3 connection.

The Common Criteria Evaluated Configuration

Evaluated Configuration

The information provided in this document details the evaluated configuration for the certification. Administrator changes to configuration are outside the scope of the certification, so should not be made.

Physical Components of the Evaluated Configuration

The evaluated configuration includes the following components:

- A Check Point Smart-1 Security Management Server appliance installed with its evaluated R81.10 firmware image.
- When in single appliance deployment:
    - A **Check Point Security Gateway** appliance installed with its evaluated R81.10 firmware image.
- When in Scalable Platform deployment:
    - Multiple **Check Point Scalable Platform (Maestro) Gateway** appliances installed with the evaluated R81.10 firmware image.
    - One or more **Check Point Maestro Hyperscale Orchestrator** appliances installed with the evaluated R81.10 firmware image.

The hardware platforms used to evaluate the TOE firmware:

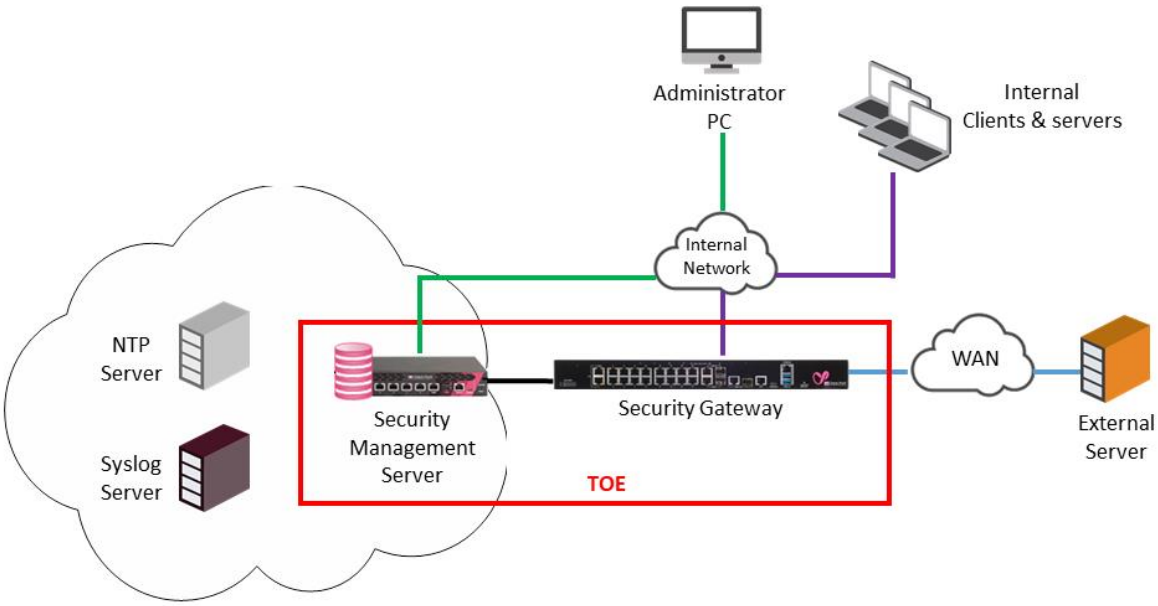
- Maestro appliances running **R81.10** firmware:
    - Maestro Hyperscale Gateway
        - 6200, 6600, 6700, 7000, 16600, 28600
- Security Gateway appliances running **R81.10** firmware:
    - High End Enterprise Data Center
        - 16000, 16200, 26000, 28000, 28600, 16600
    - Enterprise
        - 6200, 6400, 6500, 6600, 6700, 6900, 7000
    - Small Business and Branch Office
        - 3600, 3800
- Virtual appliances running **R81.10** firmware (VM image including the Security Gateway appliance firmware image):
    - CloudGuard for ESXi running on a HPE D360 G10

- Smart-1 Security Management Server appliances running the Gaia **R81.10** firmware (Security Management Server image)
- High End Enterprise:
    - 625, 600-M, 600-S, 6000-L, 6000-XL
- Orchestrator appliances running the Gaia **R81.10** firmware
    - Maestro Hyperscale Orchestrator 140
    - Maestro Hyperscale Orchestrator 170
    - Maestro Hyperscale Orchestrator 175

The Administrator of the Target of Evaluation (TOE) additionally requires a direct console CLI connection during the TOE installation and configuration, and a host co-located on the internal protected network with the Security Management Smart-1 for managing the TOE over Check Point REST API.

Check Point Security Gateway Appliances mediate information flows between clients and servers located on internal and external networks governed by the firewall, as shown in Figure 1 below. The TOE imposes traffic-filtering controls on mediated information flows between clients and servers according to the site's security policy rules.

Figure 1 TOE deployment – single appliance

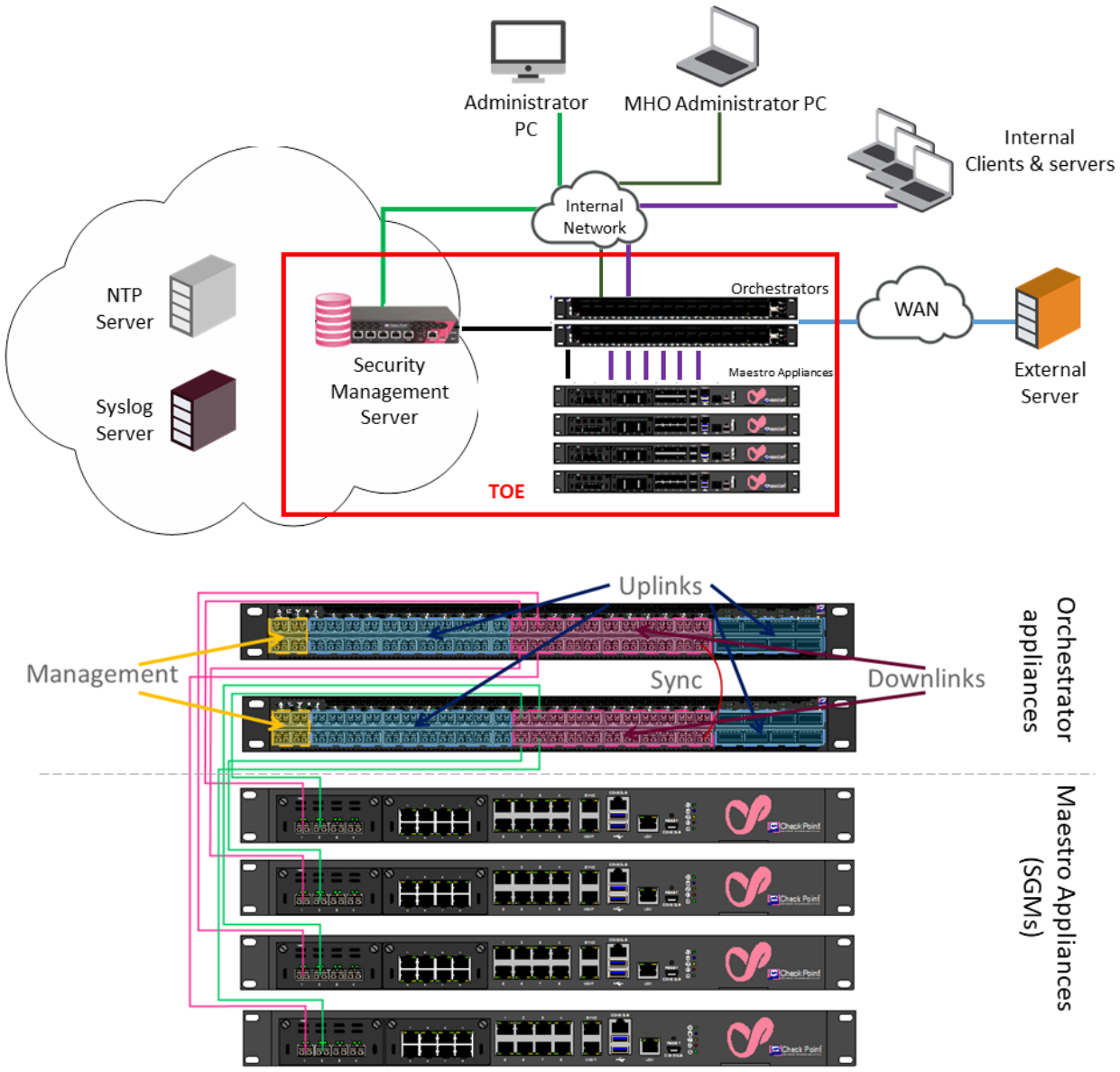


The following figures show firstly an example Scalable Platform deployment and secondly the connection of the Maestro components (Orchestrator appliance and Maestro appliances) within a Scalable Platform deployment. The Orchestrator appliances must be physically located in the same protected environment.

In Scalable Platform, deployment traffic is received from untrusted networks by Orchestrator appliances which then distribute the traffic to the SGMs (the SGMs in Scalable Platform deployment are also known as Maestro appliances). The security and Threat Prevention policies are enforced on the traffic by each SGM, before the SGM forwards the traffic to the

trusted networks via the Orchestrator appliance downlink. Every SGM in the cluster has the same security policy.

Figure 2 TOE deployment – Scalable Platform



The evaluated configuration is configured to interact with these external entities:

- NTP servers for time synchronization
- External syslog server
- Administrator PC host

Traffic inspection is the same whether the TOE is configured as a single appliance or as part of a Scalable Platform deployment with Maestro components.

To operate in a Scalable Platform deployment Security Groups are established. A Security Group is a logical group forming an active / active cluster segregated from other Security Groups. Security groups include network interfaces (uplinks), Management interfaces and Appliances (SGMs). A single IP address is assigned per Security Group for management communications and policy installation. This is concept is known as Single Management Object (SMO).

There is a relationship between a downlink port and SGM, so in this way an Orchestrator appliance determines which SGM will inspect the traffic.

The Orchestrator appliance provides traffic load-balancing mechanisms across Security Group members, calculating traffic distribution dynamically so that members of the security group can be seamlessly added and removed. HyperSync is used as the Cluster Synchronization mechanism.

Within the same cluster (Security Group) each connection is synchronized to two Security group members (Active and Backup). One of SGMs is Active per given connection (it enforce security policy with all related inspections and protections), another one is Backup (keep connection in its connection table) and will replace Active in case of failure. The SGM receiving the connection will decide which is its backup SGM, and will forward connection information to that backup SGM over the SYNC-VLAN. The REST API is used by the SGM to inform Orchestrator if a SGM is unavailable.

The Security Groups are managed from an MHO Administrator PC using the Maestro Gaia portal (WebUI) provided on the Orchestrator appliance. This communication between the MHO Administrator PC and the Orchestrator appliance is protected using TLS v1.3.

When a new SGM is added to a cluster, Orchestrator uses LLDP (Link Layer Discovery Protocol) to discover it and notify the other SGMs that a new SMG has been added.

In a Single site deployment, all components (SGMs, Orchestrator appliances and, Management Server) are all physically connected using Direct Attached Copper (DAC) or fiber cables, within a single secure location. Use of multiple Orchestrator appliances within a single site deployment is supported. The Orchestrator appliances communicate with each other using REST API. In a dual site deployment, a direct (tunneled) connection is required between the two Orchestrator appliances, which is also communication in the environment of the TOE. However, this dual site deployment is outside the TOE configuration.

Functionality Excluded from the Evaluation

The Check Point Security Gateway appliances can provide a broad range of services (product types), features and capabilities. Functionality is excluded from the evaluation if a feature is:

- Disabled in the evaluated configuration
- Not configured and therefore not enabled in the evaluated configuration
- Unavailable where additional products or licenses are required

The features below are only allowed to be configured only during the installation and configuration process:

1. Configuration of Secure Internal Communications protocol for Security Management Server and Security Gateway appliances.
2. WebUI for Management, Gateway and SP Gateway (disabled in “Installation Setting” section)
3. SSH (disabled in the “Post Install Configuration” section)
4. CLI system administration interfaces
5. LOM (iDRAC) Management for Smart-1 626/6000-L/6000-XL/600-M Appliances (disabled by default and by executing “UnsetiDRACUser <UserID>” through expert mode)

Table 1 Functionality excluded from the evaluated configuration and how it is excluded

Functionality excluded from the evaluation	**How it is excluded**	**Guidance to Administrator**
Security Gateway appliances and Security Management appliances hardware	N/A	N/A
IPv6	Disabled by default	Do not configure on NIC
VPN, including IKE v2/IPsec interface for realization of Virtual Private Networks	Disabled by default	Do not configure
The Online Certificate Status Protocol (OCSP) interface	Disabled by default	Do not configure
SecureXL and PPack	Blocked by default	None
Configuration of Secure Internal Communications protocol for Security Management Server and Security Gateway	SIC must be configured before the TOE is operational . No further action is required.	None during operation of the TOE
IPsec clients	Disabled by default	Do not configure
TLS-based VPN functionality	Blocked by default	None
Anti-virus functionality	Disabled by default	Do not configure
SNMP daemon	Disabled by default	Do not configure

Functionality excluded from the evaluation	How it is excluded	Guidance to Administrator
Dynamic Routing and Constraint-based Routing Label Distribution Protocol (CR-LDP)	Disabled by default	Do not configure
Management Server WebUI – web-based system administration of the Smart-1 Security Management Server	Blocked by default	None
SSH	Blocked by default	None
CLI system administration interfaces	Administrator Guidance	Do not use
LOM (iDRAC) Management for Smart-1 625/6000-L/6000-XL/600-M/600-S Appliances	Disabled by default and by executing `UnsetiDRACUser <UserID>` through expert mode	None
CPMI	Blocked by default	None
GUI Clients (e.g. SmartConsole)	Blocked by default	None
On-line IPS Update	Blocked by default	None
Administrator authentication protocols: RADIUS, LDAP, TACACS, TACACS+	Disabled by default	Do not configure
Remote management (management through a public network)	Disabled by default	Do not configure
Virtual Systems and VSX	Disabled by default	Do not configure
Clustering	Disabled by default	Do not configure
Proxy servers (including HTTPS, SMTP, FTP, Telnet)	Disabled by default	Do not configure

Functionality excluded from the evaluation	How it is excluded	Guidance to Administrator
Certificate-based administrator authentication	Disabled by default	Do not configure
SSL Network Extender	Disabled by default	Do not configure
OPSEC and associated interfaces	Disabled by default	Do not configure
Administrator permission profiles	Disabled by default	Do not configure
Administrator management	Disabled by default	Do not configure
Mobile Access	Disabled by default	Do not configure
Multi-Domain management	Disabled by default	Do not configure
Data Leakage Prevention - DLP	Disabled by default	Do not configure
Identity Awareness	Disabled by default	Do not configure

Security Environment Considerations

The following issues should be taken into account when preparing the security environment of the evaluated configuration.

Physical Access Control: Physical access must be controlled. The Security Management Server, Check Point REST API workstations, and firewall appliances must be located in secure locations, protected from physical access by unauthorized persons.

Permitted Applications: You may not install any general-purpose applications, public data or other capabilities that are outside the evaluated configuration on any firewall or Security Management Server host. In particular, you must not install services (e.g. an FTP server) that can be accessed remotely by non-administrative users.

Trustworthy Administrators: Only trustworthy administrators should receive authorization to manage the evaluated configuration.

Traffic Mediation: A configured firewall shall mediate traffic for at least two networks. You must ensure that all information paths between mediated networks pass through a firewall in the evaluated configuration.

Administrative Workstation: The evaluated configuration of R81.10 firmware shall be managed from an administrative workstation, through the Check Point REST API.

Preventing Access by Untrusted Users: The following components must be installed on subnets connected to a firewall interface that is protected by the Security Policy such that they cannot be accessed by untrusted users.

- Check Point Smart-1 appliance
- Administrator PC host (for administration of the Security Management Server) and MHO Administrator PC (for administration of the Maestro Orchestrator)
- NTP server
- Syslog server

Restricted Access to Directly-connected LANs: Recommended network configurations place additional network equipment (i.e. routers and/or switches) between users and Security Gateways.

Table 2 Functionality excluded from the evaluated configuration and how it is excluded

Functionality excluded from the evaluation	How it is excluded	Guidance to administrator
LOM	Disabled by default	Do not configure

Secure Delivery Procedures

Overview

This section provides information on verifying the secure delivery of the Check Point Security Gateway Appliances and Smart-1 Appliances. Product delivery consists of hardware and software components.

Check Point Security Gateway Appliances are not sold by Check Point directly to customers. Instead, Check Point makes use of established Value Added Resellers (VARs) to sell its software and hardware. A customer purchases the certified system by placing an order for the software with a distributor. Customers purchase third-party evaluated hardware directly from the hardware manufacturer.

Note - Check Point resource for contacting its sales organization: http://www.checkpoint.com/sales/index.html

The customer is then responsible for completing the installation and configuration of the evaluated configuration, as described in this guide.

Hardware Delivery

Hardware Platforms

The evaluated configuration in Check Point manufactured appliances for the Security Gateway and Smart-1 Security Management Server.

The customer purchases the hardware appliance identified in the *Check Point R81.10 Gateway and Maestro Configurations Security Target*, and installs the R81.10 firmware.

Standard PC workstations are required by the trusted administrator in the Management Network for managing the Security Management Server (over the Check Point REST API) and the Maestro Orchestrator (via the Maestro Gaia portal). The workstations are not considered part of the TOE, and is not specified in the Security Target.

Hardware Acquisition and Delivery

Check Point Security Appliances are manufactured by a trusted Check Point supplier, and shipped from regional distribution centers directly to the customer-specified location. The hardware platforms identified in the Security Target have been validated to assure the correct operation of the underlying hardware and firmware in order to meet the security requirements of the evaluated configuration. It is important that the customer ensure that valid hardware has been received.

The following are recommendations that can be used to further mitigate the risks of hardware substitution:

- Buy hardware from people you trust. In particular, it is good practice to purchase hardware directly from the hardware vendor, according to the procedures provided on the hardware vendor's web site.
- Prefer new hardware to used or refurbished equipment.
- Attempt to make hardware purchases seem random. If possible, do not identify upfront the purpose for which these platforms are going to be used. Use platform types that have been purchased by your organization for other purposes as well.
- Use reputable commercial carriers to deliver hardware to your organization. Request tracking information and use shipper web sites to determine that the hardware did not take any suspicious routes or was mislaid en-route. Where possible, pick it up yourself.
- Apply physical access controls throughout the hardware platform's lifetime, including any periods of time when the hardware is in storage, before product installation.

If the hardware is to be installed in extreme environmental conditions (heat, cold, humidity, power spikes, vibration, etc.), verify that these conditions are compatible with the hardware vendor's specifications.

Hardware Verification Procedure

Use the following steps to verify that valid hardware has been received:

- Examine the outside packaging and markings of the delivery container containing the hardware to ensure that it arrived via the contracted commercial carrier from the hardware vendor.
- Examine the shipping and tracking information available with the package to look for any unexpected information related to the timing and route for the shipment. If there is any doubt about the veracity of the shipment, contact the vendor and confirm that the product was indeed ordered by your organization and sent by the vendor.
- Visually examine the hardware platform to determine that it is labeled in accordance with the hardware vendor's standard markings, and that it matches the platform model that was ordered.

Note - If the Check Point security appliances have been delivered with Lights Out Management (LOM) cards installed, do not enable the cards in the BIOS menu.

Software Delivery

Software Package Distribution

Each release of the product is identified by a unique reference that consists of a release number and (after the initial base release) a Hotfix Accumulator (HFA) designator.

Check Point releases and hotfixes are distributed to customers as downloadable packages off the Check Point web site. The HFA installation is applied as an upgrade to the General Availability (GA) release, or to previous HFAs, replacing one or more packages with newer builds of those packages.

Note - Releases are distributed electronically as `.iso` files. HFA and hotfix packages are typically distributed as compressed file archives that are installed as upgrades to an already-installed appliance.

The unique reference for the evaluated firmware is identified in the *Check Point R81.10 Gateway and Maestro Configurations Security Target*. Check Point provides a CLI-based CPInfo utility for a complete breakdown of the installed image. The output for each of the TOE firmware images is provided in an appendix provided to the Security Target. The administrator is instructed to use this for validating receipt of the TOE evaluated image.

