19 May 2020

CHECK POINT
1200R/1400 APPLIANCES
CENTRALLY MANAGED

R77.20.81
Models: L-61i, L-71, L-71W, L-71WD, L-72, L-72W, L-72P

Administration Guide
Important Information

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

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page

Check Point R77.20.81
For more about this release, see the R77.20.81 home page

Latest Version of this Document
Open the latest version of this document in a Web browser

Download the latest version of this document in PDF format

To learn more, visit the Check Point Support Center

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point 1200R/1400 Appliances Centrally Managed R77.20.81 Administration Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 May 2020</td>
<td>LAN as WAN supported in SMP</td>
</tr>
<tr>
<td>18 October 2018</td>
<td>First release of this document</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Sample Configuration File</td>
<td>40</td>
</tr>
<tr>
<td>Preparing the Configuration Files</td>
<td>41</td>
</tr>
<tr>
<td>Deploying the Configuration File - Initial Configuration</td>
<td>41</td>
</tr>
<tr>
<td>Deploying the Configuration File - Existing Configuration</td>
<td>41</td>
</tr>
<tr>
<td>Viewing Configuration Logs</td>
<td>42</td>
</tr>
<tr>
<td>Troubleshooting Configuration Files</td>
<td>42</td>
</tr>
<tr>
<td>Using the set property Command</td>
<td>44</td>
</tr>
<tr>
<td>Appliance Configuration</td>
<td>45</td>
</tr>
<tr>
<td>Introduction to the WebUI Application</td>
<td>45</td>
</tr>
<tr>
<td>The Home Tab</td>
<td>46</td>
</tr>
<tr>
<td>Viewing System Information</td>
<td>46</td>
</tr>
<tr>
<td>Controlling and Monitoring Software Blades</td>
<td>46</td>
</tr>
<tr>
<td>Setting the Management Mode</td>
<td>47</td>
</tr>
<tr>
<td>Managing Licenses</td>
<td>49</td>
</tr>
<tr>
<td>Viewing the Site Map</td>
<td>50</td>
</tr>
<tr>
<td>Managing Active Devices</td>
<td>50</td>
</tr>
<tr>
<td>Viewing System Logs</td>
<td>51</td>
</tr>
<tr>
<td>Viewing Reports</td>
<td>53</td>
</tr>
<tr>
<td>Using System Tools</td>
<td>54</td>
</tr>
<tr>
<td>Managing the Device</td>
<td>56</td>
</tr>
<tr>
<td>Configuring Internet Connectivity</td>
<td>56</td>
</tr>
<tr>
<td>Configuring the Wireless Network</td>
<td>61</td>
</tr>
<tr>
<td>Configuring the Local Network</td>
<td>64</td>
</tr>
<tr>
<td>Configuring a Hotspot</td>
<td>72</td>
</tr>
<tr>
<td>Configuring the Routing Table</td>
<td>74</td>
</tr>
<tr>
<td>Configuring MAC Filtering</td>
<td>77</td>
</tr>
<tr>
<td>Configuring the DNS Server</td>
<td>79</td>
</tr>
<tr>
<td>Configuring the Proxy Server</td>
<td>80</td>
</tr>
<tr>
<td>Backup, Restore, Upgrade, and Other System Operations</td>
<td>80</td>
</tr>
<tr>
<td>Configuring Local and Remote System Administrators</td>
<td>84</td>
</tr>
<tr>
<td>Configuring Administrator Access</td>
<td>89</td>
</tr>
<tr>
<td>Managing Device Details</td>
<td>90</td>
</tr>
<tr>
<td>Managing Date and Time</td>
<td>91</td>
</tr>
<tr>
<td>Configuring DDNS and Access Services</td>
<td>91</td>
</tr>
<tr>
<td>Using System Tools</td>
<td>93</td>
</tr>
<tr>
<td>Managing Installed Certificates</td>
<td>93</td>
</tr>
<tr>
<td>Configuring High Availability</td>
<td>94</td>
</tr>
<tr>
<td>Configuring Advanced Settings</td>
<td>94</td>
</tr>
<tr>
<td>Managing Users and Objects</td>
<td>96</td>
</tr>
<tr>
<td>Configuring Local Users and User Groups</td>
<td>96</td>
</tr>
<tr>
<td>Configuring Local and Remote System Administrators</td>
<td>97</td>
</tr>
<tr>
<td>Managing Authentication Servers</td>
<td>102</td>
</tr>
<tr>
<td>Managing System Services</td>
<td>104</td>
</tr>
<tr>
<td>Managing Service Groups</td>
<td>105</td>
</tr>
<tr>
<td>Managing Network Objects</td>
<td>106</td>
</tr>
<tr>
<td>Managing URL Lists</td>
<td>108</td>
</tr>
<tr>
<td>Logs and Monitoring</td>
<td>110</td>
</tr>
<tr>
<td>Viewing Security Logs</td>
<td>110</td>
</tr>
<tr>
<td>Viewing System Logs</td>
<td>111</td>
</tr>
<tr>
<td>Configuring External Log Servers</td>
<td>112</td>
</tr>
<tr>
<td>Managing Active Devices</td>
<td>112</td>
</tr>
<tr>
<td>Viewing Infected Hosts</td>
<td>112</td>
</tr>
<tr>
<td>Viewing VPN Tunnels</td>
<td>114</td>
</tr>
</tbody>
</table>
Check Point 1200R and 1400 Appliance Overview

Check Point 1200R and 1400 appliances support the Check Point Software Blade architecture and provide independent, modular and centrally managed security building blocks. You can quickly enable and configure the Software Blades to meet your specific security needs.

These appliances run an embedded version of the Gaia operating system. It includes core configuration elements such as clish interface, SNMPv2/3 and routing stack implementations. In addition to the Gaia features, Embedded Gaia contains support for built-in network switches, wireless networks, 4G/LTE Internet connectivity, multiple Internet connections (more than 2) in High Availability or Load Sharing mode, Policy Based Routing, and DDNS support. Quick deployment with USB is supported for all appliances, and with SD card for the 1200R and 1400 appliances. For more information, see the 1400 Security Gateway series product page https://supportcenter.checkpoint.com/supportcenter/portal?model=&version=R77&os=&eventSubmit_doShowproductpage=&productTab=documents&product=490.

The Check Point 1200R appliance is a ruggedized appliance that delivers Next Generation Threat Prevention for critical infrastructure and industrial control systems. This solid-state appliance is specifically designed to secure SCADA (supervisory control and data acquisition) protocols and OT (operational technology) equipment that operates under harsh environmental conditions. It complies with industrial specifications IEEE 1613, IEC 61850-3, IEC 60068-2 for heat, vibration and immunity to electromagnetic interference (EMI).

This guide describes all aspects that apply to central management mode. For more information on central management, see the Check Point 1200R/1400 Locally Managed Administration Guide.  

Note - Some topics only apply to specific appliances or models.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Model</th>
<th>Appliance Homepage</th>
</tr>
</thead>
</table>
| 1200R     | Wired | sk105379
http://supportcontent.checkpoint.com/solutions?id=sk105379 |
| 1430/1450 | Wired, WiFi, WiFi + DSL | sk110985
http://supportcontent.checkpoint.com/solutions?id=sk110985 |
| 1470/1490 | Wired, WiFi, PoE Wired | sk110985
http://supportcontent.checkpoint.com/solutions?id=sk110985 |

For front and back panel details for each appliance, see the relevant Getting Started Guide.