The physical boundary of the TOE is the Security Gateway Appliances R81.10 firmware and Security Management Server firmware (i.e. it is a software-only TOE boundary). There are three variants of the R81.10 firmware depending on which the Gaia operating system is supported by the appliance:

Table 3 TOE Firmware Packages

Firmware Package	Download file	SHA-256 hash value
Security Gateway or Management Server	Check_Point_R81.10_T335.iso	17817e134c4f0a1c65b59af74baab8939b29a64f653476cad5e4b219f5fd147d
Scalable Platform (Maestro) Gateway and Maestro Hyperscale Orchestrator	Check_Point_R81.10_T338_ScalablePlatform.iso	4215084137b8b66185340f9ec09592ec172b039f4b390547ae31b074b9c5b621
R81.10 EAL4 certification Hotfix	Check_Point_R81_10_JHF_T22_EAL4_HF_MAIN_Bundle_T4_FULL.tar	754e0d0604da6b773dc6d1db6035fd581835976c36c2d32a60d8S20c160b75b

`show version all`

Security Gateway appliance	Maestro appliance
Product version Check Point Gaia R81.10	Product version Check Point Gaia R81.10
OS build 335	OS build 338

OS kernel version 3.10.0-957.21.3cpx86_64	OS kernel version 3.10.0-957.21.3cpx86_64
OS edition 64-bit	OS edition 64-bit

Smart-1 Security Management Server	Orchestrator appliance
Product version Check Point Gaia R81.10	Product version Check Point Gaia R81.10
OS build 335	OS build 338
OS kernel version 3.10.0-957.21.3cpx86_64	OS kernel version 3.10.0-957.21.3cpx86_64
OS edition 64-bit	OS edition 64-bit

```
cpinfo -y all
```

Security Gateway appliance (the order may be different)
This is Check Point CPinfo Build 914000215 for GAIA
[IDA]
No hotfixes
[MGMT]
HOTFIX_R81_10_JHF_T22_EAL4 _HF_MAIN Take: 4
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 HOTFIX_GOT_TPCONF_AUTOUPDATE
FW1 build number:
Check Point software version R81.10 - Build 883
kernel: R81.10 - Build 002
[SecurePlatform]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[PPACK]
No hotfixes..
[AutoUpdater]
No hotfixes
[CPinfo]
No hotfixes
[DIAG]
No hotfixes
[CVPN]

Security Gateway appliance (the order may be different)
No hotfixes..
[hcp_wrapper]
HOTFIX_HCP_AUTOUPDATE
[CPUpdates]
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 BUNDLE_GOT_TPCONF_AUTOUPDATE Take: 96 BUNDLE_HCP_AUTOUPDATE Take: 44

Maestro Gateway (Scalable Platform Security Gateway) appliance
This is Check Point CPinfo Build 914000215 for GAIA
[IDA]
No hotfixes
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 HOTFIX_GOT_TPCONF_AUTOUPDATE
FW1 build number:
This is Check Point's software version R81.10 - Build 884 kernel: R81.10 - Build 002
[SecurePlatform]
HOTFIX_R81_JHF_T22_EAL4_HF_MAIN Take: 4
[PPACK]
No hotfixes..
[AutoUpdater]
No hotfixes
[CPinfo]
No hotfixes
[SMO]
No hotfixes..
[DIAG]
No hotfixes
[CVPN]
No hotfixes..
[hcp_wrapper]
HOTFIX_HCP_AUTOUPDATE
[CPUpdates]

Maestro Gateway (Scalable Platform Security Gateway) appliance
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 BUNDLE_GOT_TPCONF_AUTOUPDATE Take: 96 BUNDLE_HCP_AUTOUPDATE Take: 44

Smart-1
This is Check Point CPinfo Build 914000215 for GAIA
Local host is not a Gateway
[IDA]
No hotfixes
[MGMT]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 HOTFIX_GOT_MGMT_AUTOUPDATE HOTFIX_WEBCONSOLE_AUTOUPDATE HOTFIX_GOT_TPCONF_MGMT_AUTOUPDATE
FW1 build number:
This is Check Point Security Management Server R81.10 - Build 220 This is Check Point's software version R81.10 - Build 883
[SecurePlatform]
HOTFIX_ R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[AutoUpdater]
No hotfixes..
[CPinfo]
No hotfixes..
[DIAG]
No hotfixes..
[Reporting Module]
No hotfixes..
[CPuepm]
No hotfixes
[VSEC]
No hotfixes
[SmartLog]
No hotfixes..
[SFWR77CMP]
No hotfixes..

Smart-1
[SFWR80CMP]
No hotfixes..
[R77CMP]
No hotfixes..
[R8040CMP]
No hotfixes..
[MGMTAPI]
No hotfixes..
[CPUpdates]
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 BUNDLE_DC_CONTENT_AUTOUPDATE Take: 12 BUNDLE_GOT_MGMT_AUTOUPDATE Take: 91 BUNDLE_DC_INFRA_AUTOUPDATE Take: 26 BUNDLE_WEBCONSOLE_AUTOUPDATE Take: 43 BUNDLE_HCP_AUTOUPDATE Take: 44 BUNDLE_GOT_TPCONF_MGMT_AUTOUPDATE Take: 32
[hcp_wrapper]
HOTFIX_HCP_AUTOUPDATE
[itp_wrapper]
HOTFIX_GOT_MGMT_AUTOUPDATE

Orchestrator appliance
This is Check Point CPinfo Build 914000215 for GAIA
[IDA]
No hotfixes
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
FW1 build number:
This is Check Point's software version R81.10 - Build 884
[SecurePlatform]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[PPACK]
No hotfixes..
[AutoUpdater]
No hotfixes.
[CPinfo]

Orchestrator appliance
No hotfixes.
[SMO]
No hotfixes..
[CPUpdates]
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4

HFA Downloads

As part of Check Point's Common Criteria-evaluated flaw remediation procedures, Check Point publishes updated Hotfix Accumulators (HFAs) and provides them to customers with a Software Subscription license.

The customer should check for updated HFAs for Check Point Software Technologies Ltd. R81.10 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher and request a hotfix from support for the TOE evaluated configuration.

WARNING - HFA downloads other than the identified evaluated versions are outside the evaluated configuration.

The Common Criteria evaluation was performed on the identified HF or HFAs as identified in the Security Target and this Installation Guide. Other HFAs might include changes to the product that violate evaluated security requirements.

However, it should be noted that the Check Point process for implementing and distributing HFAs was included in the evaluation. Given the above mentioned caveat, Check Point does recommend that customers download and install the latest HFA available. HFAs may only be installed during the installation and configuration. Therefore, when a new HFA is published, to install, you must consider the TOE to be out of operational use and back in its preparative state. Download and verify the package, and then install before considering it to be back in operational use.

Download the HFA package for the Gaia operating system. You will be asked to log in to your Check Point User Center account and agree to the Software Subscription Download Agreement. See information for User Center Registration and Access for instructions in Check Point User Center (on page 90).

License Confirmation and Verification

As part of the installation procedure of Check Point Security Gateway Appliances, it is necessary for a customer to enter his license details, which define the product purchased to the installation software.

Check Point provides instructions on how to register to the Check Point User Center and perform license registration. The customer registers the product, using the provided unique certificate key printed on the back of the case containing the purchased product. The Certificate key is a complex combination of alphanumeric and special characters which are not easily identified via a trial and error process. Once the certificate key has been entered,

customers are advised of the product type they have purchased. This is an initial check that the customer is getting the product that he/she intended to purchase. See the Check Point User Section (on page 90).

The permanent license required to install the product is then generated for the customer. Only those features bundled in the license are activated.

Single Gateway Deployment

In the context of this evaluation, a distributed deployment is supported.

You will need to:

- Install a Security Management Server
- Install one or more Security Gateway appliances
- Use a workstation for Check Point REST API communication to manage the Security Management Server

The Check Point Security Management Server is the server used by the Security Management Server Administrator to manage the Security Policy. The databases and policies of the organization are stored on the Security Management Server, and are downloaded to the Security Gateway.

Scalable Platform Deployment

In the context of this evaluation, a scalable deployment is supported.

You will need to:

- Install a Security Management Server
- Install one or more Orchestrator Security Gateway appliances
- Install one or more Maestro Gateway appliances
- Use a workstation for Check Point REST API communication to manage the Security Management Server and a workstation for WebUI communication to manage the Orchestrator appliance via the Gaia Portal

As for single gateway deployment, the Check Point Security Management Server is the server used by the Security Management Server Administrator to manage the Security Policy. The databases and policies of the organization are stored on the Security Management Server, and are downloaded to the Security Gateway.

In addition for Scalable Platform Deployment, the Orchestrator is the server used by the Orchestrator Administrator to manage the security groups of which the Maestro appliances are members.

Security Gateway

The Check Point Security Gateway is installed in its operational environment in a configuration where IP packets (datagrams) flowing between controlled networks are routed so that they pass through the Security Gateway. This allows the Security Gateway to inspect and optionally modify these information flows.

Maestro Gateway

The Check Point Maestro Gateway is installed in its operational environment in a configuration where Orchestrator redirects IP packets (datagrams) flowing between controlled networks to be scanned before they can be sent on. This allows the Check Point Maestro Gateway to inspect and optionally modify these information flows.

Security Management Server

The Security Management Server is the server used by the system administrator to manage the Security Policy. The databases and policies of the organization are stored on the Security Management Server, and are downloaded to the Security Gateway.

Orchestrator appliance

The Orchestrator appliance is used by the system administrator to manage the Security Groups and the traffic load balancing between the gateways within a Security Group.

Installation

Although outside their responsibilities once the TOE is operational, these are expected to be performed by those with the same authorization as:

- Security Management Server Administrator to install the TOE components for Single Security Gateway deployment.
- Both Security Management Server Administrator and Orchestrator Administrator for Scalable Platform deployment.

Pre-installation

Important - All the steps in the Installation and Configuration chapters must be completed before connecting the TOE to the internet.

1. Verify IP address allocations. Make sure you know what the network looks like.
2. Confirm that static DNS resolution is working properly. Make sure you know the DNS names that need to be resolved by the firewall and their addresses.
3. Have licensing information ready for the installation.
4. Download any applicable HFAs, software, and utilities.

Note - Administrators must check any download against the published hash (SHA-256), including Hotfixes and IPS signature updates before use.

R81.10 Fresh Installation

Overview

You must install each separate component on the relevant machine.

In single gateway deployment, install the Security Management Server .iso file on the Smart-1 appliance and install the applicable Security Gateway .iso file on the gateway appliance.

In scalable platform deployment, install the Security Management Server `.iso` file on the Smart-1 appliance, install the Maestro Gateway appliance `.iso` file on the gateway appliances and install the Orchestrator appliance `iso` file on the Maestro Hyperscale Orchestrator appliances.

After you complete installing a Security Management Server, Gateway or Orchestrator appliance, and you make them operational in your network, administrators must not log in directly into these hosts nor use the CLI interfaces.

Some tasks require access to the CLI. In particular, installing patches and hotfixes, adding network interfaces, reconfiguring the network, etc., are to be performed in the context of a reinstallation in order to ensure that the evaluated configuration remains in a secure state. It is possible to reinstall each host and appliance separately without requiring reinstallations of the other hosts.

The installation of HFAs that might be available at the time of installation: Check Point recommends that such HFAs be installed. However, such HFAs are not part of the evaluated configuration. For more details, see *HFA Downloads* in Software Delivery (on page 22).

The minimal evaluated configuration consists of one of each component.

Note - Additional Security Gateways may be installed as described above, after the evaluated configuration is made operational. There is no need to access the Security Management Server CLI for this purpose.

Introduction to Gaia OS installation

The installation of the Check Point Gaia operating system is the first installation step for the installation of the Gaia software.

The Gaia installation process includes:

- The **initial installation phase** in which the disk is formatted, and the operating system is installed.
- The **initial configuration phase** begins with a reboot of the operating system and an initial configuration session using the Web Portal. Configuration is completed via a console login.

Check Point Security Appliance Software Distribution

The Check Point Security Appliances are delivered with the appropriate Check Point Software Blades software pre-installed on the appliance. However, in order to ensure that the installed software version is identical to the evaluated version, it is recommended to download an appliance-specific image of the R81.10 firmware from the Check Point web site.

Installing the GAIA OS

1. Create a Check Point support center account and log in to the portal. Check the “User Center Authorization” section for instructions – sk93364 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93364.
2. Obtain the R81.10 ISO according to the “**Download URL**” column for each link.

Platform	**Download URL**
Security Gateway or Management	Check_Point_R81.10_T335.iso
Maestro Security Gateway	Check_Point_R81.10_T338_ScalablePlatform.iso

Maestro Orchestrator build guidance can be found in the URL below:

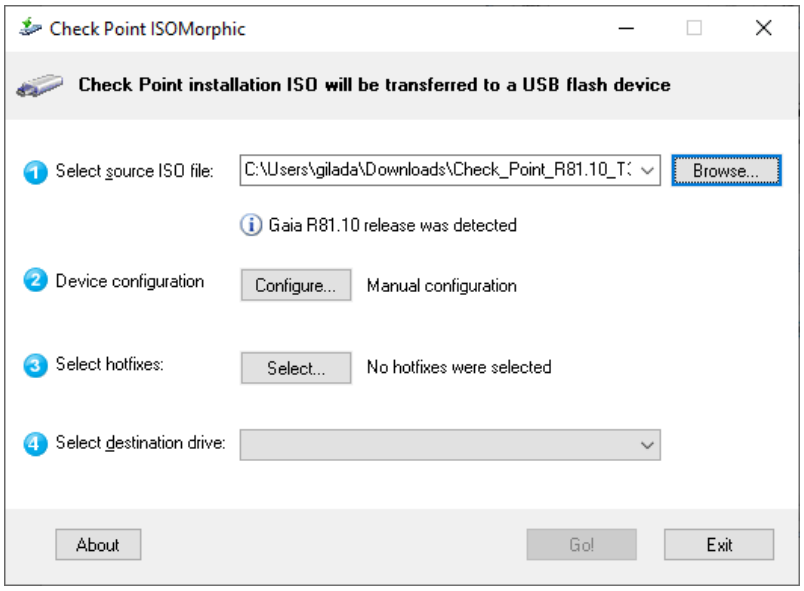
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk173363

1. Insert usb stick to the appliance and check device name by running “fdisk –l”
   Usually it will be /dev/sdb1
2. Start fdisk in interactive mode for the usb device (/dev/sdb) by running “fdisk /dev/sdb1”
3. Create new partition table by pressing ‘o’.
4. Create new partition by pressing ‘n’.
5. Choose primary partition by pressing “p” followed by Enter. Use default values and press enter 3 times.
6. Change the partition type by pressing “t” followed by Enter. New partition type id should be ‘7’ and press enter.
7. Save new configuration, press ‘w’.
8. Proceed to ISOMorphic instructions which will format it and flesh gaia version.

Disk on key instructions and download for the Check Point ISOMorphic tool can be found in sk65205
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk65205

Physical appliance installation (Non-VM)

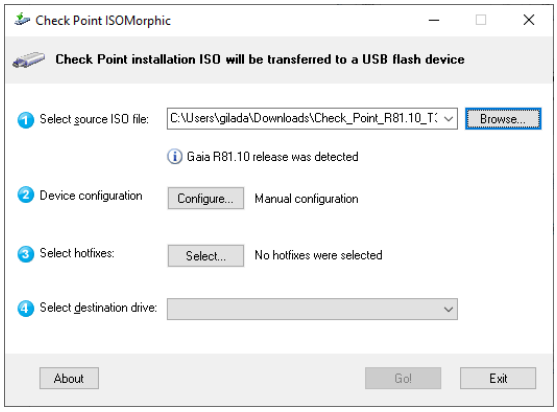
3. Open the ISOMorphic tool:



Select one of the ISO images obtained in step 2.

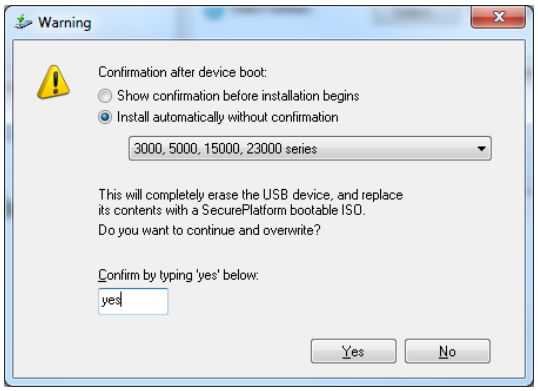
Note - The user will have to perform this procedure for both ISO images obtained in step 2: One for the Smart-1 and another for the appliance.

4. The main window opens again:



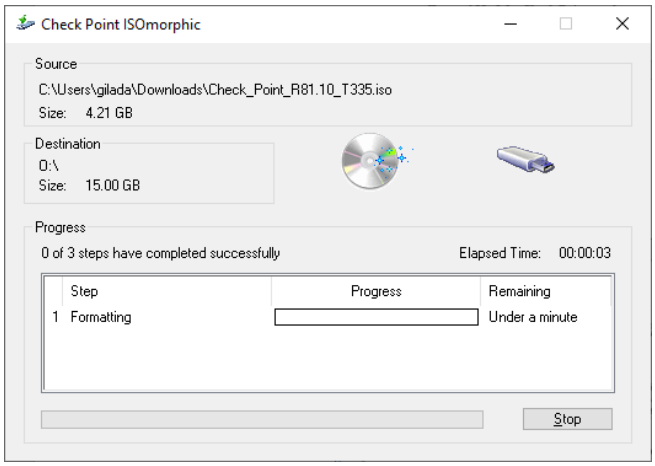
Select the destination USB drive and click **GO**.

5. A warning window opens.



Select **Show confirmation before installation begins**, enter **yes** in the confirmation box, and click **Yes**.

6. Installation is in progress:



7. The Success window opens:

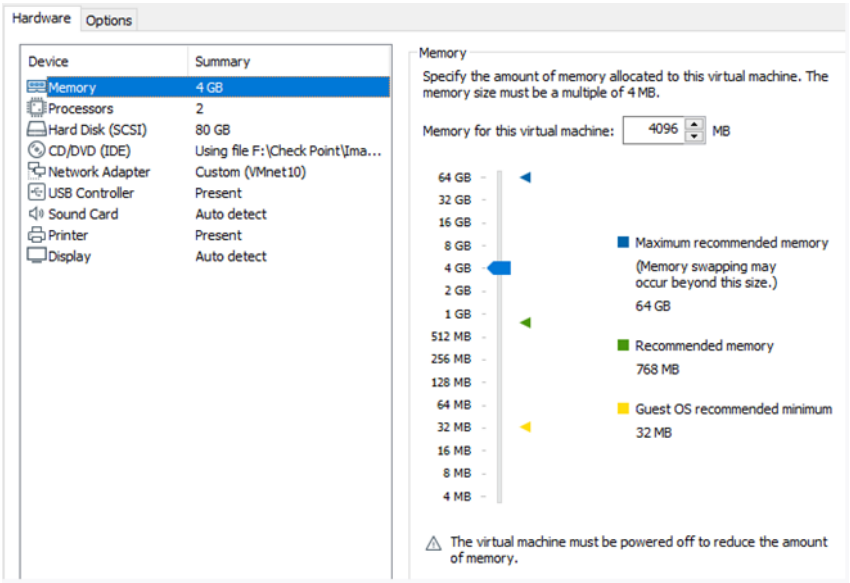
Click **OK**.

8. Insert the USB into the appliance and physically reboot it by turning it off and on.
9. Orchestrator only: Press ESC+7 during start up to enter the BIOS.
10. Orchestrator only: Type the BIOS password (NebulaH11) and press Enter.
11. Orchestrator only: Select the connected DOK device (Sandisk or similar), press Enter and boot.
12. Select the relevant appliance from the list once the USB device is booted.
13. The LCD panel (if it exists) and console show a success message for Smart-1 / Security Gateway appliance.

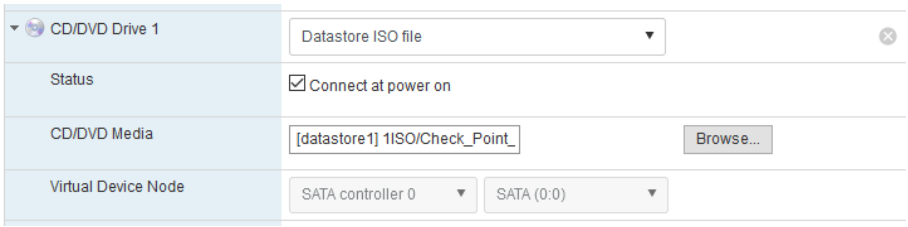
Disconnect the USB Disk On Key and reboot the appliance physically or by entering **Ctrl+C**.

Virtual Machine Installation

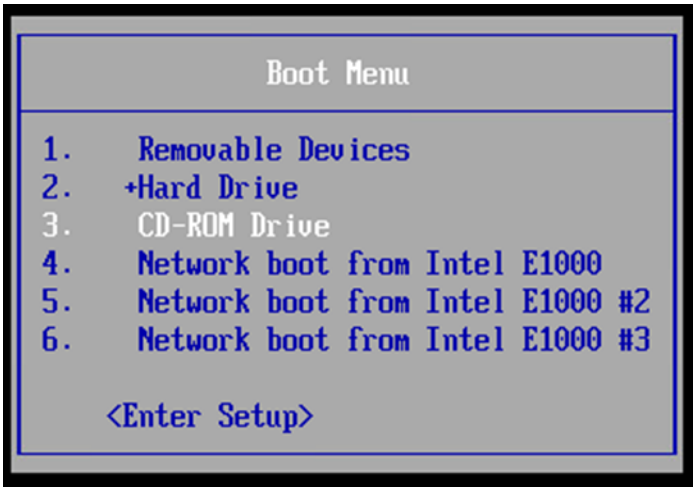
1. Copy the R81.10 ISO to the Virtual Machine host.
2. Create a new virtual machine according to the Check Point open server minimum requirements (4GB RAM and Intel Pentium IV, 2 GHz with 2 cores or equivalent and 110GB HDD):



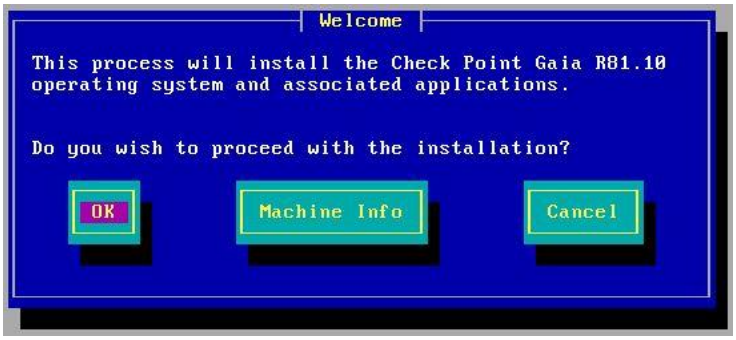
3. Mount the R81.10 ISO to the virtual machine DVD:



4. Power on the machine and boot from the ISO and boot from the CD/DVD drive:

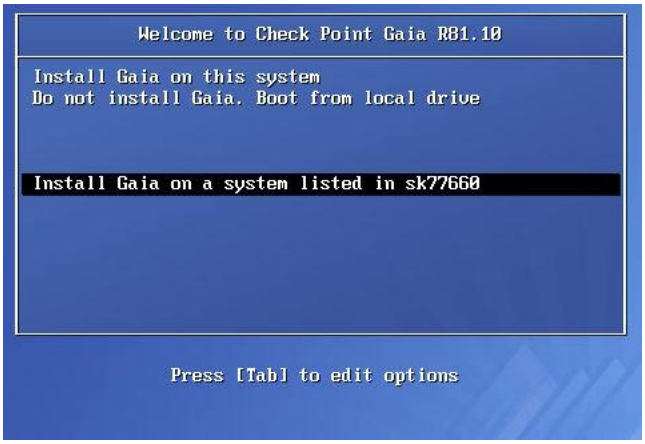


5. The first Welcome window opens:



Click **OK**.

6. The second Welcome window opens:

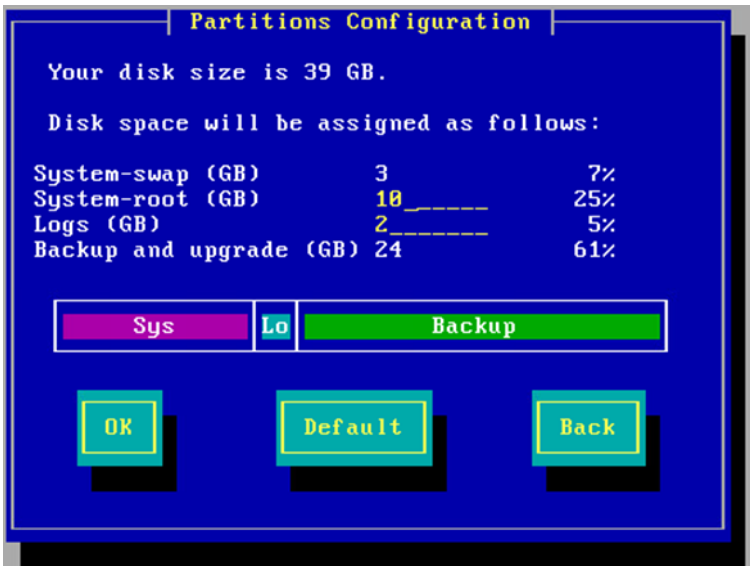


Select Install Gaia on this system and click OK.

7. The Language window opens:

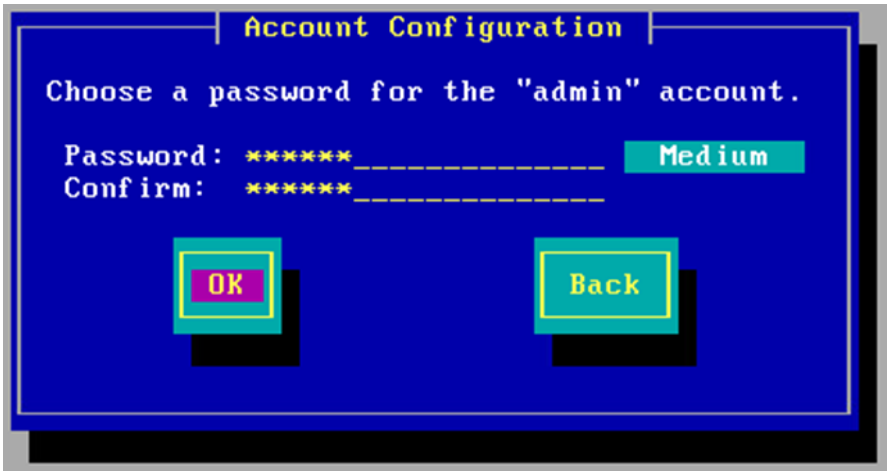
Select the desired language and click **OK**.

8. The Partitions Configuration window opens:



Change it according to your preference and click **OK**.

9. The Account Configuration window opens:

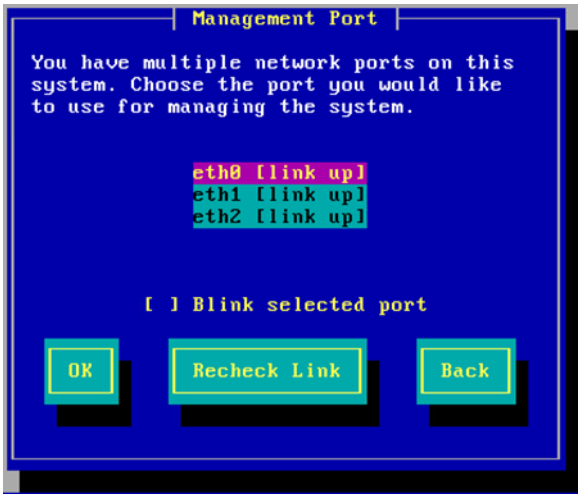


Enter the desired password twice and click **OK**.

The password must conform to the following operating system-enforced complexity requirements:

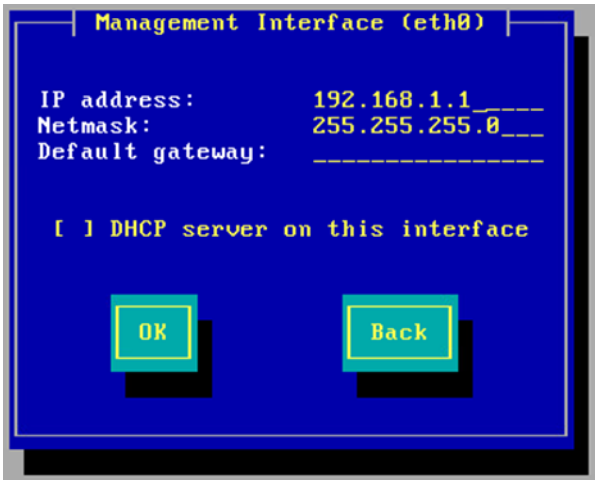
- At least 15 characters, in length
- A mixture of alphabetic, upper case, lower case, numeric and special characters
- At least four different characters
- Does not use simple dictionary words, or common strings such as “qwerty”

10. The Management port window opens:



Select the Management interface and click **OK**.

11. The Management interface window opens:

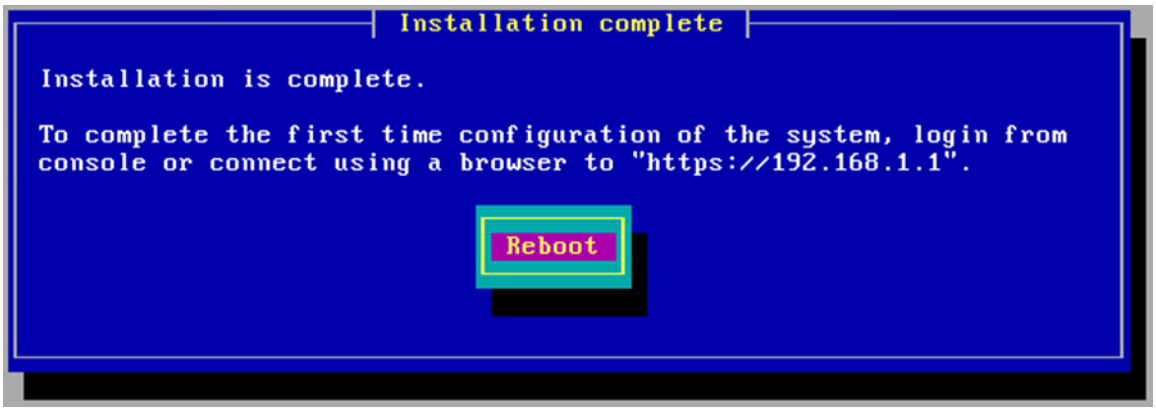


Enter the Management interface **IP address**, **Netmask** and **Default gateway** (if applicable) and then click **OK**.

12. The Confirmation screen opens:

Click **OK**.

13. The Installation completion window opens:



Click **Reboot**.

Console Login

1. Log in to the Gaia console interface.

For MHO (Orchestrator appliance):

a. Change the password according to the on screen instructions.

The password must conform to the following operating system-enforced complexity requirements:

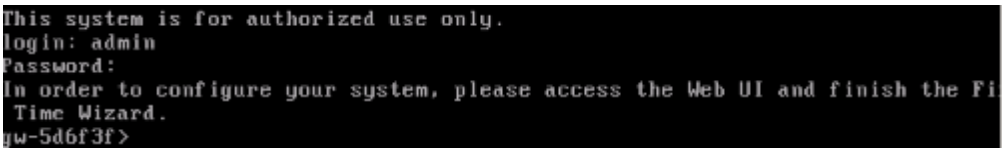
- At least 15 characters in length
- A mixture of alphabetic, upper case, lower case, numeric and special characters
- At least four different characters
- Does not use simple dictionary words or common strings such as "qwerty"

b. Press “y” followed by Enter key once asked for Orchestrator activation.

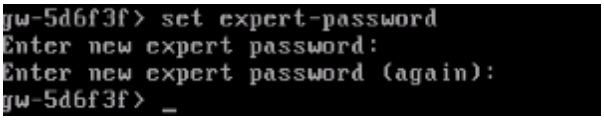
c. Type, “set hostname <hostname>” and press Enter.

For the non-MHO appliances:

- First Time Login - If you are logging in for the first time, use admin user and admin password (for VM use defined password).



Note - The password for the admin account is only used for the installation process. Do not perform a console login once the evaluated configuration is operational.



The password must conform to the following operating system-enforced complexity requirements:

- At least 15 characters in length
- A mixture of alphabetic, upper case, lower case, numeric and special characters
- At least four different characters
- Does not use simple dictionary words or common strings such as "qwerty"

2. Set the IP addresses and route using the commands below (but not on Maestro gateways):

```
set interface <interface> mask-length <Mask Length> mask-length <Mask Length>
set interface <interface> state on
set static-route default nexthop gateway address <default_gw_ip_address> on
```


3. Run: save config

Orchestrator appliance Login

1. On the MHO, Execute the commands below followed by the Enter key:

- "set expert-password"
- Type the current password and the new password twice
- "`set maestro configuration orchestrator-amount 1`" > "`y`" > type the administrator name > Press Enter > "`y`" > "`save config`".
- Enter expert mode by typing "`expert`" and typing the defined password
- "`orchd restart`" > "`y`" > type the administrator name > Press Enter > "`y`"

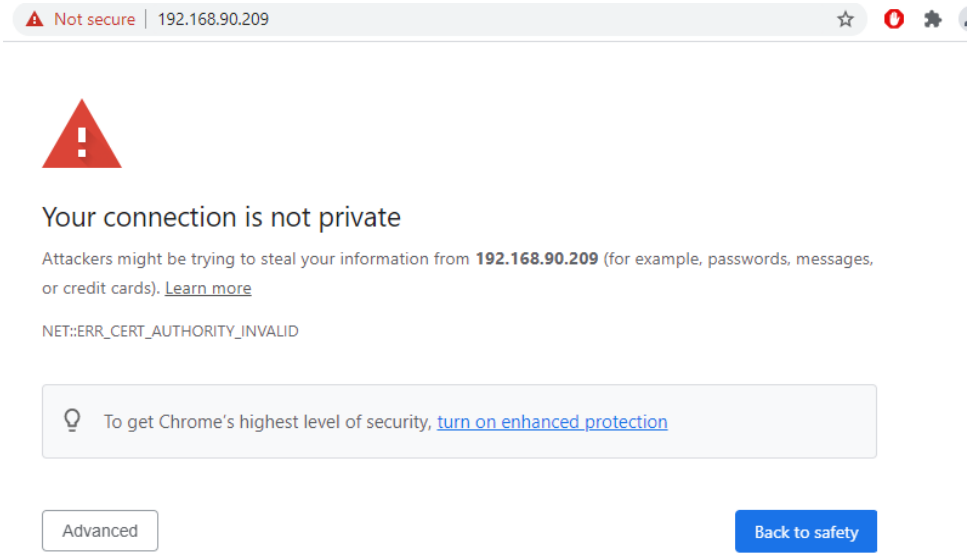
Installing the Security Gateway Appliance or Smart-1 Server

Gaia First Time Configuration Wizard (Single gateway deployment, non-SP)

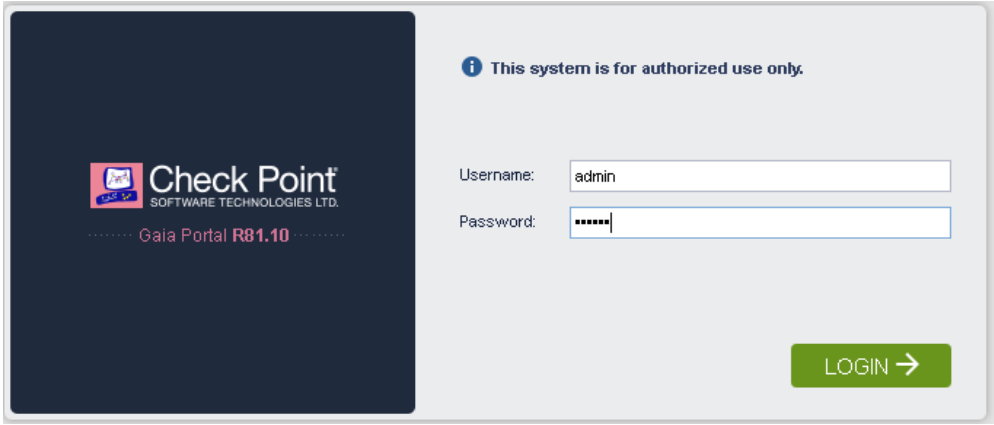
The Gaia Portal is a Check Point utility used to configure the Gaia operating system on both appliances. After connecting to the Gaia Portal, the First Time Wizard runs after the installation. It guides the administrator through the various menus.

1. Connect the Gaia portal using HTTPS on the defined port.

Note - Disregard the security certificate warning if displayed.

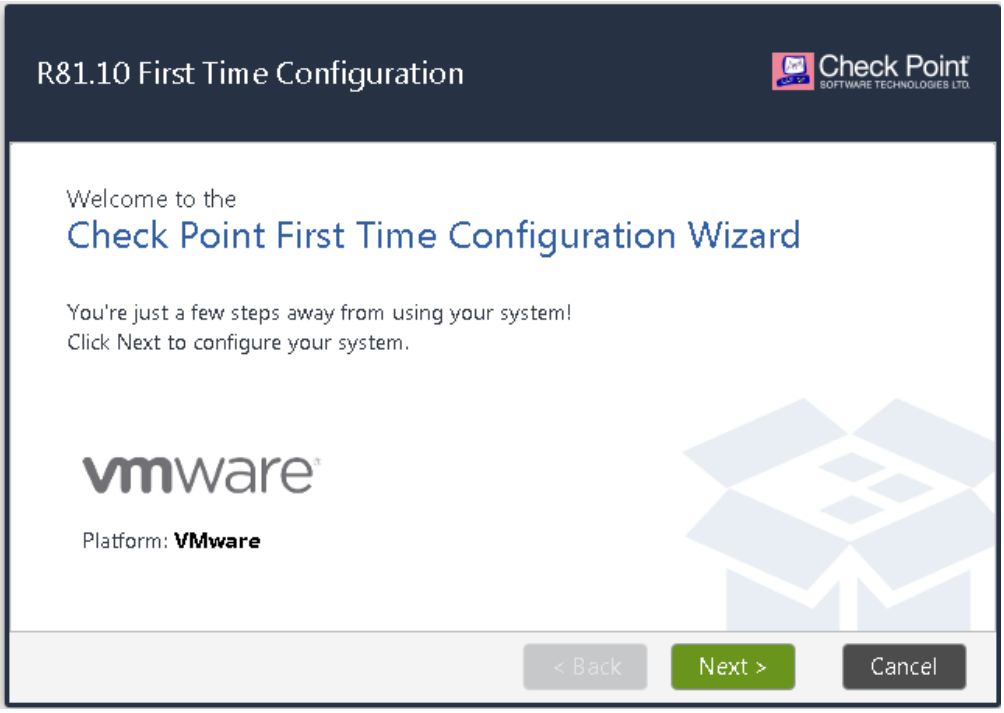


2. The login screen opens.



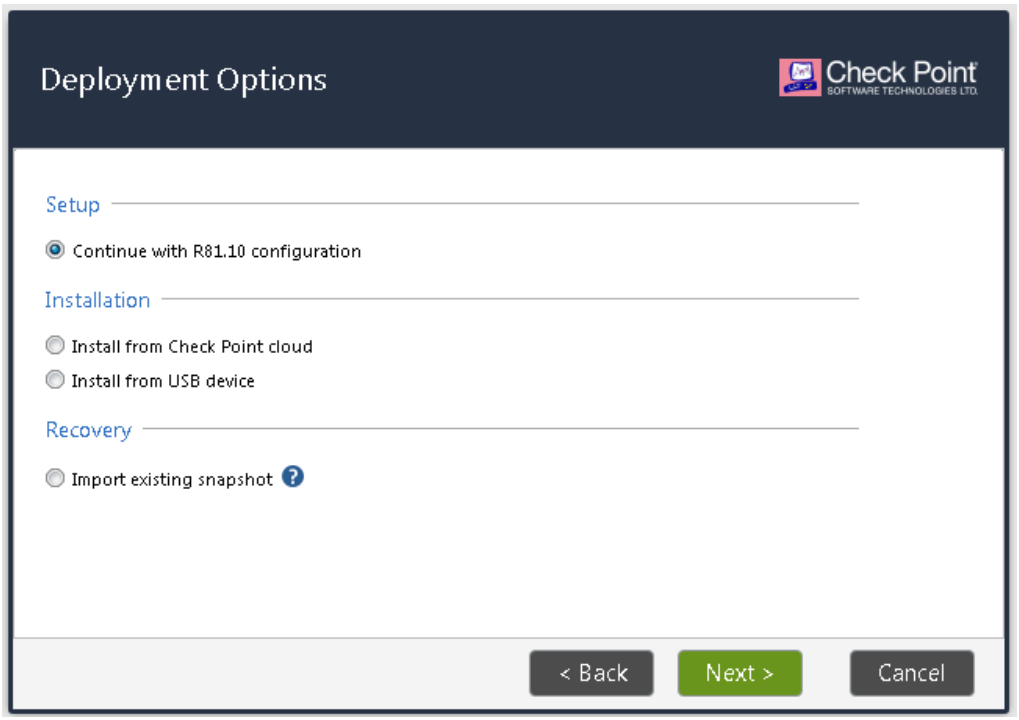
Enter the Username and Password and click LOGIN.