Review these materials before doing the procedures in this guide:

- *R77.20.81 Release Notes*
- Known Limitations
- Resolved Issues
- Getting Started Guide
- Small Business Security video channel
  https://www.youtube.com/playlist?list=PLMAKXIJBvfAhDnKJwE5dFgiChiSqVVoW

See the R77.20.81 home page http://supportcontent.checkpoint.com/solutions?id=sk137212.
Installation

In This Section:

- Setting Up the Check Point Appliance ................................................................. 8
- Connecting the Cables ............................................................................................ 8
- About the PoE ......................................................................................................... 9
- Deployment Types ................................................................................................ 9
- Predefining a Centrally Managed Deployment ...................................................... 9
- Small-scale Deployment Installation ..................................................................... 10
- Large-scale Deployment Installation .................................................................... 22

Setting Up the Check Point Appliance

1. Remove the Check Point Appliance from the shipping carton and place it on a tabletop.
2. Identify the network interface marked as LAN1. This interface is preconfigured with the IP address 192.168.1.1.

Connecting the Cables

1. Connect the power supply unit to the appliance and to a power outlet.
   The appliance is turned on when the power supply unit is connected to an outlet.
   The Power LED on the front panel lights up. This indicates that the appliance is turned on.
   The Alert LED on the front panel starts to blink. This indicates that the appliance is booting up.
   When the Alert LED turns off, the appliance is ready for login.
2. Connect the standard network cable to the LAN1 port on the appliance and to the network adapter on your PC.
3. If you use an external modem:
   Connect the Ethernet cable to the WAN port on the appliance back panel and plug it into your external modem or router’s PC/LAN network port. The WAN Link LED on the appliance front panel lights up when the Ethernet is connected.
4. If you do not use an external modem:
   Connect the telephone cable to the DSL port on the appliance back panel and plug it into the DSL line socket. The DSL Link LED as well as the Internet Link LED remains off until you configure the appliance, including setting up the DSL as an internet connection.
About the PoE

The PoE wired model is in 1470/1490 appliances only.

The PoE switch is a type of PSE (Power Sourcing Equipment), and delivers power to the PD (Powered Devices) end point. By default, the PoE port automatically provides power when a compliant PD is connected. There are no specified management requirements.

The PoE standard model is fully supported. It is fully compliant with 802.3af (PoE) and 802.3at (PoE+). All 4 ports support 802.3af. Due to power budget limitations, only 2 ports at a time support 802.3at.

The total power dedicated for all PoE ports is 62W:
- 802.3af maximum power delivery per port is 15.4W
- 802.3at maximum power delivery per port is 31W

Deployment Types

There are two types of centrally managed deployments:

- **Small-scale deployment** - Where you configure between 1 and 25 Check Point Appliance gateways using SmartDashboard. Then you can manage device settings from SmartProvisioning.
- **Large-scale deployment** - Where you configure over 25 Check Point Appliance gateways using a SmartLSM profile and SmartProvisioning or a configuration file that is stored on a USB drive.

For both deployment types, you must configure objects and other elements in SmartDashboard and in SmartProvisioning.

Predefining a Centrally Managed Deployment

To manage the Check Point Appliance in a centrally managed deployment, you must install a Security Management Server and SmartConsole clients that operate with the Check Point Appliance.

The Check Point Appliance operates with Security Management Server versions R77.30 and higher.

For installation instructions, see the version’s Release Notes.

After you install the SmartConsole clients you can define the Check Point Appliance object in SmartDashboard (in small-scale deployments) or create a SmartLSM profile (in large-scale deployments) and prepare the security policy.
Small-scale Deployment Installation

In This Section:

Small-scale Deployment Workflow ................................................................. 10
Defining a Gateway Object ............................................................................. 10
Defining a Gateway Cluster Object ................................................................. 13
Creating the Security Policy .......................................................................... 17
Setting Server IP Behind a 3rd Party NAT Device ......................................... 21

This chapter contains procedures for defining a gateway or a gateway cluster. Do the procedures that match your requirements, then install the policy.

Small-scale Deployment Workflow

This is the suggested workflow for small-scale deployments:

1. Create the necessary gateway or cluster objects for your appliances in SmartDashboard.
2. Install the Security Policy in SmartDashboard.
3. Configure the relevant appliances with the First Time Configuration Wizard. Alternatively, you can use a USB drive to quickly configure many appliances without the First Time Configuration Wizard. For more details, see Deploying from a USB Drive.
4. Manage the appliance settings in SmartProvisioning for the gateway or cluster objects.

Defining a Gateway Object

You can use the SmartDashboard creation wizard to define a Check Point Appliance before or after you configure the appliance on site.

Options to define a gateway object:

- **Management First** - Define the gateway object in SmartDashboard before you configure and set up the actual appliance on site. This is commonly used for remotely deployed appliances or appliances that connect to the Security Management Server with a dynamic IP (assigned by a DHCP server or an ISP), as the IP is not known at the time of the configuration of the object in SmartDashboard. You can prepare a policy that the appliance pulls when it is configured.

- **Gateway First** – Configure and set up the Check Point Appliance first. It then tries to communicate with the Security Management Server (if this is configured) at 1 hour intervals. If there is connectivity with the gateway during object creation in SmartDashboard, the wizard can retrieve data from the gateway (such as topology), and then help in configuration.

To define a single gateway object:

1. Log in to SmartDashboard using your Security Management credentials.
2. From the Network Objects tree, right click **Check Point** and select **Security Gateway**.
   The Check Point Security Gateway Creation window opens.
3. Select **Wizard Mode**.
   The wizard opens to General Properties.
4. Enter a name for the Check Point Appliance object and select the hardware type for the hardware platform. If the appliance does not appear in the hardware list in the R77.30 SmartDashboard, see sk111292 http://supportcontent.checkpoint.com/solutions?id=sk111292.

5. Set the Security Gateway Version to R77.20.

6. Select the Static IP address or Dynamic IP address to get the gateway’s IP address.

7. Click Next.

To configure a static IP address:

1. In the Authentication section, select Initiate trusted communication securely by using a one-time password or Initiate trusted communication without authentication (less secure).

2. If you selected Initiate trusted communication securely by using a one-time password, enter a one-time password and confirm it. This password is only used to establish the initial trust. Once established, trust is based on security certificates.

   **Important** - This password must be identical to the one-time password you define for the appliance in the First Time Configuration Wizard.

3. In the Trusted Communication section, select Initiate trusted communication automatically when the Gateway connects to the Security Management server for the first time or Initiate trusted communication now.

4. Click Connect.

   A status window appears.

5. Click Next.

To configure a dynamic IP address:

1. In the Gateway Identifier section, select one identifier: Gateway name, MAC address or First to connect.

2. In the Authentication section, select Initiate trusted communication securely by using a one-time password or Initiate trusted communication without authentication (less secure).

3. If you select Initiate trusted communication securely by using a one-time password, enter a one-time password and confirm it. This password is only used for establishing the initial trust. Once established, trust is based on security certificates.

   **Important** - This password must be identical to the one-time password you define for the appliance in the First Time Configuration Wizard.

4. Click Next.

To configure the software blades:

In the Blade Activation page, select the software blades that you want to activate and configure.

To configure blades later:

1. Select Activate and configure software blades later.

2. Click Next.
To configure blades now:

1. Select **Activate and configure software blades now**.
2. Select the check boxes next to the blades you want to activate and configure.
3. Configure the required options:
   - **NAT** - the *Hide internal networks behind the Gateway’s external IP* checkbox is selected by default.
   - **QoS** - Set the inbound and outbound bandwidth rates.
   - **IPSec VPN** - Make sure that the VPN community has been predefined. If it is a star community, the Check Point Appliance is added as a satellite gateway. Select a VPN community that the Gateway participates in from the **Participate in a site to site community** list.
   - **IPS** - Select a profile from the **Assign IPS Profile** list or click **Manage** to create/edit an IPS profile.
   - **User Awareness** - Complete the wizard pages that open to define the User Awareness acquisition sources. In the Active Directory Servers page of the wizard, make sure to select only AD servers that your gateway works with.
4. Click **Next**.