3. The Welcome window opens along with the platform type. Click **Next**.



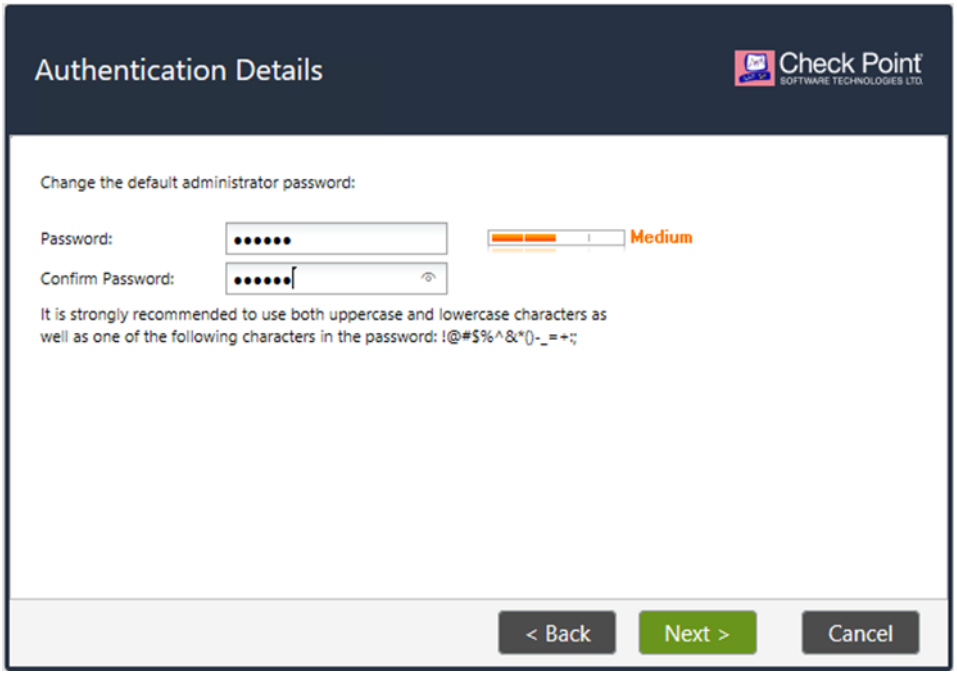
Click Next.

4. The Deployment window opens.



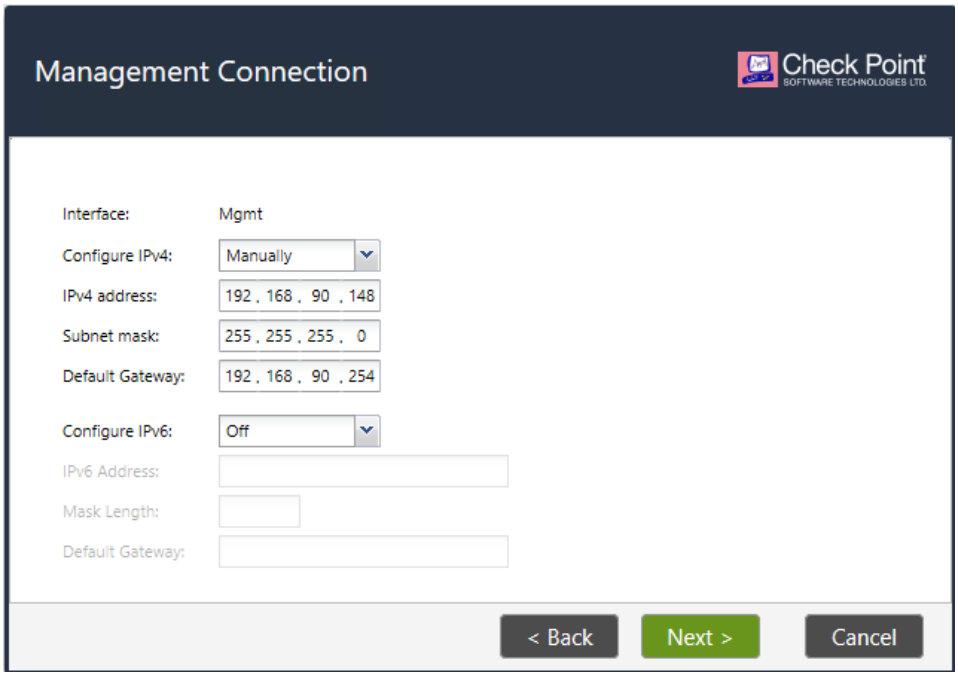
Click Next.

5. For some appliances, the Authentication Details window opens.



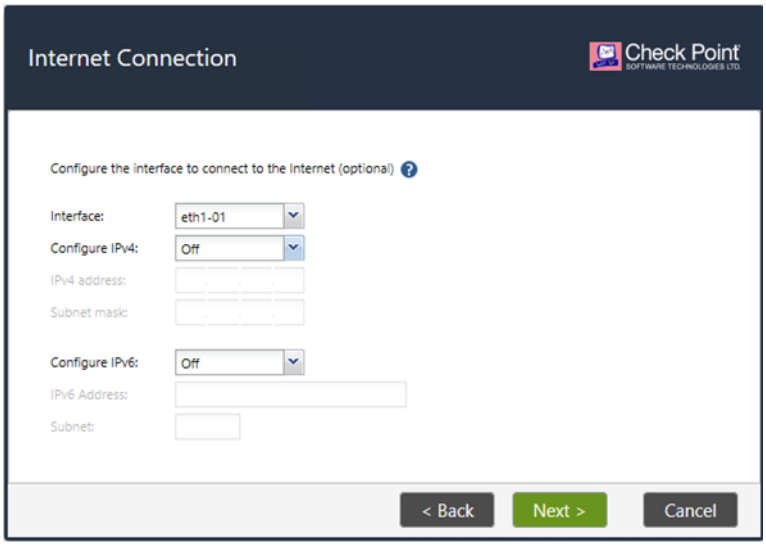
Define the desired Password and click Next.

6. The Management Connection window opens.



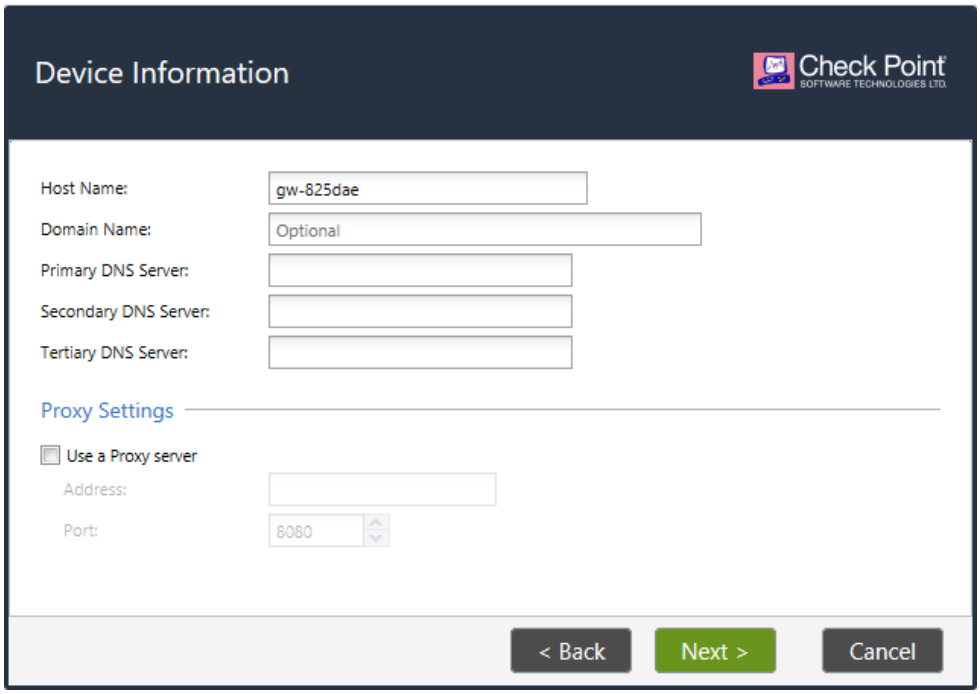
Define the management connection IP address and Subnet mask, and click Next.

7. The Internet Connection window opens.



On the Security Gateway only, define the internal connection IP address and subnet, and click Next.

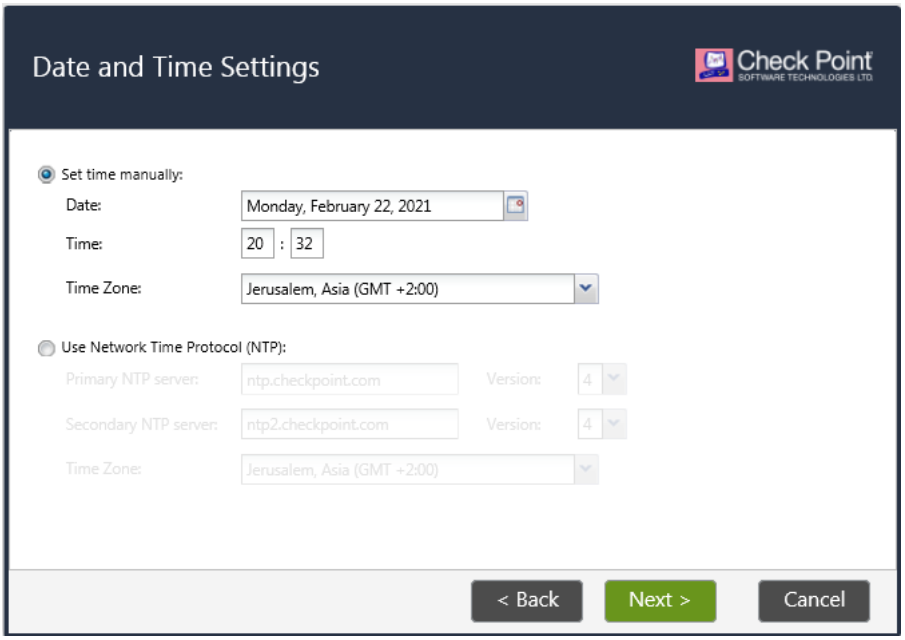
8. The Device Information window opens.



Enter the desired Host Name, Domain Name, DNS and Proxy servers.

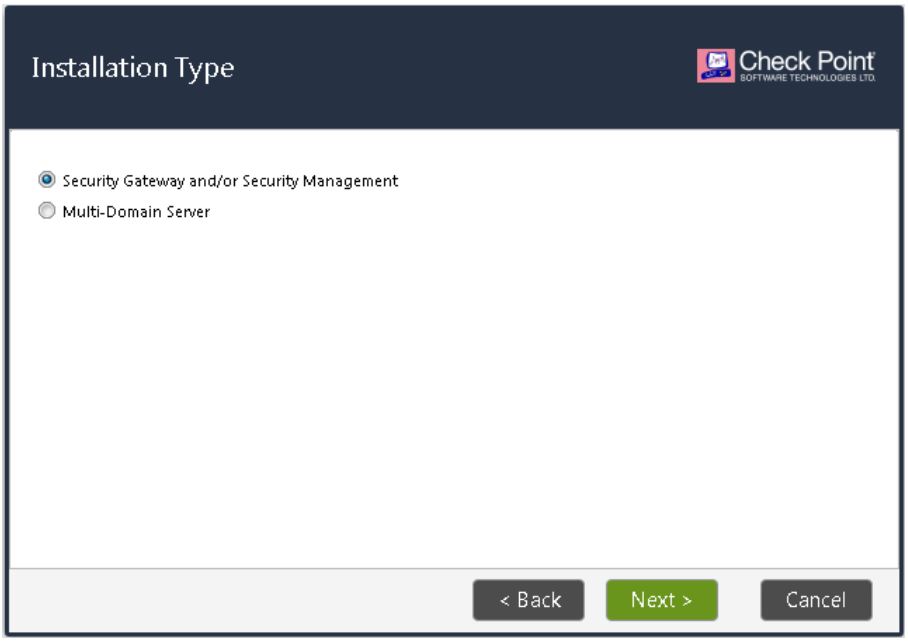
Click Next to continue.

9. The Date and Time Settings window opens.



Set the current Date, Time and Time Zone. Click Next.

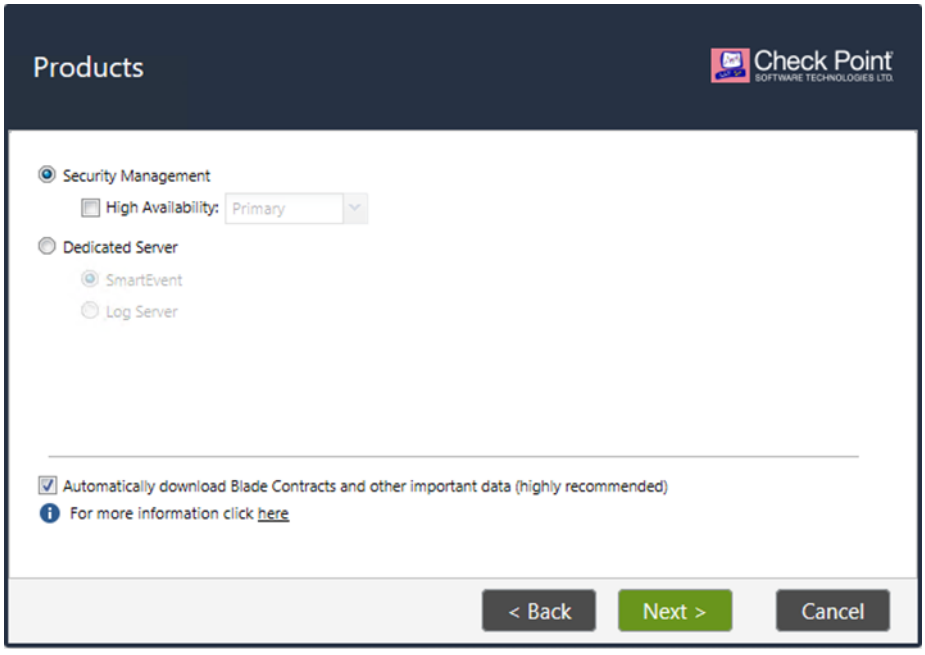
- For VM, Installation Type window displayed:



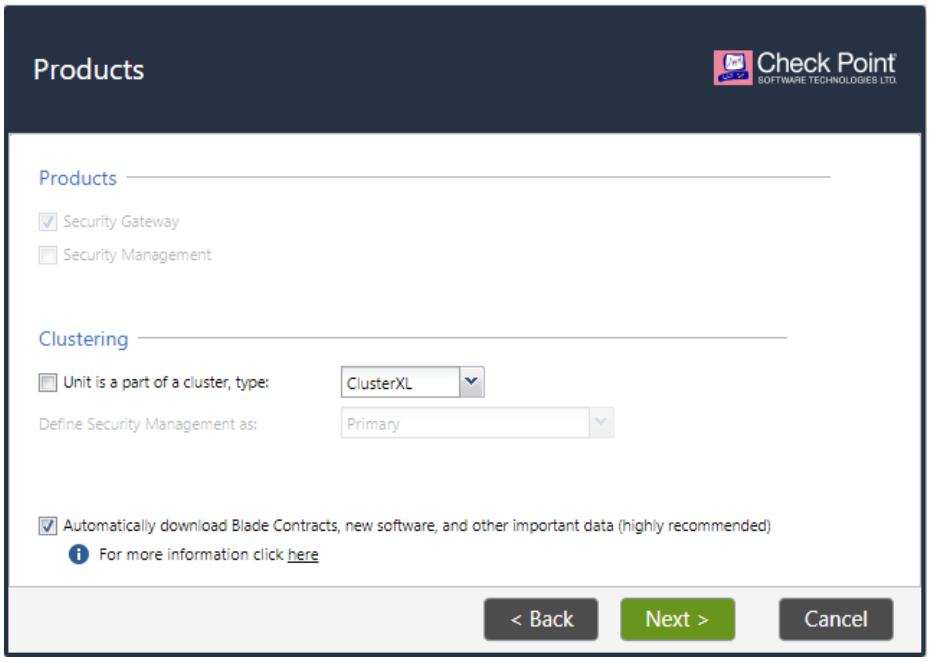
Set up the **Security Gateway and/or Security Management** option, Press **Next**.

10. The Products window opens.

For Smart-1 appliances:

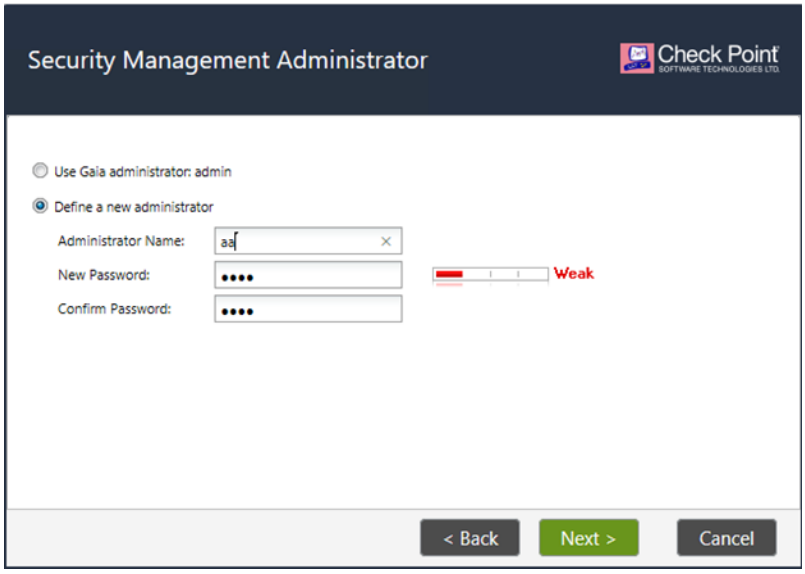


For Security Gateway appliances (for **VM Products** checkboxes are not greyed out):



Set the desired configuration and click Next.

11. For the Security Management server, the Security Management Administrator window opens.

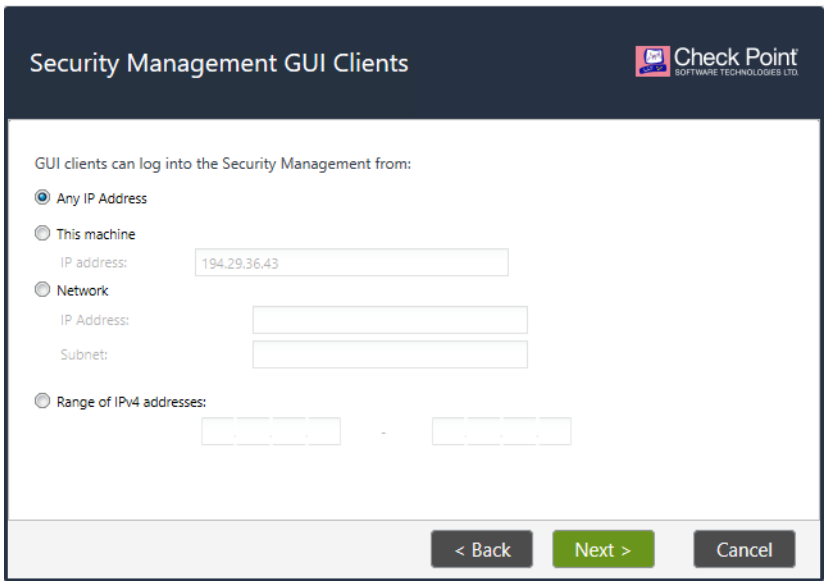


Enter the Administrator Name and Password. Click Next.

The password must conform to the following operating system-enforced complexity requirements:

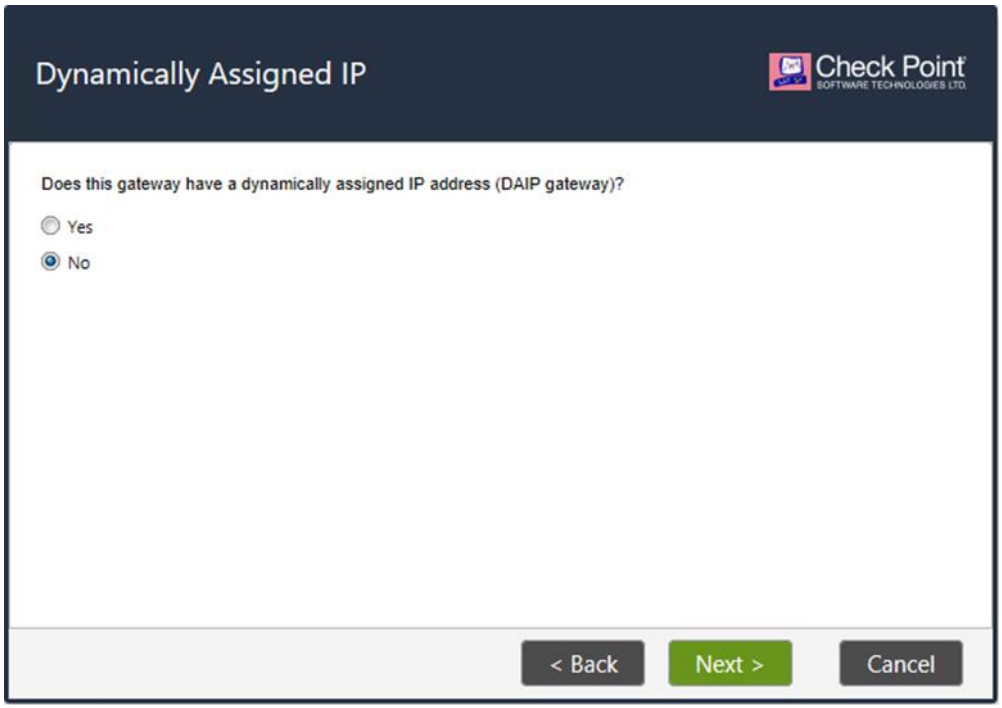
- At least 15 characters, in length
- A mixture of alphabetic, upper case, lower case, numeric and special characters
- At least four different characters
- Does not use simple dictionary words, or common strings such as "qwerty"

12. For Security Management, the Security Management GUI Clients window opens.



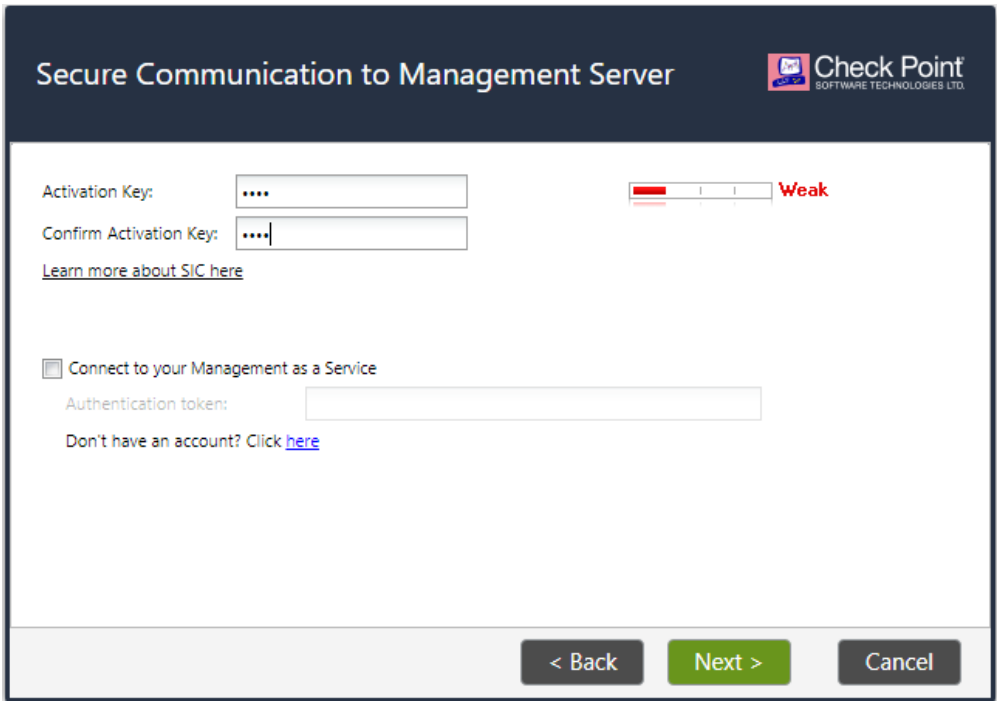
Set the desired GUI clients and click Next.

13. For the Security Gateway, the Dynamically Assigned IP window opens.



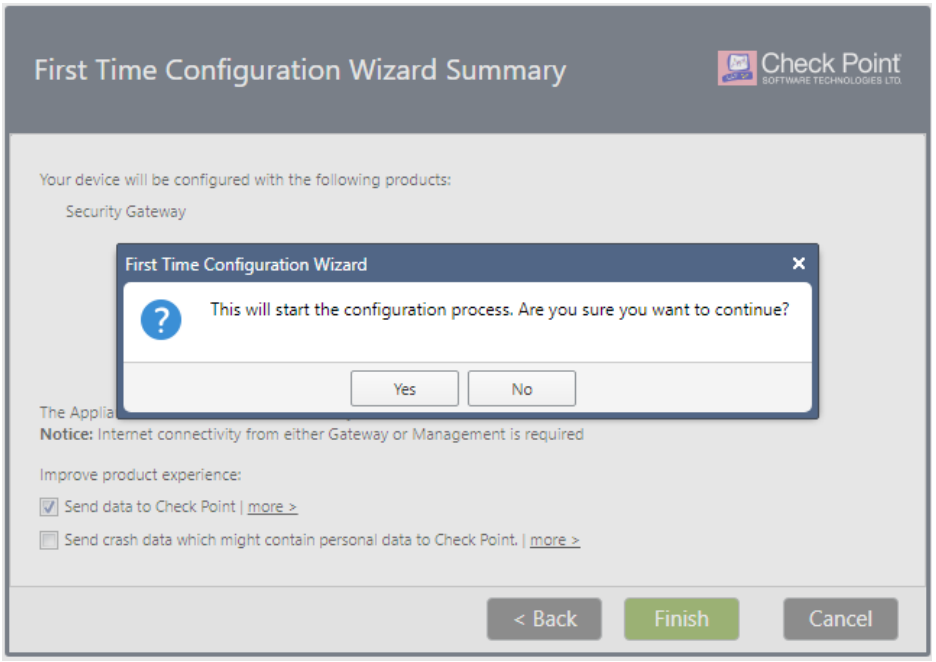
Select No and click Next.

14. For the Security Gateway, the Secure Internal Communication (SIC) window opens.



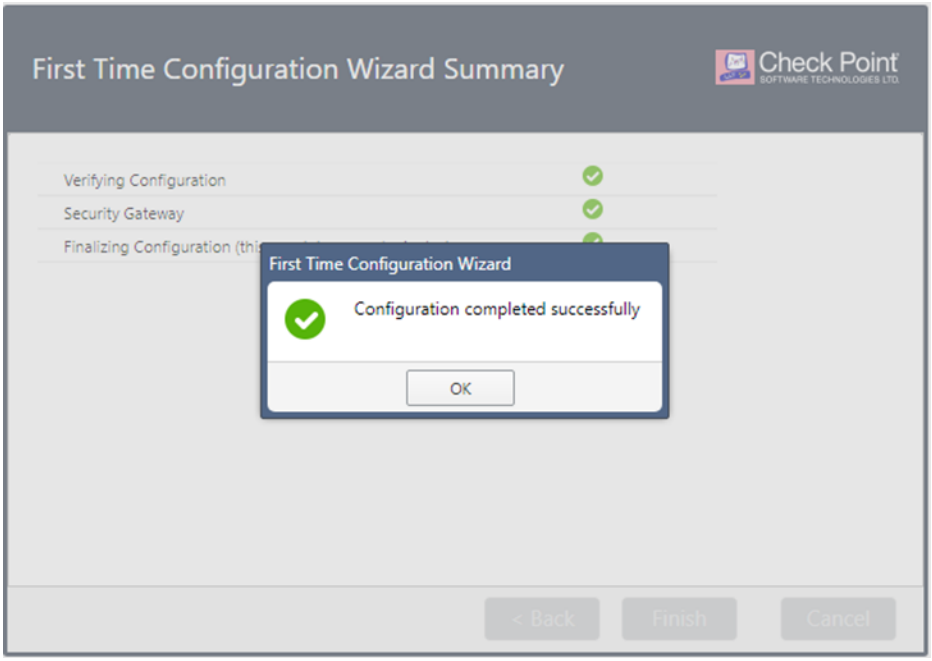
Enter the Activation Key and confirm it. Click Next.

15. The Summary window opens.



Make sure that the Summary is correct. Click Finish and click Yes to approve.

16. The Completion window opens.



Click **OK**.

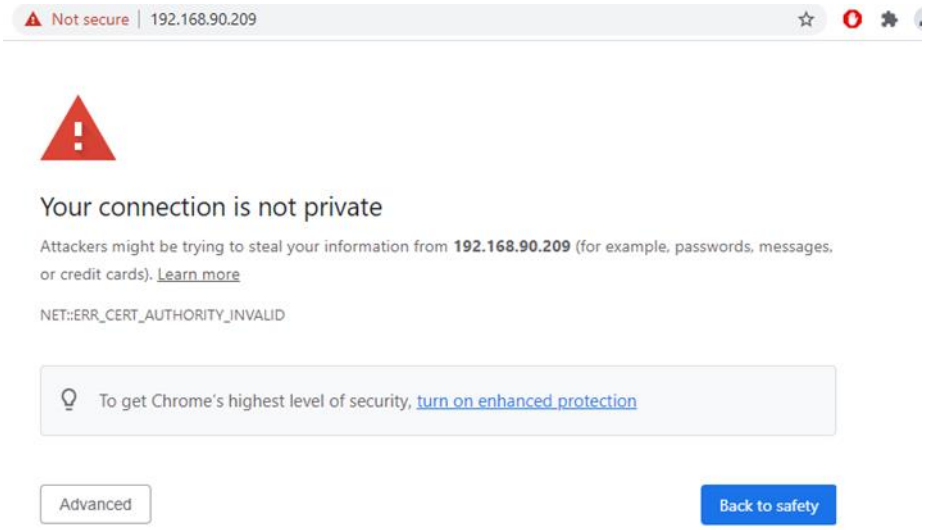
SP Security Group Configuration (for SP deployment)

1. Before you begin the Security Group configuration, refer to the Maestro Getting Started Guide: https://sc1.checkpoint.com/documents/Maestro/GSG/EN/Topics/Introduction.htm.
2. Enable the connected interfaces by running “set maestro port <port> admin-state up”.
3. Set the GW connected ports on the MHO to downlinks by running “set maestro port <port> type down link” followed by the “save config” command.

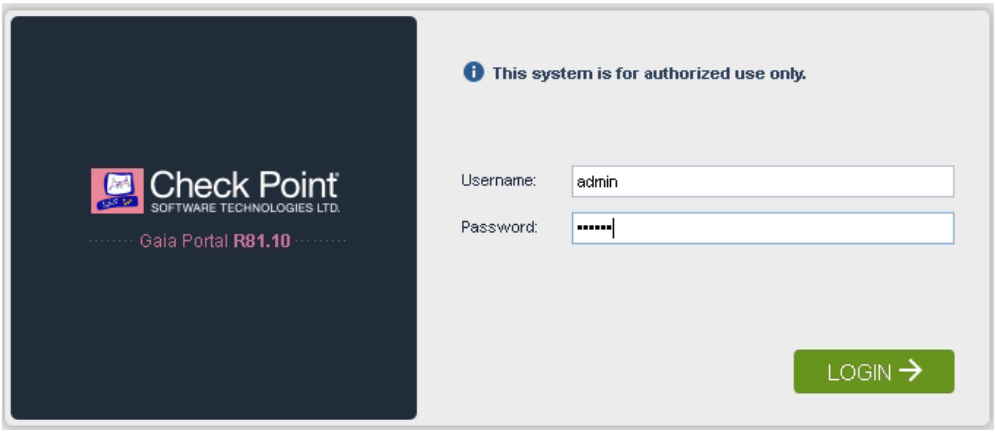
In particular, the separate networks whose traffic is to be inspected must be connected to Orchestrator using either separate Networking Devices or a single Networking Device configured as per example deployment on page 50 of the Orchestrator Getting Started Guide. These Networking Devices (switches) are in the environment of the TOE, but are critical to ensuring the traffic is inspected before it is communicated between the separate networks. The administrator is responsible for ensuring sufficient confidence can be placed in the Networking Device to maintain separation of traffic between disparate networks.

The connectivity between Orchestrator appliance(s) and SGMs, and between Orchestrator appliance(s) and the Management Server must be consistent with that shown in the example deployment on page 50 of the guide. Namely, the Management Server should only be connected using the Management Port on the Orchestrator appliance(s), and the uplink and down link ports of the Orchestrator appliance(s) are used to connect to the SGMs.

1. Connect to the Orchestrator Gaia portal using HTTPS on the defined port (disregard the security certificate warning if displayed).



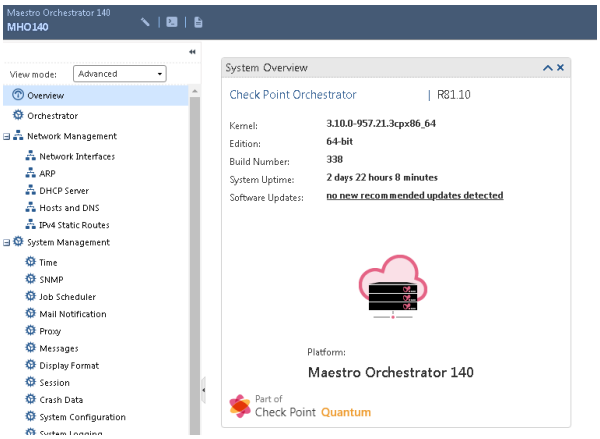
2. The login screen opens.



Enter the user name and password, and click **LOGIN**.

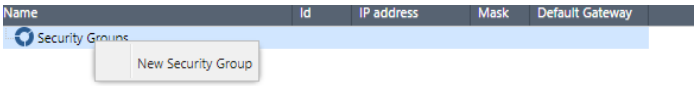
If necessary, acquire lock by pressing on the lock icon followed by clicking yes:

3. The main screen opens.



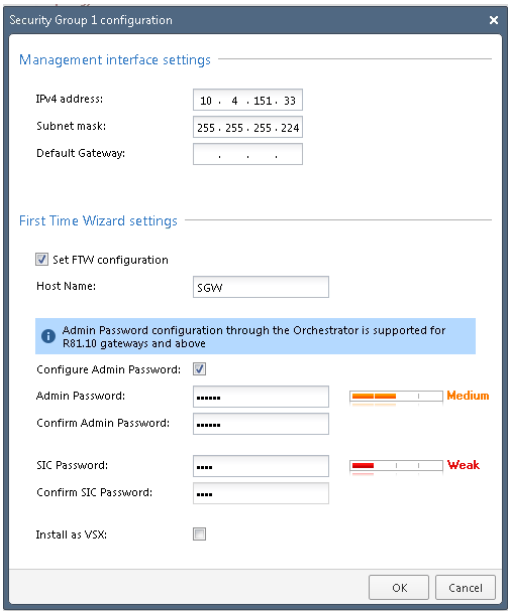
Click the **Orchestrator** tab.

4. The Orchestrator screen opens.



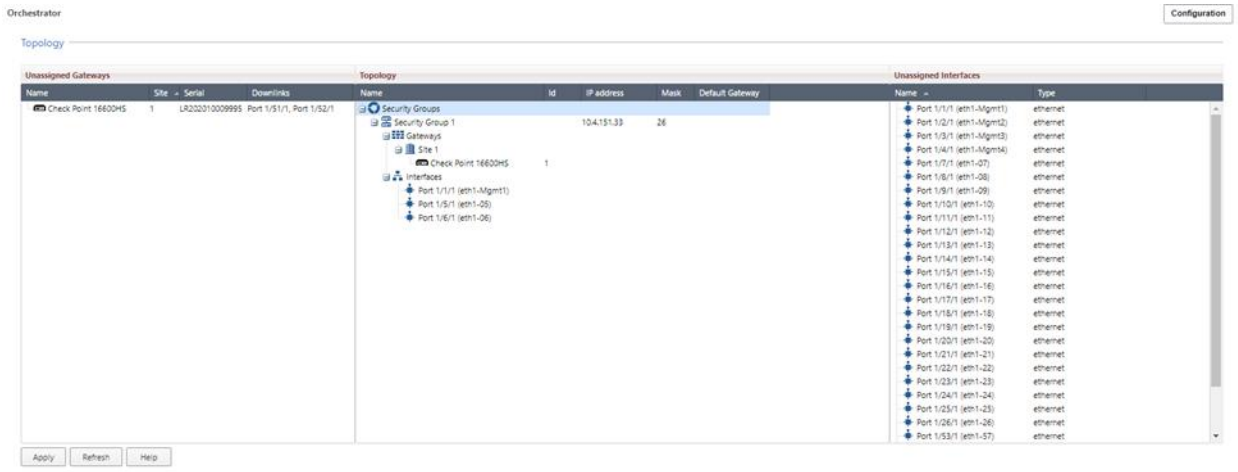
Right click Security Groups > New Security Group.

5. The Security Group configuration screen opens.



- Enter the **IP address**, **Subnet Mask**, **Default Gateway** (if required) and select the **Set FTW** checkbox.
- Set the Configure Admin Password checkbox and type the required password twice.
- Enter the **Host Name** and **Activation Key** twice and then click **OK**.