To hide the VPN domain:

Select **Hide VPN domain behind this gateway’s external IP**.

Select this option only if you want to hide all internal networks behind this gateway’s external IP. All outgoing traffic from networks behind this gateway to other sites that participate in VPN community will be encrypted.

With this option, connections that are initiated from other sites that are directed to hosts behind this gateway are not encrypted. If you need access to hosts behind this gateway, select other options (define VPN topology) or make sure all traffic from other sites is directed to this gateway’s external IP and define corresponding NAT port-forwarding rules, such as: Translate the destination of incoming HTTP connections that are directed to this gateway’s external IP to the IP address of a web server behind this gateway.

To create a new VPN domain group:

1. Make sure that the **Create a new VPN domain** option is selected.
2. In the **Name** field, enter a name for the group.
3. From the **Available objects** list, select the applicable objects and click **Add**. The objects are added to the VPN domain members list.

To select a predefined VPN domain:

1. Click **Select an existing VPN domain**.
2. From the **VPN Domain** list, select the domain.
3. Click **Next**.
   
   In the Installation Wizard Completion page, you see a summary of the configuration parameters you set.
4. If you want to configure more options of the Security Gateway, select **Edit Gateway properties for further configuration**.
5. Click **Finish**.
   
The General Properties window of the newly defined object opens.
Defining a Gateway Cluster Object

A Check Point Appliance Security Gateway is a group of 2 members. Each represents a separate Check Point Appliance which has High Availability software installed. ClusterXL is the Check Point clustering solution. Third party OPSEC Certified clustering products are not supported.

High Availability

High Availability allows organizations to maintain a connection when there is a failure in a cluster member. Only one machine is active (Active/Standby operation) in this configuration. Load sharing is not supported on this appliance.

Prerequisites

During Cluster configuration, only a “Gateway First” installation path is supported. Therefore, you must first configure the gateways with their actual IPs. Only afterward should you create the cluster object in SmartDashboard or SmartProvisioning. The policy installation from the Security Management Server alerts the gateways that they are configured as cluster members.

Before you define a Check Point Appliance cluster, make sure you defined all of the network interfaces used for each of the Check Point Appliance gateways. The interfaces must be defined in the same subnet. To verify definitions, access the WebUI of the appliance.

These actions are only required to work with the Cluster Wizard in SmartDashboard:

- Make sure a cable is connected between the two LAN2/SYNC ports of both appliances. You do not need to assign them IPs as those are created automatically later. If you do assign them, make sure the LAN2/SYNC interfaces use the same subnet.
  You can use a different SYNC interface other than LAN2. For more information, see sk52500 http://supportcontent.checkpoint.com/solutions?id=sk52500 (you can use the Cluster Wizard in SmartDashboard but you need to make further adjustments to the cluster object before policy installation).

- The Cluster Wizard assumes that the WAN interface is part of the cluster. Make sure the WAN interfaces in each of the gateways are configured with a static IP of a matching subnet.

- When you configure the appliances that are used in the cluster, make sure to set both of the appliances with the same one-time password you used to authenticate and establish trusted communication. Without this, you cannot use the Cluster Wizard in SmartDashboard and you need to create the cluster object in Classic Mode. Trusted communication without authentication is not supported on Check Point Appliance cluster members.

Creating a Cluster for New Gateways

To create a cluster for new gateways:

- Set up and configure the Check Point Appliance gateways.
- Create and configure the cluster object in SmartDashboard that represents the gateways.
**Configuring the Check Point Appliance Gateways**

See your Check Point Appliance *Getting Started Guide* for full instructions to set up and connect the Check Point Appliance.

This is the general workflow:

1. Connect your computer to the Check Point Appliance on its LAN1 interface.
2. Configure your computer to get an IP address automatically.
3. Open your Web browser, and connect to: http://my.firewall

   When you configure two Check Point Appliance gateways from your web browser, connect only one to a power source. Follow the instructions below to configure it and then disconnect it from the power source. Then do the same for the second appliance and reboot it at the end.

   If you do not follow these instructions, you cannot use the http://my.firewall URL correctly and you need to connect with the gateway’s actual IP address. (That IP address is initially 192.168.1.1 on LAN1 before you configure it with the Check Point Appliance).

   After you configure and connect both appliances to a power source, install a policy and renew the dynamic IP of the computer. You can then use http://my.firewall to access the active member of the cluster.

4. Follow the steps to configure the Check Point Appliance with the First Time Configuration Wizard.
5. On the appliance’s local network, configure the cluster SYNC interface on the same subnet as the SYNC interface of the second cluster member (use a cross Ethernet cable for SYNC interface connection).

   When you use the SmartDashboard cluster wizard, the LAN2 interface is the SYNC interface between cluster members. You do not have to configure an IP on LAN2 at any stage of the gateway side configuration. If you do not configure them, LAN2 SYNC interfaces are automatically set to 10.231.149.1 and 10.231.149.2. To set a different SYNC interface (not LAN2), see sk52500 http://supportcontent.checkpoint.com/solutions?id=sk52500.

   Remember the one-time password. You need it to configure the cluster in SmartDashboard. It must be the same on both clusters.

   IP addresses must be configured on both cluster members before you open SmartDashboard and run the Cluster configuration wizard. To configure IPs in interfaces other than WAN and LAN1, do so in each gateway’s WebUI application with the Internet or Local Network pages. Make sure that for each interface that is part of the cluster, you configure an IP in the same subnet as the second cluster member.

**Configuring the Cluster Object in SmartDashboard**

To create a cluster for two new Check Point Appliance gateways:

1. Log in to SmartDashboard with your Security Management credentials.
2. From the Network Objects tree, right click Check Point and select Security Cluster > Small Office Appliance.

   The Check Point Security Gateway Cluster Creation dialog box opens.

3. Select Wizard Mode.

   The wizard opens to General Properties.

4. Enter a name for the Check Point Appliance cluster.

5. Click Next.

   The wizard opens to Cluster Members.
6. In the First Member and Second Member sections, enter a **Member name** and **Member IP address**.
   If you want to check the communication and connectivity, clear the **Define the second cluster member now** check box. This allows you to complete the wizard definitions for the first member only.

7. Enter and confirm the **One-time password** to establish initial trust.
   When trust is established, it is based on security certificates. This password must be identical to the same one-time password defined for both members in their appliances’ First Time Configuration Wizard or WebUI.

8. Click **Next**.
   The wizard opens to Cluster Interface Configuration.
   When you configure the WAN interface, you cannot disable High Availability. (For other configurations, edit the Cluster object later).
   If the WAN interface was not defined, edit the Cluster object in SmartDashboard with the wizard and select a correct main IP for the cluster object. (This IP is used, for example, in VPN as one of the Link selection options).

9. Enter a virtual **IP Address** and **Net Mask** for the cluster. The virtual IP is applied in the next policy installation.

10. Click **Next**.
11. To enable High Availability on the interface, select the **Enable High Availability on <name> interface** checkbox. <name> shows the network interface defined in the Check Point Appliance.
12. When High Availability is selected, enter a virtual **IP Address** and **Net Mask** for the cluster. The virtual IP is applied in the next policy installation.

13. Click **Next**.
14. Repeat steps 12 - 14 for each defined interface.
15. Click **Finish** or select **Edit Cluster in Advanced mode** to further configure the cluster.

**Cluster Interface Configuration**

In the Cluster Interface Configuration window, you define if a network interface on the Check Point Appliance is part of the security gateway cluster. This window shows for each network interface that was configured in the Check Point Appliance. The total number of interfaces configured for the gateway shows in the window title. For example, if 3 interfaces are configured for the gateway, a total of 3 windows require configuration. The first window displays (1 of 3 interfaces). The name of the interface you are currently configuring shows in the Interface column.