6. The defined Security Group shows in the Orchestrator page.

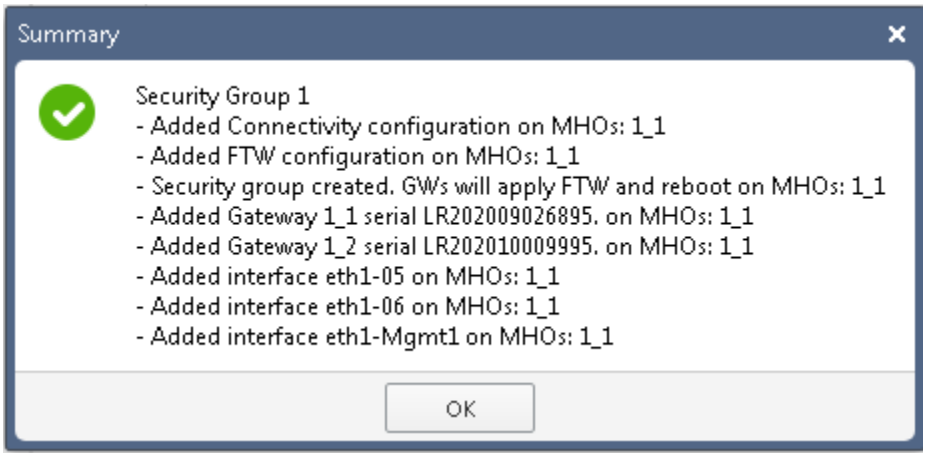


Drag the desired appliances and interfaces to the Security Group and click **Apply**.

7. The Apply Topology confirmation window opens.

Click **Yes**.

8. The Summary window opens.



Click **OK**.

Installing Hotfixes (HFs)

Obtain all files from SK173465
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk173465

Obtain the DA (Deployment Agent) from SK92449:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92449

1. Execute the commands below using the console port (through CLISH) mode for Security Gateway and Security Management **only**).

On all of the appliances:

- `set user admin shell /bin/bash`
- If required: `set expert-password`
- Enter the current password and the new password twice
- `save config`
- Enter expert mode by typing “expert”
- Copy the Deployment Agent package to the Smart-1 appliance /var/log/[custom_folder]/
- Extract it with gtar -zxvf DeploymentAgent_000002193_1.tgz
- Stop DA watchdog - dastop
- Stop DA agent – dbget installer:stop
- Stop confd tellpm process:clishd
- Stop clishd tellpm process:confd
- Install extracted RPM – rpm -Uhv --force CPda-00-00.i386.rpm
- At this stage Gaia web session will be terminated – if you were connected to the Gaia web GUI, you should relodgin.
- Start clishd tellpm process:clishd t
- Start confd tellpm process:confd t
- sleep 5
- Start DA agent dastart
- Reboot the machine

2. Execute the commands below using the console port (through CLISH mode) on the Security Management Smart-1 appliance and the Security Gateway and the first SP Security Gateway (through GCLISH):
   - On SP Security Gateway execute “`set smo image auto-clone state off`”, “`set expert-password`” and “`set user admin shell /bin/bash`”
   - On SP Security Orchestrator, type “`set user admin shell /bin/bash`”.
   - Run “`set time <time>`”, “`set timezone <timezone>`” and “`set date <date>`”, “`set time <time >`” if necessary.
   - Run “`save config`”
   - Copy the file below to the `/home/admin` directory over SSH:


```
Check_Point_R81_10_JHF_T22_EAL4_HF_MAIN_Bundle_T4_FULL.tar
```

- From CLISH run:

```
installer import local
/home/admin/Check_Point_R81_10_JHF_T22_EAL4_HF_MAIN_Bundle_
T4_FULL.tar
```

- On Security Gateway and Security Management run:

```
> cpstop
> installer import local >
/home/admin/Check_Point_R81_10_JHF_T22_EAL4_HF_MAIN_Bundle_T2_FULL.t
ar
> installer install <number>
```

- Click "y"
- On SP Security Gateway and Orchestrator type "y" and press Enter
- On SP Security Gateway and Orchestrator type "y" and press Enter
- On SP Security Gateway and Orchestrator, if prompted, type your name and press Enter
- On SP Security Gateway and Orchestrator, if prompted, press Enter
- Once the Security Management server is up run on it (through expert mode), enter:

```
echo "ENABLE_ACCESS_TO_CPM_ONLY_FROM_LOOPBACK=1; export
ENABLE_ACCESS_TO_CPM_ONLY_FROM_LOOPBACK" >> $CPDIR/tmp/.CPprofile.sh
```

- On Security Management server run:

```
cpstop
```

- On Security Management server run:

```
cpstart
```

You may now perform any or all of the configuration steps described in the previous step that require Security Management Server console access before you move on to the next step. These steps describe installation settings that have been documented and evaluated as being compatible with the evaluated security policy.

Version Verification

As part of the version verification, the steps below must be run on all of the appliances.

1. Connect to the appliance CLI interface.
2. Execute: `cpinfo -d -D -i -y all`

Compare the output values given by `cpinfo -y all` in Table 4 (on page 18).

Configuration

Post Install Configuration

There are a number of configuration steps that needs to be performed across the various components in the deployed configuration. Although outside their responsibilities once the TOE is operational, these are expected to be performed by those with the same authorization as the Security Management Server Administrator and (when in SP deployment) the Orchestrator Administrator.

1. Download Putty client or similar SSH/Console client https://www.putty.org.
2. Connect the Console port on the machine to a client or console server.
3. Perform login with the defined credentials in the First Time Wizard.
4. Add licenses for all of the servers including the Orchestrator.
5. Using CLI, execute "expert" and enter the administrator password on both Security Gateway and Security Management.
6. On both Security Gateway (and SP) and Security Management run (from expert mode):

   ```
   echo export PASSWORD_MIN_LENGTH=15 > /etc/environment
   ```

7. On the Security Management, run

   ```
   > dbedit
   > modify properties firewall_properties log_local_inf_addr_spoofing log
   > modify properties firewall_properties log_loopback_addr_spoofing log
   > quit > y
   ```

Note - This enables the system to log spoofed addresses with the machine interface IP and the loopback interface so that these packets can be logged properly.

8. On the Security Gateways (including SP), if not defined, define the internal/external IP address (through GCLISH). Run:

   ```
   > set interface <internal_interface> ipv4-address <ip_address> mask-length <mask_length>
   > set interface <internal_interface> state on
   ```

9. On the SP Security Gateway(through GCLISH), run:

   ```
   > set smo image auto-clone state on
   > save config
   ```

10. On the Security Gateway (without SP), if necessary, set up management interface by running the command below using CLISH:

    ```
    > set management interface <interface>
    > save config
    ```


11. On the Management server, if not defined, add additional REST API administrator. Run the command:

```
> mgmt_cli add administrator name "<name>" password "<password>" must-change-password false authentication-method "check point password" permissions-profile "super user" --domain "System Data" -r true
```

Note - The password must conform to the following operating system-enforced complexity requirements:

- At least 15 characters, in length
- A mixture of alphabetic, upper case, lower case, numeric and special characters
- At least four different characters
- Does not use simple dictionary words, or common strings such as “qwerty”

12. On the Management server, if applicable, delete the previously created REST API administrator (from the installation phase). Run the command:

```
> mgmt_cli delete administrator name "<name>" --domain 'System Data' --format json -r true
```

13. On the Security gateway, run the commands below to enforce usage of TLSv1.3:

```
> ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 CKPSSL_MIN_TLS_VERSION TLS1.3
> cpstop;cpstart
```

14. On the Security Management, run the commands below to enforce minimum usage of TLSv1.2[1]:

```
> sic_conf_tool set local protocol_version TLSv1.2
> ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 CKPSSL_MIN_TLS_VERSION TLS1.2
> cpstop;cpstart
```

15. On the Security Management, add the Security Gateway. Run the command:

```
> mgmt_cli add simple-gateway name <GW_name> ipv4-address <GW_MGMT_IP> firewall true version "R81" one-time-password <one time password> interfaces.1.name <name>  interfaces.1.ipv4-address <ip> interfaces.1.ipv4-network-mask <mask> interfaces.1.anti-spoofing true interfaces.1.topology <EXTERNAL/INTERNAL> interfaces.2.name <name> interfaces.2.ipv4-address <ip> interfaces.2.ipv4-network-mask <mask> interfaces.2.anti-spoofing true interfaces.2.topology <EXTERNAL/INTERNAL> interfaces.2.security-zone true interfaces.2.security-zone-settings.auto-calculated true interfaces.2.topology-settings.ip-address-behind-this-interface "LOCAL_NETWORK" interfaces.3.name <name> interfaces.3.ipv4-address <ip> interfaces.3.ipv4-network-mask <mask> interfaces.3.anti-spoofing true interfaces.3.topology <EXTERNAL/INTERNAL> interfaces.3.security-zone true interfaces.3.security-zone-settings.auto-calculated true
```

[1] Although the minimum is set to TLS v1.2, the SIC communication between the Security Management Server and Gateway will still be established using TLS v1.3 because of the enforcement of TLS v1.3 by the Gateway.


```
interfaces.3.topology-settings.ip-address-behind-this-interface
"LOCAL_NETWORK" logs-settings.reject-connections-when-free-disk-space-
below-threshold  true -r true
```

16. On Security Management, enable IPS on the Security Gateway. Run:

```
> mgmt_cli set simple-gateway name <GW name> ips true -r true
```

Note – Do not enable any other blades except of the Firewall and IPS blades as this will take you out of the evaluated configuration.

17. For SP configuration only, change the HW type by running the commands below:

```
> mgmt_cli show simple-gateway name "SGW" -r true | grep uid
> Copy the first uid shown.
> mgmt_cli set generic-object uid <uid> applianceType "Maestro Gateway"
-r true
```

18. Obtain the offline IPS signature update package according to sk93724 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93724.
19. Upload the obtained offline IPS package to the Security Management

```
> /opt/CPsuite-R81.10/fw1/tmp/uploaded_file/<file_name> directory.
```

20. Update the IPS package. Run:

```
> mgmt_cli run-ips-update package-path /opt/CPsuite-
R81/fw1.10/tmp/uploaded_file/<file_name> -r true
```

21. On the Security Management, create a new IPS profile with all protections in "Prevent" mode:

```
> mgmt_cli -r true add threat-profile name AllPrevent active-
protections-performance-impact high active-protections-severity "Medium
or above" confidence-level-high Prevent confidence-level-low Prevent
confidence-level-medium Prevent ips true
```

22. On the Security Management, create IPS policy (to enable the restricted IPS policy for the evaluation). Run the following (note the uid is presented at the top of the results for the first command and the value for the AllPrevent UID should be used in the second command):

```
> mgmt_cli -r true show threat-profile name AllPrevent details-level
uid
> mgmt_cli -r true set threat-rule rule-number 1 action <AllPrevent
UID> layer "Standard Threat Prevention"
```

23. On Security Management, execute this command to define the minimum password length for newly created administrators:

```
> mgmt_cli -d "System Data" -r true show generic-objects class-name
"com.checkpoint.management.mgmt_blade.objects.PasswordPolicySettings"
```

Copy the **first** (1st) UID of the object with the name "System Data" and execute the command:

```
> mgmt_cli -d "System Data" -r true set generic-object uid <UID>
minLength <length> -r true
```

Follow the same process for the third UID.

24. On the Security Management, disable online IPS updates. Run:

```
> mgmt_cli -r true set ips-update-schedule enabled false
```

25. On Security Management, define policy for the gateway to send system logs to the syslog server and to be able to synchronize with the NTP server. Define a host for the NTP server and a host for the log server. Use the host for the destination in the following access-rules.

```
> mgmt_cli add host name <ntp_server_name> ip-address
<ntp_server_ip_address> -r true
> mgmt_cli add access-rule name <rule name> layer Network position top
service.1 "NTP" action "Accept" track.type "Log" source.1 <GW_name>
source.2 <MGMT_name> destination <ntp_server_name> -r true
> mgmt_cli add host name <syslog_server_name> ip-address
<syslog_server_ip_address> -r true
> mgmt_cli add access-rule name <rule name> layer Network position top
service.1 "syslog" action "Accept" track.type "Log" source "Any"
destination <syslog_server> -r true
> mgmt_cli add host name host_0.0.0.0 ip-address 0.0.0.0 -r true
> mgmt_cli add network name Net_240.0.0.0 subnet 240.0.0.0 subnet-mask
240.0.0.0 -r true
> mgmt_cli add network name Net_169.254.0.0 subnet 169.254.0.0 subnet-
mask 255.255.0.0 -r true
> mgmt_cli add access-rule name TOP layer Network position top
service.1 "Any" action "Drop" track.type "Log" destination "Any"
source.1 host_0.0.0.0 source.2 Net_240.0.0.0  -r true
> mgmt_cli add access-rule name TOP layer Network position top
service.1 "Any" action "Drop" track.type "Log" source "Any"
destination.1 host_0.0.0.0 destination.2 Net_240.0.0.0  -r true
> mgmt_cli add access-rule name TOP layer Network position top
service.1 "Any" action "Drop" track.type "Log" destination "Any"
source.1 Net_169.254.0.0 -r true
> mgmt_cli add access-rule name TOP layer Network position top
service.1 "Any" action "Drop" track.type "Log" source "Any"
destination.1 Net_169.254.0.0 -r true
> mgmt_cli show generic-objects name "Sequence Verifier" details-level
full -r true | grep "1963f7ae-ea67-4826-ac48-e449bf5d2937" -A 3 | grep
"uid"
```

copy the uid parameter from the previous command and insert it to the <protection_uid> section in the command below:

```
> mgmt_cli set generic-object uid <protection_uid> activeParser true
parserActivation.action "6c488338-8eec-4103-ad21-cd461ac2c473"
parserActivation.override "OVERRIDE" -r true
```


26. From the Security Management, install the policy on the Security Gateway. Run the command:

```
> mgmt_cli install-policy policy-package <Standard> access true threat-prevention true -r true
```

27. From the Security Management, install the policy on the Security Gateway. Run the command:

```
> mgmt_cli install-policy policy-package <Standard> access true -r true
```

28. On the Security Management, enable log forwarding to the external syslog server. Use the syslog protocol and run these commands from CLISH:

```
> cp_log_export add name <syslog_server_name> target-server <syslog_server_ip> target-port 514 protocol tcp
> cp_log_export restart name <syslog_server_name>
```

29. Run the commands below (twice if necessary) on both Security Management (including SP) and Security Gateways from (G)CLISH (ignore errors):

```
> add syslog log-remote-address <syslog_server_ip> level all
> save config
```

30. On the Security Gateway (including SP) run:

```
> set syslog cplogs on
> save config
```

31. On all machines, define the NTP server accordingly via expert mode:

A. Put a key in the key file - **/etc/ntp/keys** file:

```
[key number] M [key password]
```

Make sure that:

- the '`key number`' is between 1 and 65535
- the '`key password`' is between 1 and 31 characters (spaces or '#' character are **not** allowed)

B. Configure the following in the /etc/ntp.conf file:

```
restrict default ignore
restrict 127.0.0.1
trustedkey [key number] [another key number] ...
keys /etc/ntp/keys
driftfile /var/lib/ntp/ntp.drift
```

C. For every NTP server:

- If it is IPv4 or Host name:

```
server [IPv4 address or Host name of NTP server] version [version number 1...4] iburst key [key number]
restrict [IPv4 address or Host name of NTP server] nomodify notrap nopeer noquery
```


32. On all machines define NTP server by running through CLISH:

```
> set ntp server primary <server IP> version 4
> set ntp active on
> save config
```

This is required for the gateway to operate in Kernel mode.

33. In both Security Management and Security Gateway, execute as below to disable the WEBUI through expert mode:

Comment out (by '#') the following entry in /web/templates/httpd2.conf.templ:

```
<Directory "/web/cgi-bin2">
****
</Directory>
```

34. On both Security management and SP orchestrator run the commands below:

```
> cp /web/templates/httpd-ssl.conf.templ /web/templates/httpd-ssl.conf.templ_ORIGINAL
> chmod u+w /web/templates/httpd-ssl.conf.templ
>sed -i -e 's/HIGH:!RC4:!LOW:!EXP:!aNULL:!SSLv2:!MD5/ECDHE-RSA-AES256-SHA384:AES256-SHA256:!ADH:!EXP:RSA:+HIGH:+MEDIUM:!MD5:!LOW:!NULL:!SSLv2:!eNULL:!aNULL:!RC4:!SHA1/g' /web/templates/httpd-ssl.conf.templ
> sed -i -e 's/{ifcmp = $httpd:ssl3_enabled 1}+{else}-{endif}SSLv3 +TLSv1.2/TLSv1.3/g' /web/templates/httpd-ssl.conf.templ
> chmod u-w /web/templates/httpd-ssl.conf.templ
> /bin/template_xlate : /web/templates/httpd-ssl.conf.templ /web/conf/extra/httpd-ssl.conf < /config/active
> tellpm process:httpd2
> tellpm process:httpd2 t
```

35. On all appliances execute the commands below through expert mode:

```
> echo 'USE_ONLY_GOOD_ENTROPY=1; export USE_ONLY_GOOD_ENTROPY' >> $CPDIR/tmp/.CPprofile.sh
> chkconfig --add jitterentropy_rngd_init
> echo 'fw log -f -t -n -l $FWDIR/log/fw.adtlog|logger -p local5.info -t CP_FireWall &' >> /etc/rc.d/init.d/cpboot
```

36. On the SP appliance, run the command::

```
> sed -i 's/Scalable Platform rules/Scalable Platform rules\nModules ; ME ; 256 ; fetch_packets ; sslca\nANY ; ME ; ANY ; sync,syncn ; any_method/g' $CPDIR/conf/sic_policy.conf
```

37. On the Smart-1 machine run "echo 0 > /proc/sys/net/ipv4/ip_forward".
38. Reboot all the machines.
39. For SP environment only, Connect to the Orchestrator WebUI by typing: "https://<orchestrator_ip_address>" from your browser > "Orchestrator" tab > Add the rest of the desired SP Security Gateways by dragging them to the security group > press

apply.

40. Run `service sshd stop` on all machines to stay within the TOE boundary.
41. Run `chkconfig --del sshd` on all machines to stay within the TOE boundary.

Notes:

- When you are finished, do not log in through the local Console interface on both the Security Gateway and the Security Management server as it is outside of the evaluated configuration. Do not use the `dbedit` interface.
- Although the console access is not supported in operational mode, it should be noted in the installation section that there is a maintenance mode, aka Expert mode, which is a mode only available via the console and therefore cannot be reached via the REST API.
- To use LOM interface for Smart-1 625/6000-L/6000-XL/600-M/600-S appliances follow sk173406: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk173406

Operational Modes

REST API is the only operational mode supported in the TOE.

Console access and Expert mode are not supported operational modes.

Configuring the Management LAN as an Isolated Network

Important - It is mandatory to create an isolated network accessible only by the Management Server, the Security Gateway and the hosts (workstation host, NTP server, Syslog server) during the evaluation. You must do this without allowing any other traffic through the gateway. This is possible when REST API sets an Access Rule for the Management Server and another access rule to connect the Management Server, the gateway and the hosts without external connections.

See more about Access Rules in **Concepts of Security Management** (on page 62).

See more about REST API calls in **Using REST API** (on page 71).

Configuring an isolated network:

1. Use REST API `add-host` to create a unique object name for the workstation host, NTP server, and Syslog server in the subnet that you have configured. Add each of these to the source and destination in the first `add-access-rule` below.

Note - The mgmt object is there by default. When you connect a gateway to the management, it creates a gateway object.

2. Use REST API to add a rule that blocks access to the Management Server from all networks.
3. Use REST API to add a rule that allows access between the Management Server, the

gateway and the workstation host.

The REST API calls to isolate the server and then connect the server, gateway and workstation host:

URL: `https://<mgmt ip>/web_api/login`

Body:

```
{
"user" : <username>,
"password" : <password>
}
```

URL: `https://<mgmt ip>/web_api/add-access-rule`

Body:

```
{
"name" : "Allow_Objects_only",
"layer" : <layer_name>,
"position" : "top",
"source" : ["mgmt", "gw", "int_host", "des_host"],
"destination" : ["mgmt", "gw", "int_host", "des_host"],
"service" : "any",
"action" : "Accept"
}
```

URL: `https://<mgmt ip>/web_api/add-access-rule`

Body:

```
{
"name" : "cleanup",
"layer" : <layer_name>,
"position" : "bottom",
"source" : "any",
"destination" : "any",
"service" : "any",
"action" : "Drop"
}
```

URL: `https://<mgmt ip>/web_api/publish`

Body:

```
{
"uid" : <session uid – not mandatory>
}
```

URL: `https://<mgmt ip>/web_api/logout`

Body:

```
{
}
```


Required Rules for the "Standard" Package and Add-Package

When you use REST API `add-package` to create a Rule Base, it is mandatory to add rules to isolate the Management LAN. Each package requires these rules.