Each network interface (on both members) has a unique IP address. If High Availability is enabled on the interface, then the cluster requires an additional unique virtual IP address. This IP address is visible to the network and ensures that failover events are transparent to all hosts in the network.

When High Availability is not enabled, the interface is considered not-monitored private (it is not cluster related).

You can configure High Availability for all network interfaces except for the WAN interface. By default, the WAN interface is always part of the cluster. If you do not want the WAN interface to be part of the cluster, double-click on the Check Point Appliance security gateway cluster object, and select **Topology node > Edit Topology**.
If the WAN interface was not defined, edit the Cluster object in SmartDashboard with the wizard and select a correct main IP for the cluster object. (This IP is used, for example, in VPN as one of the Link selection options).

The breadcrumb image at the top of the window shows you the interface you are currently configuring. You do not configure the LAN2 interface as it is automatically configured by the wizard and is used only for the SYNC interface. Make sure a cable is connected between the two LAN2/SYNC ports of both appliances.

**Note** - SYNC interface is only supported with IPv4 addresses.

The image at the bottom of the page shows if the interface is set for High Availability. When you configure High Availability, the physical IPs of both members meet at a point indicated by the cluster’s virtual IP address.

**To configure more advanced options for interfaces:**

1. Click **Edit Cluster in Advanced mode** at the end of the wizard.
2. Edit the topology of the cluster and make the necessary changes.
   
   **Note** - Cluster in bridge in Active/Standby mode is supported in 1200R and 1400 appliances.

**Converting an Existing Check Point Appliance to a Cluster**

Do these procedures to convert an existing Check Point Appliance to a cluster.

**Note** - The procedures require some downtime.

Terms used:

- **GW** - the existing Check Point Appliance gateway object that has already established trust and has an installed policy.
- **Cluster** - the new Check Point Appliance cluster object that you create.
- **GW_2** - the new cluster member object that joins the existing gateway.

**To configure the new appliance GW_2 with the First Time Configuration Wizard:**

1. Make sure to configure the actual IP addresses and not the virtual IP addresses that are used by the existing gateway **GW**.
2. Clear the **Enable switch on LAN ports** checkbox.
   
   If you do not do this, the default switch configuration is automatically removed during the cluster’s first policy installation, as it is not supported in a cluster configuration.

   **Note** - It is more secure to remove the switch configuration before initial policy installation.
3. Configure the LAN2 port (used for cluster synchronization) with an IP address that is in the same network as the other cluster member. It is recommended to assign a static IP address for the sync interface.
4. Do not fetch the policy from the Security Management Server.

**To create and configure the cluster in SmartDashboard:**

1. Use the wizard to create a new Check Point Appliance cluster.
2. Define the IP address as the IP used by the existing gateway **GW**.
3. Define the first member with **GW_2**’s IP address.

   **Important** - Do not define the second member using the wizard.
4. Establish trusted communication.
5. Define all the IP addresses of the clustered interfaces. Use the existing gateway GW IP address as the virtual IP of the cluster.
6. At the end of the wizard, select the Edit the cluster in Advanced Mode checkbox.
7. In Advanced Mode, enter all the relevant configuration settings from the GW to the cluster object.

To reconfigure the existing Check Point Appliance:
1. In the WebUI, go to the GW and connect to it.
2. Reconfigure the IP addresses of the clustered interfaces with the actual IP addresses that is used by the gateway as a member of the cluster.
   
   Important - Downtime starts.

To configure the cluster in SmartDashboard:
1. Change the main IP and the IPs that appear in the topology table of the GW object.
2. Install policy on Cluster.
   
   Important - Downtime ends. At this point, the cluster contains only one member, GW_2.
3. Go to Cluster Members > Add > Add existing gateway and edit the Cluster object.
4. If GW does not show in the list, press Help and make sure GW does not match any of the categories that prevent it from being added to a cluster.
   
   Note - Use the information on this Help page to determine if there are any configuration settings you want to copy to the new Cluster object.
5. Under the new GW object, click Topology > Get Topology to edit the topology of the Cluster object.
6. Install policy on Cluster.

Viewing Cluster Status in the WebUI

After you complete policy installation on the Check Point Appliance gateway and the gateway works as a cluster member, you can view cluster status in the WebUI application (Device > High Availability).

Creating the Security Policy

Working with Security Zone Objects

A security zone object is a logical object that represents the network behind a specified interface. For example, an InternalZone object represents the internal network IPs behind all of the internal gateway interfaces.

You can use security zone objects to create a generic Security Policy and reduce the amount of rules necessary in the Rule Base. This Security Policy can be applied to numerous Check Point Appliance gateways. Resolution of the security zone is done by the actual association on the Check Point Appliance gateway object in SmartDashboard.
Workflow
1. Associate a security zone object with an interface on the gateway object.
2. Use the security zone object in a rule.
3. Install policy.

To associate a security zone object with an interface on the gateway object:
1. In SmartDashboard, from the Network Objects tree, double-click a Check Point Appliance gateway object.
2. From Topology, select the applicable interface and click Edit. The Interface Properties window opens.
3. Select one of the predefined Security Zone options.
4. If you want to create a new zone, click New, fill in the details and click OK.
5. Click OK. The Check Point Appliance Gateway General Properties is shown.
6. Click OK.

To create a rule with a security zone:
After you associated a security zone object to the applicable interface on the gateway, you can use it in a rule. To create a rule with a security zone, just add the security zone object to the Source or Destination cell.

For example, to create a rule that allows internal users access to any external network, create a rule with these fields:

<table>
<thead>
<tr>
<th>Policy Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>InternalZone</td>
</tr>
<tr>
<td>Destination</td>
<td>ExternalZone</td>
</tr>
<tr>
<td>Action</td>
<td>accept</td>
</tr>
<tr>
<td>Install On</td>
<td>gateway object or SmartLSM profile</td>
</tr>
</tbody>
</table>

1. Open the Firewall > Policy page.
2. Use the Add Rule buttons to position the rule in the Rule Base.
3. Enter a Name for the rule.
4. In the Source field, right-click the + icon, click Network Objects, select InternalZone from the list, and click OK.
5. In the Destination field, right-click the + icon, click Network Objects, select ExternalZone from the list, and click OK.
6. In the Action field, select accept.
7. Right-click the Install On field, select Add > Targets, and select the gateway object or SmartLSM profile.
Installing a Security Policy

Use this procedure to prepare the policy for automatic installation when the gateway connects.

**Note** - If the Check Point Appliance is physically set up and configured, when you successfully complete this step, the policy is pushed to the gateway. For a list of possible statuses, see Viewing the Policy Installation Status (on page 19).

At the end of the Install Policy process, the policy status for a Check Point Appliance that is not yet set up is "waiting for first connection." This implies that trusted communication is not yet established between the Security Management Server and the Check Point Appliance. When the gateway connects it establishes trust and attempts to install the policy automatically.

To install a security policy:

1. Click **Policy > Install** from the menu.
   
   The Install Policy window opens.

2. Select the installation targets - the Check Point Appliance Security Gateways on which to install the policy and the policy components (such as Network Security or QoS).
   
   By default, all gateways that are managed by the Security Management Server are available for selection.

3. In the Installation Mode section, select how the Security Policy should be installed:
   
   - On each selected gateway independently
   - On all selected gateways, if it fails do not install on gateways of the same version

4. Click **OK**.

   The Installation Process window shows the status of the Network Security Policy for the selected target.

   **Important** - If the Check Point Appliance object is defined by the appliance is not set up and it is in the "Waiting for first connection status", you see a message that says "Installation completed successfully". This means that the policy is successfully prepared for installation.

   Continue tracking the status of the Security Policy installation with the Policy Installation and the status bar ("Viewing the Policy Installation Status" on page 19).

Viewing the Policy Installation Status

You can see the installation status of managed gateways with the status bar that shows at the bottom of the SmartDashboard window. The status bar shows how many gateways are in Pending or Failed mode.

- Pending - gateways that are in the waiting for first connection status or are in the pending status (see below for detailed explanations).
- Failed - gateways that have failed to install the policy.

The status bar is updated dynamically each time a gateway tries to install a policy or tries to connect to the Security Management Server. The results of these actions are also shown in SmartDashboard popup notification balloons when such events occur. You can configure these notifications.

To monitor the status of the last policy installed on each gateway, you can use the Policy Installation Status window.
The window has two sections. The top section shows a list of gateways and status details regarding the installed policy. You can use the filter fields to see only policies of interest and hide other details by defining the applicable criteria for each field. After you apply the filtering criteria, only entries that match the selected criteria are shown. If the system logs trusted communication (SIC) attempts from unknown gateways, a yellow status bar opens below the filter fields.

The bottom section shows details of a row you select in the gateway list (errors that occurred, the date the policy was prepared, verification warnings). If there is a yellow status bar, click **Show details** to show the details of unknown gateways that try to connect to the Security Management Server.

These are the different statuses in this window:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Policy status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Succeeded</td>
<td>Policy installation succeeded.</td>
</tr>
<tr>
<td>✔</td>
<td>Succeeded</td>
<td>Policy installation succeeded but there are verification warnings.</td>
</tr>
</tbody>
</table>
| 🔄    | Waiting for first connection | A Check Point Appliance object is configured, but the gateway is not connected to the Security Management Server (initial trust is not established).  
   - If a policy is prepared, it is pulled when the gateway is connected.  
   - If a policy is not prepared, the Policy Type column shows “No Policy Prepared.” When the gateway is first connected, only trust is established. |
| 🔄    | Waiting for first connection | Same as above, with warnings that attempts to establish trust failed or there are verification warnings. |
| 🔄    | Pending           | The policy remains in the pending status until the gateway successfully connects to the Security Management Server and retrieves the policy. This status is shown only if there was at least one successful policy installation.  
   For example, when the Security Management Server has problems connecting to the Gateway (the Gateway is unavailable for receiving communication, as in behind NAT). |
| 🔄    | Pending           | Same as above but there are verification warnings.                           |
| ⚠️    | Warning           | Warning.                                                                    |
| 📸    | Information       | Information.                                                                |
| 🚨    | Failed            | Policy not installed due to a verification error.                            |
| 🚨    | Failed            | Policy installation failed.                                                 |
You can access the Policy Installation Status window in these ways:

- From the menu bar - Click **Policy > Policy Installation Status**.
- From the toolbar - Click the Policy Installation Status icon.
- From the status bar - Click **Failed** or **Pending**. The contents of the Policy Installation Status window are shown filtered according to the link clicked.
- From notification balloons - Click **See Details** in the balloon.

**Setting Server IP Behind a 3rd Party NAT Device**

When you use the *Management First* deployment scenario, the policy is prepared to be fetched by appliances when they are configured.

During each appliance’s first time configuration, the routeable IP address of the Security Management Server is manually configured to create a first connection.

When SIC is established between the appliance and Security Management Server, the policy is fetched for the first time. Then, an automatic mechanism calculates the routeable IP address of the Security Management Server for the periodic policy fetch attempts. However, if the Security Management Server is located behind a 3rd party NAT device, the automatic mechanism fails.

In such cases, you can manually determine the routeable IP address of the Security Management Server, not only for the first connection. You can request that the appliance always attempt a connection with a manually configured IP address. You can configure this from the First Time Configuration Wizard - Security Management Server Connection page (select **Always use this IP address** and enter the IP address) or from the WebUI **Home > Security Management** page.
Large-scale Deployment Installation

In This Section:

- Supported Security Management Versions ........................................................... 22
- Large-scale Deployment Workflow ...................................................................... 22
- Defining a SmartLSM Gateway Profile for a Large-scale Deployment .............. 23
- Defining a SmartLSM Appliance Cluster Profile ................................................... 23
- Deploying with SmartProvisioning ....................................................................... 24
- Installing a Security Policy ................................................................................... 25
- Viewing the Policy Installation Status ................................................................... 25

Supported Security Management Versions

Large-scale deployment is supported in all centrally managed appliances in R77.30.
Make sure your version supports LSM. Currently, LSM is supported for R77.20 and R80.20.

1400 Appliances

For R77.30:
- Manage the 1400 appliances as 1100-series SMB appliances.
- To upgrade firmware with SmartProvisioning and SmartUpdate, use this firmware upgrade package: CP1400AS1100*
  If you do not use the CP1400AS1100, you cannot select the package in the view.

For R80.20:
| Manage the 1400 appliances as 1400 SMB appliances.

Large-scale Deployment Workflow

When you define a SmartLSM profile for a gateway or cluster in SmartDashboard, you can use SmartProvisioning to provision multiple gateways.

Workflow for large-scale deployments:

1. Create the necessary profiles for your deployment groups (gateways or clusters of gateways) in SmartDashboard.
2. Install the Security Policy in SmartDashboard.
3. Create the actual cluster or gateway objects in SmartProvisioning based on the SmartLSM profiles defined in SmartDashboard. For more details, see SmartProvisioning on page 28.
4. Configure the relevant appliances with the First Time Configuration Wizard.
   Or
   Use a USB drive to quickly configure multiple appliances without the First Time Configuration Wizard. For more details, see Deploying from a USB Drive.
5. Manage the appliance settings in SmartProvisioning.
Defining a SmartLSM Gateway Profile for a Large-scale Deployment

SmartLSM lets you manage a large number of Check Point Appliance gateways from one Security Management Server. When you use a SmartLSM profile, you reduce the administrative overhead as you define the gateway properties and policy per profile. The SmartLSM profile is a logical object that contains the firewall and policy components.

Use SmartDashboard to define a single SmartLSM profile for the Check Point Appliance.

To define a single SmartLSM profile Check Point Appliance:

1. Log in to SmartDashboard with your Security Management credentials.
2. Open the Security Policy that you want to enforce on the Check Point Appliance SmartLSM Security Gateways.
3. From the Network Objects tree, right-click Check Point and select SmartLSM Profile > Small Office Appliance Gateway.
   The SmartLSM Security Profile window opens.
4. Define the SmartLSM security profile through the navigation tree in this window.
   To open the online help for each window, click Help.
5. Click OK and then install the policy.
   Note - To activate SmartProvisioning functionality, you must install a security policy on the LSM profile.

Defining a SmartLSM Appliance Cluster Profile

The SmartLSM Appliance Cluster Profile is a logical object like the SmartLSM Appliance Gateway profile. It contains the firewall and policy components but also requires logical topology configuration.

The topology table in the SmartLSM Cluster Profile is a template for all SmartLSM clusters that is created with this profile. The SmartLSM Cluster Profile automatically assigns the configuration settings and security policies to the SmartLSM cluster.

The SmartLSM Cluster Profile and its topology are configured in SmartDashboard. Then the SmartProvisioning SmartConsole GUI is used to connect and manage the appliances by the Security Management Server.

Before you do the procedure:

- Prepare two appliances.
- Configure matching internal interfaces with IP addresses in the same subnet. For example, if you use LAN1 on one of the appliances, you must use LAN1 on the second appliance.
- Prepare the WAN interfaces on the same subnet.
- Select a random IP address from the WAN and the Internal networks addresses pool to use as the Cluster Virtual IP.
To create a SmartLSM Cluster profile:

1. In SmartDashboard, from Network Objects, right-click **Check Point > SmartLSM profile > Small Office Appliance Cluster**.
2. In General Properties, enter a **Name** for the profile (for example, ClusterProfile1).
3. Select the **Cluster Members** tab and click **Add** to add the two cluster members to the profile.
4. Select the **Topology** tab and click **Edit** to insert a template topology.
   