See more about the mandatory access rules in **Configuring the Management LAN as an Isolated Network** (on page 56).

See more about Access Rules in **Concepts of Security Management** (on page 62).

See more about REST API calls in **Using REST API** (on page 71).

The REST API required rules to isolate the Management LAN are:

URL: `https://<mgmt ip>/web_api/login`

Body:
```
{
"user" : <username>,
"password" : <password>
}
```

URL: `https://<mgmt ip>/web_api/add-access-rule`

Body:
```
{
"name" : "Allow_Objects_only",
"layer" : <layer_name>,
"position" : "top",
"source" : ["mgmt", "gw", "int_host", "des_host"],
"destination" : ["mgmt", "gw", "int_host", "des_host"],
"service" : "any",
"action" : "Accept"
}
```

URL: `https://<mgmt ip>/web_api/add-access-rule`

Body:
```
{
"name" : "cleanup",
"layer" : <layer_name>,
"position" : "bottom",
"source" : "any",
"destination" : "any",
"service" : "any",
"action" : "Drop"
}
```

URL: `https://<mgmt ip>/web_api/publish`

Body:
```
{
"uid" : <session uid - not mandatory>
}
```

URL: `https://<mgmt ip>/web_api/logout`

Body:
```
{
}
```


The REST API required rules to drop network packets where the source or destination added of the network packet is defined as unspecified (i.e., 0.0.0.0) or an address "reserved for future use" (i.e., 240.0.0.0/4) as specified in RFC 5735 for ipv4:

URL: `https://<mgmt ip>/web_api/login`

Body:

```
{
    "user" : <username>,
    "password" : <password>
}
```

URL: `https://<mgmt ip>/web_api/add-host`

Body:

```
{
    "name" : "host_0.0.0.0",
    "ip-address" : "0.0.0.0"
}
```

URL: `https://<mgmt ip>/web_api/add-network`

Body:

```
{
    "name" : "Net_240.0.0.0",
    "subnet" : "240.0.0.0",
    "subnet-mask" : "240.0.0.0"
}
```

URL: `https://<mgmt ip>/web_api/add-network`

Body:

```
{
    "name" : "Net_169.254.0.0",
    "subnet" : "169.254.0.0",
    "subnet-mask" : "255.255.0.0"
}
```

URL: `https://<mgmt ip>/web_api/add-access-rule`

Body:

```
{
    "name" : "TOP",
    "layer" : "Network",
    "position" : "top",
    "service" : "any",
    "action" : "drop",
    "track" : {
         "type" : "Log"
    }
    "destination" : "any",
    "source" : ["host_0.0.0.0", "Net_240.0.0.0"]
}
```

URL: `https://<mgmt ip>/web_api/add-access-rule`

Body:

```
{
```



```
    "name" : "TOP",
    "layer" : "Network",
    "position" : "top",
    "service" : "any",
    "action" : "drop",
    "track" : {
         "type" : "Log"
    }
    "source" : "any",
    "destination" : ["host_0.0.0.0", "Net_240.0.0.0"]
}
```

URL: `https://<mgmt ip>/web_api/publish`

Body: {

```
    "uid" : <session uid – not mandatory>
}
```

URL: `https://<mgmt ip>/web_api/logout`

Body: {

}

Note - The last two `add-acess-rule` commands operate on the "Standard" package. For a different package, the layer name should reflect it.

Notification and Receipt of Latest IPS Signature Packages

To receive notifications of updates, you can subscribe to the Security Advisories Subscription https://www.checkpoint.com/defense/advisories/public/sdnews/.

After receiving the notification of the update, you must download and install it.

The IPS Service offers two types of Security Advisories to help you secure your network.

Weekly Update - Receive real-time updates and configuration information from Check Point IPS to ensure your protection against the latest threats.

Monthly Update - The advisory contains new information about:

- **Hot Protections** - The most critical threats to your network security with summaries of the threats and recommendations for the right protection.
- **Highlighted Updates** - Summarized in an easy-to-read table with links to more information to help you plan your configuration of these important updates.
- **Product and Security Information** - News related to IPS and other Security Services and recent security topics.

Note - See the list of advisories on **Advisories Archive** https://www.checkpoint.com/advisories/.

Adding Administrators

Using REST API to add administrators of the Security Management Server requires these rules in the evaluation configuration.

Administrators must use the authentication method `"check point password"` and no other method.

Administrators must use strong passwords:

- At least 15 characters in length.
- A mixture of alphabetic, upper case, lower case, numeric and special characters.
- At least four different characters.
- Does not use simple dictionary words or common strings such as "qwerty".

Administrators must have full privileges.

The REST API call to add Security Management Server administrators:

URL: `https://<mgmt ip>/web_api/add-administrator`

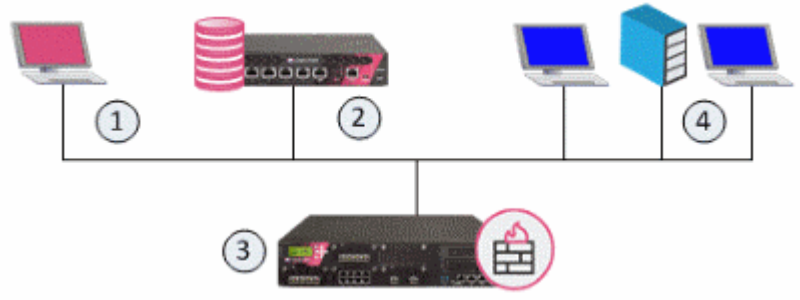
Body: {

```
"name" : "admin",
"password" : <password>,
"authentication-method" : "check point password",
"must-change-password" : false,
"email" : <email>,
"phone-number" : <phone>,
"permissions-profile" : "read write all"
}
```


Concepts of Security Management

Check Point offers effective Security Management solutions to help you keep up with constantly growing needs and challenges of your organizational network. This Administration Guide focuses on the basic Security Management Server deployment to be applied by a Security Management Server Administrator.

These are the basic components of Check Point security architecture.



Item	Description
1	REST API Interface for connection to and management of Security Management Servers.
2	Security Management Server - Manages Security Gateways with defined security policies and monitors security events on the network.
3	Security Gateway - Placed at the perimeter of the network topology, to protect your environment through enforcement of the security policies.
4	Your environment to protect.

Object Categories

Objects represent networks, devices, and protocols.

Icon	Object Type	Examples
	Network Objects	Gateways, hosts, networks, address ranges, dynamic objects, security zones
	Services	Services, Service groups
	Time Objects	Time, Time groups

Managing Policies

Policy Packages let you group different types of policies, to be installed together on the same installation targets.

Database version control lets you track past changes to the database.

Security Management Terms

Administrator

A REST API administrator with permissions to manage Check Point security products and the network environment.

Database

The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

Log Server

Physical server that hosts Check Point product log files.

Management Server

A Check Point Security Management Server

Package

Group of files, and data about those files, delivered as one software archive (usually TGZ or RPM), for distribution and installation.

Permissions Profile

A set of access, and feature-based roles for the REST API administrator
Note - In the evaluated configuration there is a single administrator with full privileges .

Policy

A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

Rule Base

The database that contains the rules in a security policy and defines the sequence, in which they are enforced.

Security Gateway

A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

Security Management Server

A computer that runs Check Point software to manage the objects and policies in Check Point environment.

SIC

Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Software Blade

A software blade is a security solution based on specific business needs.
Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

Note - In the Evaluated configuration, only the firewall and IPS blades are enabled

Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

Access Control - consists of these types of rules:

- Firewall
- NAT

Threat Prevention - consists of IPS protections
The installation process:

Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

Note - If there are verification errors, the policy is not installed. If there are verification warnings, the policy package is installed with a warning.

Makes sure that each of the Security Gateways enforces at least one of the rules. If none of the rules are enforced, the default drop rule is enforced.

Distributes the user database and object database to the selected installation targets.

Use Case - Basic Access Control

This use case shows a Rule Base for a simple Access Control security policy.

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Critical subnet	Internal	Finance HR R&D	Any	Accept	Log	CorpGW
2	Tech support	TechSupport	Remote1-web	HTTP	Accept	Alert	Remote1GW
3	DNS server	Any	DNS	Domain UDP	Accept	None	Policy Targets
4	Mail and Web servers	Any	DMZ	HTTP HTTPS SMTP	Accept	Log	Policy Targets
5	SMTP	Mail	NOT Internal net group	SMTP	Accept	Log	Policy Targets

6	DMZ & Internet	IntGroup	Any	Any	Accept	Log	Policy Targets
7	Cleanup rule	Any	Any	Any	Drop	Log	Policy Targets

Rule	Explanation
1	Critical subnet - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and R&D.
2	Tech support - Allows the Technical Support server to access the Remote-1 web server which is behind the Remote-1 Security Gateway. Only HTTP traffic is allowed. When a packet matches the Tech support rule, the Alert action is done.
3	DNS server - Allows UDP traffic to the external DNS server. This traffic is not logged.
4	Mail and Web servers - Allows incoming traffic to the mail and web servers that are located in the DMZ. HTTP, HTTPS, and SMTP traffic is allowed.
5	SMTP - Allows outgoing SMTP connections to the mail server. Does not allow SMTP connections to the internal network, to protect against a compromised mail server.
6	DMZ and Internet - Allows traffic from the internal network to the DMZ and Internet.
7	Cleanup rule - Drops all traffic that does not match one of the earlier rules.

Types of Rules in the Rule Base

There are three types of rules in the Rule Base - explicit, implied and implicit.

Explicit Rules

The rules that the administrator configures explicitly to allow or to block traffic based on specified criteria.

Important - The default Cleanup rule is an explicit rule that is added by default to every new layer. You can change or delete the default Cleanup rule. We recommend that you have an explicit Cleanup rule as the last rule in each layer.

Implied Rules

The default rules that are available as part of the Global properties configuration and cannot be edited. You can only select the implied rules and configure their position in the Rule Base:

- First - Applied first, before all other rules in the Rule Base - explicit or implied
- Last - Applied last, after all other rules in the Rule Base - explicit or implied, but before the Implicit Cleanup Rule
- Before Last - Applied before the last explicit rule in the Rule Base

Implicit Cleanup Rule

The default "catch-all" rule for the Layer that deals with traffic that does not match any explicit or implied rules in the Layer. It is made automatically when you create a Layer.

Implicit cleanup rules do not show in the Rule Base.

For R81.10 Security Gateways, the default implicit cleanup rule action is Drop. This is because most Policies have Whitelist rules (the Accept action). If the Layer has Blacklist

rules (the Drop action), you can change the action of the implicit cleanup rule to **Accept** in the Layer Editor.

Order in which the Firewall Applies the Rules

1. First Implied Rule - No explicit rules can be placed before it.
2. Explicit Rules - These are the rules that you create.
3. Before Last Implied Rules - Applied before the last explicit rule.
4. Last Explicit Rule - We recommend that you use a Cleanup rule as the last explicit rule.
5. **Note -** If you use the Cleanup rule as the last explicit rule, the Last Implied Rule and the Implicit Cleanup Rule are not enforced.
6. Last Implied Rule - Remember that although this rule is applied after all other explicit and implied rules, the Implicit Cleanup Rule is still applied last.
7. Implicit Cleanup Rule - The default rule that is applied if none of the rules in the Layer match.

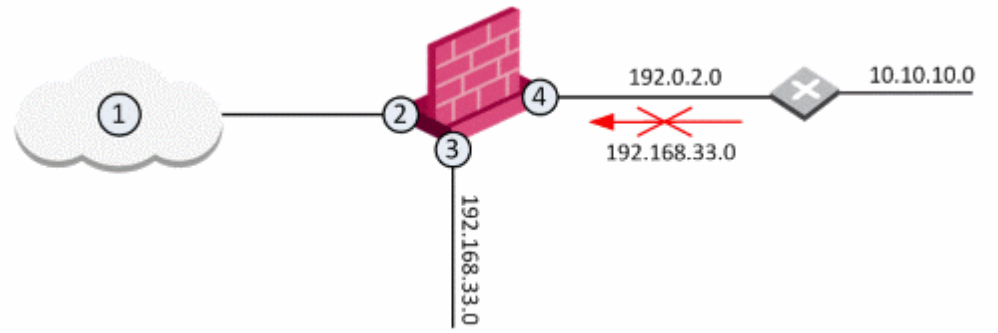
Preventing IP Spoofing

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

Anti-Spoofing detects if a packet with an IP address that is behind a certain interface, arrives from a different interface. For example, if a packet from an external network has an internal IP address, Anti-Spoofing blocks that packet.

Example:

The diagram shows a Gateway with interfaces 2 and 3, and 4, and some example networks behind the interfaces.



For the Gateway, anti-spoofing makes sure that:

- All incoming packets to (2) come from the Internet (1)
- All incoming packets to (3) come from 192.168.33.0
- All incoming packets to (4) come from 192.0.2.0 or 10.10.10.0

If an incoming packet has a source IP address in network 192.168.33.0, the packet is blocked, because the source address is spoofed.

When you configure Anti-Spoofing protection on a Check Point Security Gateway interface, the Anti-Spoofing is done based on the interface topology. The interface topology defines where the interface Leads To (for example, External (Internet) or Internal), and the Security Zone of interface.

Anti-Spoofing Options

Perform Anti-Spoofing based on interface topology - Select this option to enable spoofing protection on this external interface.

Anti-Spoofing action is set to - Select this option to define if packets will be rejected (the Prevent option) or whether the packets will be monitored (the Detect option). The Detect option is used for monitoring purposes and should be used in conjunction with one of the tracking options. It serves as a tool for learning the topology of a network without actually preventing packets from passing.

Don't check packets from - Select this option to make sure anti-spoofing does not take place for traffic from internal networks that reaches the external interface. Define a network object that represents those internal networks with valid addresses, and from the drop-down list, select that network object. The anti-spoofing enforcement mechanism disregards objects selected in the Don't check packets from drop-down menu.

Spoof Tracking - Select a tracking option.

IPS

The Intrusion Prevention Software (IPS) Blade delivers complete and proactive intrusion prevention. It delivers 1,000s of signatures, behavioral and preemptive protections. It gives another layer of security on top of Check Point firewall technology. IPS protects both clients and servers, and lets you control the network usage of certain applications. The hybrid IPS detection engine provides multiple defense layers, which allows it excellent detection and prevention capabilities of known threats, and in many cases future attacks as well. It also allows unparalleled deployment and configuration flexibility and excellent performance.

Elements of IPS

IPS protection includes:

- Detection and prevention of specific known exploits.
- Detection and prevention of vulnerabilities, including both known and unknown exploit tools, for example protection from specific CVEs.
- Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP.
- Detection and prevention of outbound malware communications.
- Detection and prevention of tunneling attempts. These attempts may indicate data leakage or attempts to circumvent other security measures such as web filtering.
- Detection, prevention or restriction of certain applications which, in many cases, are bandwidth consuming or may cause security threats to the network, such as Peer to Peer and Instant Messaging applications.

- Detection and prevention of generic attack types without any pre-defined signatures, such as Malicious Code Protector.
- Check Point constantly updates the library of protections to stay ahead of emerging threats.

Capabilities of IPS

The unique capabilities of the Check Point IPS engine include:

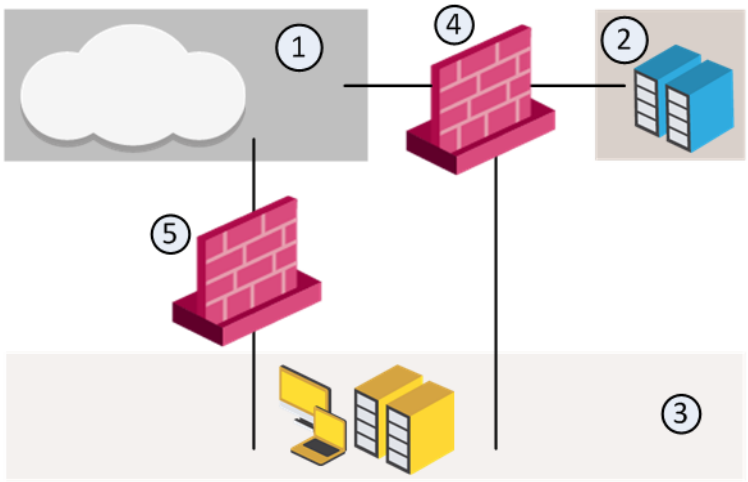
- Clear, simple management interface.
- Reduced management overhead by using one management console for all Check Point products.
- Integrated management with REST API.
- Easy navigation from business-level overview to a packet capture for a single attack.
- #1 security coverage for Microsoft and Adobe vulnerabilities.
- Resource throttling so that high IPS activity will not impact other blade functionality.

For example, some malware can be downloaded by a user unknowingly when browsing to a legitimate web site, also known as a drive-by-download. This malware can exploit a browser vulnerability to create a special HTTP response and sending it to the client. IPS can identify and block this type of attack even though the firewall may be configured to allow the HTTP traffic to pass.

Security Zones

Security Zones allow the creation of a strong Access Control Policy that controls the traffic between parts of the network.

A Security Zone object represents a part of the network, such as the internal network or the external network. You assign a network interface for a Gateway to a Security Zone. You can then use the Security Zone objects in the Source and Destination columns of the Rule Base.



This diagram shows three Security Zones in a typical network: *ExternalZone* (1), *DMZZone* (2), and *InternalZone* (3).

Gateway (4) has three interfaces. One interface is assigned to the *ExternalZone* (1), one interface is assigned to the *DMZZone* (2), and one interface is assigned to *InternalZone* (3).

Gateway (5) has two interfaces. One interface is assigned to *ExternalZone* (1) and one interface is assigned to *InternalZone* (3).

A Gateway interface belongs to only one Security Zone. Interfaces to different networks can be in the same Security Zone.

Using REST API

The instructions for use of this interface are for the Security Management Server Administrator.

Getting Started:

Administrative access to the management server is available through web-based REST API requests from a host workstation.

The host workstation must reside on the same subnet as the Smart-1 management server.

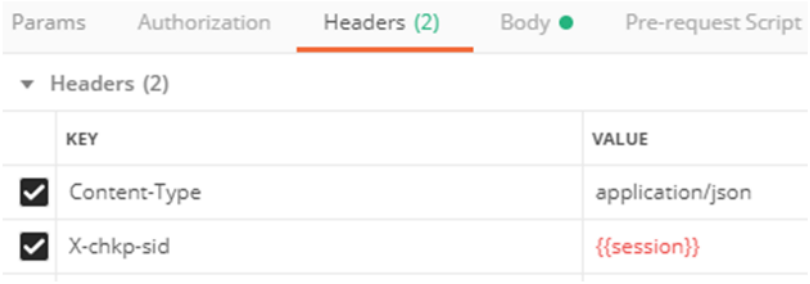
The host workstation needs a tool such as Postman installed to generate HTTP POST requests to send to REST API on the management server. A special Postman collection is available with the REST API requests to use for TOE.

The Postman tool provides administrative access to the management server.

Note - The specialized Postman collection to download and configure on Postman on the host workstation to run TOE REST API requests is available on sk162814 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk162814.

Using Postman:

1. On the drop-down list in your Postman workspace, choose POST as your method.
2. Replace <mgmt ip> with your management server's IP address.
3. Replace <api> with the API you want to use.
4. Click on the Headers tab in the Postman workspace to choose Content-Type as the Key and application/json as the value.
5. After the login, the REST API response includes a session ID. This ID is a second key for the Headers list.



USE CASE - REST API: Publish

To commit administrative changes to the management server database, use Publish:

1. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

   ```
   {
       "user" : <username>,
       "password" : <password>
   }
   ```

2. Use REST API to upload an IPS package (on page 72) and to make parameter changes.
3. Use Publish to save the IPS update and parameter changes.