   For each SmartLSM cluster, you must define at least 3 networks:
   
   - **External** (one interface for each Cluster Member and shared virtual IP address)
   - **Internal** (one interface for each Cluster Member and shared virtual IP address)
   - **Internal - Sync** (one interface for each Cluster Member)
   
   The network addresses (for example, 1.1.1.194) for each interface are not the actual addresses for your SmartLSM Cluster environment. Those are used for the template. The actual network addresses are modified in the next configuration step in the SmartProvisioning application.

   **Important**
   
   The host octet for each member’s interface address such as “59” for Member1 - WAN (for example, 1.1.1.59) must be its real host address and cannot be modified. Make sure to configure it correctly.

   The host octet for the Virtual IP addresses can be modified later.

5. For each Virtual IP interface, double-click the text field to enter the interface name, security zone, network type, IP address, and Net Mask.
6. For the Internal and Sync interfaces, select **Network defined by the interface IP and Net Mask**. Set Anti-Spoofing for each interface in the **Anti-Spoofing** tab. Keep the default settings in the Member Network tab.
7. For each cluster member, double-click the Topology text field to enter the interface name, IP address, and Net Mask. For VLANs, make sure the member names use the actual physical interface names on the machines. Note that these are the same names that are shown in the appliance’s WebUI, but replace the colon character “:” with a period character “.”
   
   For example, if the WebUI shows LAN1:10, enter here LAN1.10
8. Click **Save** and install policy on the Cluster Profile.
9. Close SmartDashboard.

**Deploying with SmartProvisioning**

You can use SmartProvisioning to manage Check Point Appliance gateways with the SmartLSM profiles defined in SmartDashboard. Configure these appliances using the First Time Configuration Wizard or a USB drive configuration file before you manage them with SmartProvisioning.

For more information about large-scale deployment using SmartProvisioning, see the **SmartProvisioning Administration Guide**.
Installing a Security Policy

Use this procedure to prepare the policy for automatic installation when the gateway connects.

**Note** - If the Check Point Appliance is physically set up and configured, when you successfully complete this step, the policy is pushed to the gateway. For a list of possible statuses, see Viewing the Policy Installation Status (on page 19). At the end of the Install Policy process, the policy status for a Check Point Appliance that is not yet set up is “waiting for first connection.” This implies that trusted communication is not yet established between the Security Management Server and the Check Point Appliance. When the gateway connects it establishes trust and attempts to install the policy automatically.

To install a security policy:

1. Click **Policy > Install** from the menu.
   The Install Policy window opens.

2. Select the installation targets - the Check Point Appliance Security Gateways on which to install the policy and the policy components (such as Network Security or QoS).
   By default, all gateways that are managed by the Security Management Server are available for selection.

3. In the Installation Mode section, select how the Security Policy should be installed:
   - On each selected gateway independently
   - On all selected gateways, if it fails do not install on gateways of the same version

4. Click **OK**.
   The Installation Process window shows the status of the Network Security Policy for the selected target.

   **Important** - If the Check Point Appliance object is defined by the appliance is not set up and it is in the “Waiting for first connection status”, you see a message that says “Installation completed successfully”. This means that the policy is successfully prepared for installation.

   Continue tracking the status of the Security Policy installation with the Policy Installation and the status bar (“Viewing the Policy Installation Status” on page 19).

Viewing the Policy Installation Status

You can see the installation status of managed gateways with the status bar that shows at the bottom of the SmartDashboard window. The status bar shows how many gateways are in Pending or Failed mode.

- Pending - gateways that are in the waiting for first connection status or are in the pending status (see below for detailed explanations).
- Failed - gateways that have failed to install the policy.

The status bar is updated dynamically each time a gateway tries to install a policy or tries to connect to the Security Management Server. The results of these actions are also shown in SmartDashboard popup notification balloons when such events occur. You can configure these notifications.

To monitor the status of the last policy installed on each gateway, you can use the Policy Installation Status window.
The window has two sections. The top section shows a list of gateways and status details regarding the installed policy. You can use the filter fields to see only policies of interest and hide other details by defining the applicable criteria for each field. After you apply the filtering criteria, only entries that match the selected criteria are shown. If the system logs trusted communication (SIC) attempts from unknown gateways, a yellow status bar opens below the filter fields.

The bottom section shows details of a row you select in the gateway list (errors that occurred, the date the policy was prepared, verification warnings). If there is a yellow status bar, click Show details to show the details of unknown gateways that try to connect to the Security Management Server.

These are the different statuses in this window:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Policy status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>Succeeded</td>
<td>Policy installation succeeded.</td>
</tr>
<tr>
<td>✅⚠️</td>
<td>Succeeded</td>
<td>Policy installation succeeded but there are verification warnings.</td>
</tr>
</tbody>
</table>
| 🔄   | Waiting for first connection| A Check Point Appliance object is configured, but the gateway is not connected to the Security Management Server (initial trust is not established).  
   - If a policy is prepared, it is pulled when the gateway is connected.  
   - If a policy is not prepared, the Policy Type column shows “No Policy Prepared.” When the gateway is first connected, only trust is established. |
| 🔄⚠️ | Waiting for first connection| Same as above, with warnings that attempts to establish trust failed or there are verification warnings. |
| 🔄   | Pending                     | The policy remains in the pending status until the gateway successfully connects to the Security Management Server and retrieves the policy. This status is shown only if there was at least one successful policy installation.  
   - For example, when the Security Management Server has problems connecting to the Gateway (the Gateway is unavailable for receiving communication, as in behind NAT). |
| 🔄⚠️ | Pending                     | Same as above but there are verification warnings.                          |
| ⚠️   | Warning                     | Warning.                                                                    |
| 🔄   | Information                 | Information.                                                                |
| 🔄⚠️ | Failed                      | Policy not installed due to a verification error.                           |
| 🔄⚠️ | Failed                      | Policy installation failed.                                                 |
You can access the Policy Installation Status window in these ways:

- From the menu bar - Click **Policy > Policy Installation Status**.
- From the toolbar - Click the Policy Installation Status icon.
- From the status bar - Click **Failed** or **Pending**. The contents of the Policy Installation Status window are shown filtered according to the link clicked.
- From notification balloons - Click **See Details** in the balloon.
Creating a Gateway

Make sure you define a SmartLSM gateway profile in SmartDashboard before you create a gateway in SmartProvisioning.

To create a new gateway:

1. Open SmartProvisioning.
2. In the Devices page, right-click an empty row in the table and select New SmartLSM > Small Office Appliance Gateway.

   The SmartLSM Security Gateway General Properties page opens.

General Properties

1. Enter a Name for the SmartLSM Security Gateway. It cannot contain spaces or non-alphanumeric characters.
2. Enter an optional Comment that identifies the SmartLSM Security Gateway.
3. Click Next.

More Information

1. In SmartLSM gateway, select the firmware version of the installed Check Point Appliance.
2. In Security Profile, select the relevant SmartLSM gateway profile that the SmartLSM Security Gateway is mapped to.
3. In OS, select the operating system of the gateway. Make sure the selection fits the hardware type.
4. In Enable Provisioning, select this checkbox to enable this gateway to be managed with provisioning configurations. For more information, see Managing Device Settings (on page 32).
5. In No Provisioning Profile, select this option if you want to enable provisioning but are not yet ready to assign a specific profile.
6. In Provisioning Profile, select the provisioning profile to assign to this gateway, from the list of profiles created in SmartProvisioning.
7. Click Next.
Communication Properties

In the Communication Properties page, you define an Activation Key that is used to set up Secure Internal Communication (SIC) Trust between the SmartLSM Security Gateway and the Security Management Server. This is the same key that you should enter in the one-time password field of the Security Management Server Authentication page of the Check Point Appliance First Time Configuration Wizard.

To generate a key automatically:
1. Select Generate Activation Key automatically.
2. Click Generate.
   The Generated Activation Key window opens.
3. Click Accept.
   The two Activation Key fields show the new key in hidden text. You cannot view it in clear text again. If you click Cancel, the generated key is discarded.

To manually define an activation key:
1. Select Activation Key.
2. Enter your own key, a string of any length.
3. In Confirm Activation Key, enter the key again. You cannot copy the text from the first field.
To clear the key, click Clear.

To initialize certification:
The SIC certificate must be shared between the Security Management Server and the SmartLSM Security Gateway. With this SmartLSM wizard, you create the key on the Security Management Server (the SIC certificate and the IKE certificate for the selected gateway are created when you finish this wizard). The certificate is pulled by the gateway when it first connects to the Security Management Server after it is configured with the Check Point Appliance First Time Configuration Wizard.

1. If you know the IP address of the SmartLSM Security Gateway, select This machine currently uses this IP address, and enter the IP address.
2. If you do not know the IP address of the SmartLSM Security Gateway, select I do not know the current IP address.
3. Click Next.

VPN Properties

1. Select how to create a VPN certificate:
   - For a CA certificate from the Internal Check Point CA, select I wish to create a VPN Certificate from the Internal CA.
   - For a CA certificate from a third party (for example, if your organization already has certificates from an external CA for other devices), clear this checkbox and request the certificate from the appropriate CA server.
2. Click Next.
Finish
1. Select **Edit SmartLSM gateway properties after creation** to work with the newly created object.
2. Click **Finish** to complete the SmartLSM Security Gateway creation.

After the SmartLSM Security Gateway object is created:
- Update the Corporate Office Gateway.
- If the VPN option was selected in the VPN Properties page, the Certificate Authority issues a certificate to the appliance. This certificate is installed on the appliance the first time that the SmartLSM Security Gateway connects to the Security Management Server.

To update the Corporate Office Gateway:
1. Select **Update Corporate Office Gateway** from the toolbar.
2. Select the **Corporate Office Gateway** from the list.

It is important to update the Corporate Office Gateway whenever SmartLSM Security Gateways are added, deleted, or modified (such as the generation of a new IKE key, a Push Policy action, or a Push Dynamic Objects action).

Creating a SmartLSM Appliance Cluster

Make sure you have a SmartLSM cluster profile defined in SmartDashboard before you create a Small Office Appliance cluster in SmartProvisioning.

To create a new SmartLSM Security Cluster:
1. Open SmartProvisioning.
2. In the **Devices** page, right-click an empty row in the table, select **New SmartLSM > Small Office Appliance Cluster**.

The SmartLSM Security Gateway General Properties page opens.

**General Properties**
1. Enter a unique **Cluster Name Prefix** (Suffix is optional). The SmartLSM Security Cluster name is: `<prefix>cluster<suffix>`.
2. In **Cluster Main IP Address**, enter the real external virtual IP address for your actual gateway cluster.
3. Click **Next**.

**Cluster Properties**
1. In **Version**, select the firmware version for the Check Point Appliance.
2. In **Security Profile**, select the SmartLSM Cluster Profile that was created in SmartDashboard (in the example ClusterProfile1).
3. In **Enable Provisioning**, select this checkbox to enable this gateway to be managed with provisioning configurations. For more information, see Managing Device Settings (on page 32).
4. In **No Provisioning Profile**, select this option if you want to enable provisioning but are not yet ready to assign a specific profile.
5. In **Provisioning Profile**, select the provisioning profile to assign to this gateway, from the list of profiles created in SmartProvisioning.

6. Click **Next**.

**Cluster Names**

The cluster members’ names are shown with the configured prefix.

Click **Next**.

**More Information**

1. Click **Edit** to override the settings of the template topology on each of the interfaces. For example, select WAN and click **Edit**. The interface window opens.

2. In **IP Address Override**, enter the actual network IP address to override the template Network address.

3. Click **OK** and do the above steps again for all the interfaces.

4. Click **Next**.

**Communication Properties**

1. Select a member and click **Initialize**. Enter the trusted communication (SIC) details and click **OK**.

2. Do this step again for the second member.

3. Click **Next**.

**VPN Properties**

1. Select how to create a VPN certificate:
   - For a CA certificate from the Internal Check Point CA, select **I wish to create a VPN Certificate from the Internal CA**.
   - For a CA certificate from a third party (for example, if your organization already has certificates from an external CA for other devices), clear this checkbox and request the certificate from the appropriate CA server.

2. Click **Next**.

**Finish**

1. Click **Finish**. After the wizard finishes, wait until the SIC initialization completes. It can take a few minutes. When it completes, you see the cluster object and its two members.

   When you double-click the cluster object you can see that the topology is configured with the actual addresses.

2. On each Check Point Appliance, open the WebUI **Home > Security Management** page and click **Fetch Policy** to manually pull the policy immediately. Alternatively, the appliance connects to the Security Management Server at predefined periodic intervals to pull the policy.
Defining SmartLSM Gateways Using LSM CLI

This is a sample SmartLSM CLI script that you can use to create a new gateway object and associate it with a SmartLSM profile. Optionally, you can also set a SIC password and initiate a SIC connection.

```
LSMcli <server> <user> <password> AddROBO CPSG80 <RoboName> <Profile> [-O=<ActivationKey> [-I=<IP>]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;server&gt;</code></td>
<td>The Security Management Server on which to create the gateway object</td>
</tr>
<tr>
<td><code>&lt;user&gt;</code></td>
<td>The username of the Security Management Server administrator</td>
</tr>
<tr>
<td><code>&lt;password&gt;</code></td>
<td>The password of the Security Management Server administrator</td>
</tr>
<tr>
<td><code>&lt;RoboName&gt;</code></td>
<td>The name for the new gateway object</td>
</tr>
<tr>
<td><code>&lt;Profile&gt;</code></td>
<td>Then name of the SmartLSM profile to associate with the gateway</td>
</tr>
<tr>
<td><code>&lt;ActivationKey&gt;</code></td>
<td>The SIC password</td>
</tr>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>The IP to use to initiate a SIC connection</td>
</tr>
</tbody>
</table>

Managing Device Settings

You can manage device settings directly on individual gateways or you can use a SmartProvisioning Profile to manage multiple gateways. For more information about provisioning profiles and creating them, see the SmartProvisioning Administration Guide.

These device settings are unique to the Check Point Appliance. They can be defined directly on the device or through the profile. Their tabs are:

- Firmware
- RADIUS
- Hotspot
- Configuration Script

Configuring Firmware

This section explains how to configure firmware installation settings for the provisioning profile for the Check Point Appliance. When you configure firmware settings on a Provisioning Profile, you give the configuration for all appliances that reference this profile.

Firmware configuration lets you replace the firmware on the Security Gateway. The Security Gateway version must match its SmartLSM profile’s version as defined in SmartDashboard for correct policy behavior. As a result, after firmware upgrade, the SmartLSM profile is replaced with the default SmartLSM security profile.
In some instances, it may be necessary to define exceptions for the default SmartLSM security profile. For example, if you do not want all gateways to use the specified default SmartLSM profile after installation, you can customize different security profiles to replace known security profiles.

Let’s say you have a scenario with these details:

- The default SmartLSM profile after installation is configured to use a SmartLSM profile called "NewLSM".
- After firmware installation, you want the "NewLSM" profile installed on all Security Gateways except for gateways that currently use the "GroupA_LSM" profile.
- You want to replace the "GroupA_LSM" profile with a profile called "GroupA_NewLSM".

In this scenario, you add an exception that replaces the "GroupA_LSM" profile with the "GroupA_NewLSM" profile.

You can install the firmware with one of these options:

- **Immediately** - Installs the firmware in two steps:
  - Downloads the firmware immediately during the next synchronization with a Security Gateway that references this profile.
  - Installs the firmware when the download completes.

- **According to time ranges** - You can define download and installation time ranges for the firmware image. The download and installation time can be limited to a specified list of time ranges in the week. They start at the nearest time range after firmware settings were applied. You can also define that the download takes place immediately as above and only installation is based on specified time ranges. For example, if the firmware installation settings were applied on Sunday and there are two time ranges:
  - One range is set to Friday 00:00 to Saturday 00:00
  - One range is set to Wednesday 23:00 to Thursday 06:00

To configure firmware installation settings on a Provisioning Profile:

1. Open the Security Gateway Profile window, and select the Firmware tab.
2. Select Manage firmware centrally from this application.
3. Click Advanced.
   The Profile Settings window is displayed.
4. Select an override profile setting:
   - Allowed
   - Denied
   - Mandatory
   For more information about override profile settings, see Configuring Profile Settings ("Configuring a Provisioning Profile" on page 36).
5. In Firmware image, click Select to select a firmware image that was uploaded through SmartUpdate.
6. In Default SmartLSM Profile after installation, select the new SmartLSM profile of the Security Gateway (the Security Gateway version must match its SmartLSM profile’s version as defined in SmartDashboard for correct policy behavior). The Security Gateway replaces its
SmartLSM profile after successful firmware installation and only if the new firmware version is different from the version you have now.

7. If necessary, click **Exceptions** to select a new SmartLSM profile for Security Gateways with a specified SmartLSM profile.
   - **Add/Edit** - Click **Add** or **Edit** to open the **Exceptions** window to define/change an exception for a SmartLSM profile replacement. SmartLSM profiles is not shown unless they are from a version higher than R71.
     - **Current SmartLSM Profile** - Select a SmartLSM profile from the list. A SmartLSM profile is shown only if the version is not R71 and not the selected firmware version. Make sure you installed a policy for the SmartLSM profile in SmartDashboard.
     - **SmartLSM Profile after installation** - Select a SmartLSM profile that replaces the SmartLSM profile after the firmware image installation. A SmartLSM profile is shown only if the version is the same as the selected firmware version. Make sure you installed a policy for the SmartLSM profile in SmartDashboard.
   - **Remove** - Click to remove a SmartLSM profile exception setting.

8. Select an option to install the firmware:
   a) **Immediately** - Downloads the firmware immediately but installs it in the next synchronization with a Security Gateway that references this profile.
   b) **According to these time ranges** - Select to use the Security Gateway time or local time.
      - **Add/Edit** - Click Add or Edit to open the Time Range window to define/change the weekdays and times for downloading and installing the firmware image. Select the days and times and click **OK**.
      - **Remove** - Select a range from the list and click **Remove** to delete a time range.
      - **Download image immediately** - Click this option to download the firmware image immediately but install the image during one of the set time ranges.

9. Click **Show profile settings** - To see the settings of the Provisioning Profile that this gateway references.

10. Click **OK**.

### Configuring RADIUS

You can configure the RADIUS server [Remote Authentication Dial In User Service] that provides authentication, authorization, and accounting for the Check Point Appliance gateways. When you configure RADIUS in the Provisioning Profile, you can configure it for all gateways that reference this profile. The RADIUS server must already be defined as a SmartDashboard object.

You can configure your appliance to contact more than one RADIUS server. If the first server in the list is unreachable, the next RADIUS server in the list is contacted for authentication.

**To configure RADIUS settings on a Provisioning Profile:**

1. Open the **Security Gateway Profile** window, and select the **RADIUS** tab.
2. Select **Manage RADIUS settings centrally from this application**.
3. Click **Advanced**.
   - The Profile Settings window opens.
4. Select an override profile setting:
   - Allowed
   - Denied
   - Mandatory
   
   For more information about override profile settings, see Configuring Profile Settings
   ("Configuring a Provisioning Profile" on page 36).

5. Select **RADIUS is activated on device** to enable RADIUS on the Check Point Appliance.

6. Click **Add** to add RADIUS servers that were defined in SmartDashboard, select a RADIUS
   server from the list and click **OK**.

7. To remove a server, select a server in the list and click **Remove**.

8. Use **Up** and **Down** to set the priority to contact RADIUS servers.

9. Click **Allow administrators from specific RADIUS groups only (comma separated)** to allow
   authentication from specified groups as defined on the RADIUS server. Only administrators
   that belong to those groups can get access.

10. Click **OK**.

### Configuring Hotspot

To configure hotspot settings on a Provisioning Profile:

1. Open the **Security Gateway Profile** window, and select the **Hotspot** tab.

2. Select **Manage Hotspot settings centrally from this application**.

3. Click **Advanced**. The Profile Settings window is displayed.

4. Select one of these override profile settings:
   - Allowed
   - Denied
   - Mandatory
   
   For more information about override profile settings, see Configuring Profile Settings
   ("Configuring a Provisioning Profile" on page 36).

5. Select **Hotspot is activated on device** to activate the hotspot.

6. Configure the fields:
   - **Portal Title** - Keep the default or enter a different title.
   - **Portal message** - Keep the default or enter a different message.
   - **Terms of use** - Select this checkbox to add an "I agree with the following terms and
     conditions" checkbox on the Hotspot portal page. Enter the terms and conditions text in the
     text box. When users click the "terms and conditions" link, the entered text is shown.
   - **Require Authentication** - To require user authentication, select the checkbox.
   - **Allow users from specific group** - Select to allow access to a specific user group and not
     all users. Enter the group’s name in the text box.

7. Click **Apply**.
Configuring a Configuration Script

To configure a configuration script on a Provisioning Profile:
1. Open the Security Gateway Profile window, and select the Configuration Script tab.
2. Select Manage Configuration Script centrally from this application.
3. Click Advanced.
   The Profile Settings window opens.
4. Select one of these override profile settings ("Configuring a Provisioning Profile" on page 36):
   • Allowed
   • Denied
   • Mandatory
5. In Configuration Script, enter a script to run on the Small Office Appliance gateway.
6. Click Apply.

Configuring a Provisioning Profile

For each set of configurations managed with a Provisioning Profile, you can decide which settings have preference: local (not provisioned) or central (from SmartProvisioning individual management or from Provisioning Profile).

To configure the settings of a Provisioning Profile:
1. In the Profiles List, right-click a profile and select Edit Provisioning Profile.
2. In the Profile window, click any category tab [other than General].
3. Select management settings for gateways that reference the profile:
   • Manage settings locally on the device: Each gateway that references this profile has its own settings, configured locally (not on SmartProvisioning). These settings cannot be overwritten by changes to the Provisioning Profile or to the SmartProvisioning gateway object. If you select this option, the Gateway window shows: settings are defined to be managed locally on the device.
   • Manage settings centrally from this application: Each gateway that references this profile gets its configuration for this setting from the Provisioning Profile or from the SmartProvisioning gateway object.
4. If you selected to manage settings centrally, click Advanced.
   The Profile Settings window opens.
5. Select an option for Overriding profile settings on device level is:
   • Allowed - You can override the profile settings with device-local settings, or with changes to these settings in the SmartProvisioning device window. You can also leave the profile settings as they are.
   • Denied - Each gateway takes the settings from the profile, with no option to override the profile settings.
   • Mandatory - Each gateway is managed without a Provisioning Profile.
6. Click OK.
This table maps the profile settings selections to the Gateway window options:

<table>
<thead>
<tr>
<th>Profile managed</th>
<th>Profile Override</th>
<th>Gateway Window Display and options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locally</td>
<td>Not relevant</td>
<td>Settings are defined to be managed locally on the device. To change this, refer to the attached Provisioning Profile <code>profile_name</code>. (controls are unavailable)</td>
</tr>
<tr>
<td>Centrally</td>
<td>Override denied</td>
<td>Overriding profile settings is