   URL: `https://<mgmt ip>/web_api/publish`

   Body:

   ```
   {
       "uid" : <session uid - not mandatory>
   }
   ```

USE CASE - REST API: IPS Updates

The Intrusion Prevention Software (IPS) Blade delivers 1,000s of signatures, behavioral and preemptive protections.

Use REST API to upload IPS packages and save them on the management server:

1. Obtain the IPS package. See **Post Install Configuration**.

   Note - Obtain the offline IPS signature update package according to sk93724 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93724.

2. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

   ```
   {
       "user" : <username>,
       "password" : <password>
   }
   ```

3. Upload the IPS package to the management server using the `generic-upload-file` API.

   URL: `https://<mgmt ip>/web_api/generic-upload-file`

   Headers:

   ```
   application/octet-stream
   x-chkp-file-name
   x-chkp-sid
   ```


Body:

```
{
"mode" : "file",
    "file" : {}
}
```

4. Use the file name from the `generic-upload-file` API response to perform `run-ips-update`.

   URL: `https://<mgmt ip>/web_api/run-ips-update`

   Body:

   ```
   {
       "package-path" : "path/to/update.upf"
   }
   ```

5. Use Publish to save the IPS update to the policy database.

   URL: `https://<mgmt ip>/web_api/publish`

   Body:

   ```
   {
       "uid":<session uid – not mandatory>
   }
   ```

6. Install the policy on the Security Gateway with `install-policy`.

   URL: `https://<mgmt ip>/web_api/install-policy`

   Body:

   ```
   {
       "policy-package" : <Name of the Policy Package to be
       installed>,
       "targets" : <GW_name>,
       "access" : true,
       "threat-prevention" : true
   }
   ```


USE CASE - REST API: Managing IPS

Managing Intrusion Prevention System (IPS) with REST API:

1. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

```
{
    "user" : <username>,
    "password" : <password>
}
```

2. Use `add-simple-gateway` to enable IPS on Gateways as you add them.

   URL: `https://<mgmt ip>/web_api/add-simple-gateway`

   Body:

```
{
    "name" : <GW_name>,
    "ipv4-address" : <GW_EX_IP>,
    "firewall" : true,
    "ips" : true,
    "version" : "R81",
    "one-time-password" : <one time password>,
    "interfaces" : [{
       "name" : <name>,
       "ipv4-address" : <ip>,
       "ipv4-network-mask" : <mask>,
       "anti-spoofing" : true,
       "topology" : <EXTERNAL/INTERNAL>
    },
    {
       "name" : <name>,
       "ipv4-address" : <ip>,
       "ipv4-network-mask" : <mask>,
       "anti-spoofing" : true,
       "topology" : <EXTERNAL/INTERNAL>,
       "security-zone" : true,
       "security-zone-settings" : {
           "auto-calculated" : true
       }
       "topology-settings" : {
           "ip-address-behind-this-interface" : "LOCAL_NETWORK"
       }
    }]
}
```


Note - See REST API: Anti-Spoofing (on page 75) and REST API: Implementing Zone-Based Security (on page 77) for more information.

3. IPS is disabled by default. Use `set-simple-gateway` to set the IPS attribute to `true` if the attribute is still `false`.

   URL: `https://<mgmt ip>/web_api/set-simple-gateway`

   Body:

```
{
    "name" : <GW_name>,
    "ips" : true
}
```

Recommended - Update the default IPS package by using `run-ips-update` (on page 72).

4. Threat Profile determines how each threat blade will act.

   To create a new profile, use `add-threat-profile` https://sc1.checkpoint.com/documents/latest/APIs/index.html?#web/add-threat-profile~v1.5%20.

5. Threat Rule specifies a distinct behavior of traffic regarding threats.

   To create a new threat rule, use `add-threat-rule` https://sc1.checkpoint.com/documents/latest/APIs/index.html?#web/add-threat-rule~v1.5%20.

6. Threat Exception permits specific behaviors that are otherwise not allowed, such as allowing traffic between two specific hosts when a rule prohibits all traffic.

   To create a threat exception, use `add-threat-exception` https://sc1.checkpoint.com/documents/latest/APIs/index.html?#web/add-threat-exception~v1.5%20.

Note - Threat Policy is the set of rules that use Threat Profiles to enforce protection.

USE CASE - REST API: Anti-Spoofing

Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access. Anti-Spoofing detects if a packet with an IP address that is behind a certain interface, arrives from a different interface.

Use Anti-Spoofing prevention to protect your security Gateways as you add them to the management server:

1. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

```
{
```



```
"user" : <username>,
"password" : <password>
}
```

2. Use `add-simple-gateway` to enable anti-spoofing on gateways as you add them.

   URL: `https://<mgmt ip>/web_api/add-simple-gateway`

   Body:

```
{
    "name" : <GW_name>,
    "ipv4-address" : <GW_EX_IP>,
    "firewall" : true,
    "ips" : true,
    "version" : "R81",
    "one-time-password" : <one time password>,
    "interfaces" : [{
       "name" : <name>,
       "ipv4-address" : <ip>,
       "ipv4-network-mask" : <mask>,
       "anti-spoofing" : true,
       "topology" : <EXTERNAL/INTERNAL>
    },
    {
       "name" : <name>,
       "ipv4-address" : <ip>,
       "ipv4-network-mask" : <mask>,
       "anti-spoofing" : true,
       "topology" : <EXTERNAL/INTERNAL>,
       "security-zone" : true,
       "security-zone-settings" : {
           "auto-calculated" : true
       }
       "topology-settings" : {
           "ip-address-behind-this-interface" : "LOCAL_NETWORK"
       }
    }]
}
```


USE CASE - REST API: Implementing Zone-Based Security

These are the predefined security zones and their intended purposes:

- WirelessZone - Networks that can be accessed by users and applications through a wireless connection.
- ExternalZone - Networks that are not secure, such as the internet and other external networks.
- DMZZone - A DMZ (demilitarized zone) is sometimes referred to as a perimeter network. It has company servers that can be accessed from external sources.
- **Note** - A DMZ lets external users and applications access specific internal servers, but prevents the external users accessing secure company networks. Add rules to the firewall Rule Base that allow traffic to the company DMZ. For example, a rule that allows HTTP and HTTPs traffic to your web server in the DMZ.
- InternalZone - Company networks with sensitive data that must be protected and used only by authenticated users.

To create a Security Zone:

1. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

```
{
    "user" : <username>,
    "password" : <password>
}
```

2. Use `add-security-zone` to add one or more Security Zones.

Note - Use an array [] if you add more than one.

URL: `https://<mgmt ip>/web_api/add-security-zone`

Body:

```
[
{
    "name" : <ZoneName>,
    "comments" : <My Security Zone 1>,
    "color" : "yellow"
},
{
    "name" : <ZoneName2>,
    "comments" : <My Security Zone 2>,
    "color" : "blue"
}
]
```


To assign an interface to a Security Zone:

1. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

```
{
     "user" : <username>,
     "password" : <password>
}
```

2. Use `set-simple-gateway` to assign a Gateway interface to a Security Zone.

   URL: `https://<mgmt ip>/web_api/set-simple-gateway`

   Body:

```
{
    "name" : <GW_name>,
    "interfaces" : {
       "name" : <name>,
       "security-zone-settings" : {
           "specific-zone" : <Zone name>
       }
     }
}
```

USE CASE - REST API: Traffic Between Two Networks

Use REST API to allow traffic between two networks:

1. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

```
{
    "user" : <username>,
    "password" : <password>
}
```

2. Use `add-network` to create the first network object.

   URL: `https://<mgmt ip>/web_api/add-network`

   Body:

```
{
    "name" : <New Network 1>,
    "subnet" : "192.0.2.0",
    "subnet-mask" : "255.255.255.0"
 }
```

3. Use `add-network` to create the second network object.

   URL: `https://<mgmt ip>/web_api/add-network`

Body:

```
{
    "name" : <New Network 2>,
    "subnet" : "192.0.2.0",
    "subnet-mask" : "255.255.255.0"
 }
```

4. Allow traffic between the two network objects with `add-access-rule`:

   URL: `https://<mgmt ip>/web_api/add-access-rule`

   Body:

```
{
    "layer" : <Layer name>,
    "position" : "top",
    "name" : "Rule name",
    "source" : <First new network name>,
    "destination" : <Second new network name>,
    "action" : "accept",
    "track" : {
       "type" : "log"
    }
}
```

USE CASE - REST API: Blocking an IP Address

Use REST API to block an IP address:

1. Log in to the management server through Postman on the host workstation.

   URL: `https://<mgmt ip>/web_api/login`

   Body:

```
{
    "user" : <username>,
    "password" : <password>
}
```

2. Use `add-host` to identify a malicious IP address.

   URL: `https://<mgmt ip>/web_api/add-host`

   Body:

```
{
    "name" : <Unique object name>,
    "ip-address" : <IP address>
}
```

3. Use `add-access-rule` to create a rule to block the IP address.

   URL: `https://<mgmt ip>/web_api/add-access-rule`

   Body:

```
    {
        "layer" : <Layer name>,
        "position" : "top",
        "source" : <Malicious host name>,
        "destination" : <any>,
        "service" : <any>,
        "action" : "drop",
        "track" : {
           "type" : "log"
        }
}
```


REST API Allowed Calls

To establish an administrative connection with the Security Management Server, a `login` request must be sent:

```
POST https://<host>:443/web_api/login
```

This full management API is documented in the Management API Reference https://sc1.checkpoint.com/documents/latest/APIs/index.html.

The following table provides a complete listing of REST APIs the Security Management Server Administrator permitted for use in the TOE configuration.

API name	Purpose	Reference
`login`	Login into the management server, authenticate and authorize the administrator. If no session identifier is provided a new work session for changes will be created. If a session identifier is provided as an argument the administrator can connect to an open session of previously unpublished changes.	`https://sc1.checkpoint.com/documents/latest/APIs/#web/login~v1.5%20`
`keep-alive`	Keeps the session active – prevents session automatic logout due to inactivity.	`https://sc1.checkpoint.com/documents/latest/APIs/#cli/keepalive~v1.5%20`
`publish`	Publishes the changes made in an administrator's private session, making them public to all administrators.	`https://sc1.checkpoint.com/documents/latest/APIs/#web/publish~v1.5%20`

API name	Purpose	Reference
discard	Discard the changes made in an administrator's private session.	https://sc1.checkpoint.com/documents/latest/APIs/#web/discard~v1.5%20
logout	Logout from the active session.	https://sc1.checkpoint.com/documents/latest/APIs/#web/logout~v1.5%20
add-host	Represents a single host in the network. This object can be used in rules within the security policy to define relevant source or destination IPs for that rule.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-host~v1.5%20
set-host		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-host~v1.5%20
delete-host		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-host~v1.5%20
add-network	A Network is a group of IP addresses defined by a network address and a net mask. This object can be used in rules within the security policy to define relevant source or destination IPs for that rule.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-network~v1.5%20
set-network		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-network~v1.5%20
delete-network		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-network~v1.5%20
add-address-range	An address range is a range of IP addresses on the network, defined by the lowest and the highest IP addresses. This object can be used in rules within the security policy to define relevant source or destination IPs for that rule.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-address-range~v1.5%20
set-address-range		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-address-range~v1.5%20
delete-address-range		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-address-range~v1.5%20

API name	Purpose	Reference
add-simple-gateway	Add, modify or delete an object that represents a gateway object. To install security policies on the Security Gateways a gateway object has to be created to specify the properties of the gateway, such as IP address.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-simple-gateway~v1.5%20
set-simple-gateway		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-simple-gateway~v1.5%20
delete-simple-gateway		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-simple-gateway~v1.5%20
add-security-zone	Security Zones let you to create a strong Access Control Policy that controls the traffic between parts of the network. A Security Zone object represents a part of the network (for example, the internal network or the external network).	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-security-zone~v1.5%20
set-security-zone		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-security-zone~v1.5%20
delete-security-zone		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-security-zone~v1.5%20
add-package	Add/Modify/Delete policy package object. Policy package bundles together Access and Threat rulebases. Policy Installation actually implies installing a specific policy package on gateway.	https://sc1.checkpoint.com/documents/latest/APIs/#cli/add-package~v1.5%20
set-package		https://sc1.checkpoint.com/documents/latest/APIs/#cli/set-package~v1.5%20
delete-package		https://sc1.checkpoint.com/documents/latest/APIs/#cli/delete-package~v1.5%20
add-time	Time objects support configuration of time-based rules in an access policy. One or more time	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-time~v1.5%20
set-time		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-time~v1.5%20

API name	Purpose	Reference
delete-time	objects specified in a rule make it active only during specified times.	https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-time~v1.5%20
add-dns-domain	A Domain object lets you define a host or DNS domain by its name only. It is not necessary to have the IP address of the site.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-dns-domain~v1.5%20
set-dns-domain		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-dns-domain~v1.5%20
delete-dns-domain		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-dns-domain~v1.5%20
add-service-tcp	Allows adding, modifying and deleting an object that represents a TCP service. These objects can be used in rules within the security policy to define the TCP services matched for that rule.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-service-tcp~v1.5%20
set-service-tcp		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-service-tcp~v1.5%20
delete-service-tcp		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-service-tcp~v1.5%20
add-service-udp	Allows adding, modifying and deleting an object that represents a UDP service. These objects can be used in rules within the security policy to define the UDP services matched for that rule.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-service-udp~v1.5%20
set-service-udp		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-service-udp~v1.5%20
delete-service-udp		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-service-udp~v1.5%20
add-service-icmp	Allows adding, modifying and deleting an object that represents a UDP service. These objects can be used	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-service-icmp~v1.5%20
set-service-icmp		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-service-icmp~v1.5%20

API name	Purpose	Reference
delete-service-icmp	in rules within the security policy to define the UDP services matched for that rule.	https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-service-icmp~v1.5%20
add-access-rule	Add an access rule to the input policy. Access rules defines allows the definition of Stateful Traffic Filtering rules.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-access-rule~v1.5%20
set-access-rule		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-access-rule~v1.5%20
delete-access-rule		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-access-rule~v1.5%20
add-threat-rule	Add / modify / delete a threat rule.	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-threat-rule~v1.5%20
set-threat-rule		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-threat-rule~v1.5%20
delete-threat-rule		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-threat-rule~v1.5%20
add-threat-exception	Add / modify / delete an Exception to Threat rule	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-threat-exception~v1.5
set-threat-exception		https://sc1.checkpoint.com/documents/latest/APIs/#web/set-threat-exception~v1.5
delete-threat-exception		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-threat-exception~v1.5
set-threat-protection	Controls individual protection behavior, by overwriting the Threat Profile's settings	https://sc1.checkpoint.com/documents/latest/APIs/#web/set-threat-protection~v1.5
add-threat-profile	Add / Modify / Delete Threat Profile. The Threat	https://sc1.checkpoint.com/documents/latest/APIs/#web/add-threat-profile~v1.5

API name	Purpose	Reference
set-threat-profile	Profile determines behavior of each individual protection.	https://sc1.checkpoint.com/documents/latest/APIs/#web/set-threat-profile~v1.5
delete-threat-profile		https://sc1.checkpoint.com/documents/latest/APIs/#web/delete-threat-profile~v1.5
run-ips-update	Updates the Management IPS protections database from an offline package that resides on the Management server.	https://sc1.checkpoint.com/documents/latest/APIs/#web/run-ips-update~v1.5
install-policy	Installs the input policy on the assigned Gateways.	https://sc1.checkpoint.com/documents/latest/APIs/#web/install-policy~v1.5
add-administrator	Allows adding, modifying or deleting administrator accounts. In the evaluated configuration, administrator accounts can only be associated with the "read write all" permissions profile.	https://sc1.checkpoint.com/documents/latest/APIs/#cli/add-administrator~v1.5%20
delete-administrator		https://sc1.checkpoint.com/documents/latest/APIs/#cli/delete-administrator~v1.5%20
set-administrator		https://sc1.checkpoint.com/documents/latest/APIs/#cli/set-administrator~v1.5%20
generic-upload-file	Upload file to the Management Server	Upload a file to the management server.

Note:

`generic-upload-file`

- Description

  This API unloads a file to the management server. The file will be uploaded to the `$FWDIR/tmp/uploaded-files` folder.

  The file will be saved under an auto-generated name, unless a specific name has been requested by providing the `X-chkp-file-name` header.

- Request URL
  `POST https://<mgmt-server>:<port>/web_api/generic-upload-file`
- Request Headers

`X-chkp-sid`	string token	Session unique identifier as it returned by the login request
`Content-type`	`application/octet-stream`	
`X-chkp-file-name`	String	Name of the file on the server. *Optional*.

- Request Body
  The file content will be sent as the request body.
- Response
  On success:
  HTTP code 200
  The full file name on the server
  On error:
  HTTP code 400, 401, 403, 404, 409, 500, 501
  Error message
- See the **USE CASE - REST API: IPS Updates** section.

Concepts of Orchestrator Management

Check Point offers effective management of the Scalable Deployment through the Orchestrator WebUI. The administrator authenticates to the Gaia portal (Web UI) on the Orchestrator by connecting with the web browser on the MHO Administrator PC to

```
https://<orchestrator_ip_address>
```

The administrative user is prompted to enter their user name and password to authenticate to the WebUI.

Management of Orchestrator administrator accounts

To create additional administrator accounts on the Orchestrator appliance navigate to User Management > Users. Select the “Add” button to open the Add User window. Enter the user details as prompted, selecting “Web” as the Access Mechanism and “adminRole” as the Assigned Role. It is advised that the “User must change password at next logon”.

To modify an existing administrator account select the “Edit” button on the User Management > Users page, and to delete an existing administrator account (other than that the user is logged in as) select the “Delete” button on the User Management > Users page.

Password Policy

The password policy to be applied when Orchestrator administrators change their password can be defined by navigating to User Management > Password Policy.

The policy should be configured to enforce a minimum of:

- At least 15 characters, in length
- A mixture of alphabetic, upper case, lower case, numeric and special characters
- At least four different characters
- Does not use simple dictionary words, or common strings such as “qwerty”

The password policy can also be used to configure the number of failed login attempts before access to the account is denied under the “Deny access after failed login attempts” settings, which should be set to “3”. The “Allow access again after time” setting should be set to 1800 seconds (30 minutes).

Session Timeout

The length of time before an inactive session is terminated can be configured by navigating to System Management > Session. The “Inactivity Timeout” value under Web UI should be set according to the organization policies for locking/disconnecting unattended workstations (e.g. 10 minutes).

System Time

To set the system clock on Orchestrator navigate to System Management > Time and click “Set Time and Date”. In the Time and Date settings window, ensure the “Set Time and Date

automatically using Network Time Protocol (NTP)" is selected, with the hostname/IP address of the NTP server(s).

System Logging

To ensure all logs are sent to the Security Management Server navigate to System Management > System Logging and set the following options:

- Select "Send Syslog messages to management server" (not selected by default)
- Select "Send audit logs to management server upon successful configuration" (selected by default)

Host access

To limit the hosts that can connect to the Gaia portal to perform management of the Orchestrator appliance(s) navigate to System Management > Host Access and click "Add" to add a new client that is authorized to connect to the Gaia portal. Enter the client details in the "Host" entry and click "OK".

Security Group

The Security Group works as one large Security Gateway and all Security Group Members are configured with the same policy. When you install a policy from the Management Server, it first installs the policy on the SMO Security Group Member. The Single Management Object (SMO) is a Check Point technology that manages the Security Group as one large Security Gateway with one management IP address.

The SMO copies the policy and Security Group Member configuration to all Security Group Members in the UP state. When the Security Group Member enters the UP state, it automatically gets the installed policy and configurations that are installed, from the SMO. When there is only one Security Group Member in the UP state, it is possible there is no SMO. Then, that Security Group Member uses its local policy and configuration.

Security Groups are configured as described in section "*SP Security Group Configuration (for SP deployment)*" above.

Check Point User Center

A description for creating a Check Point User Center account is provided under SecureKnowledge Solution ID sk22716 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk22716.

Further SecureKnowledge Solutions can be searched: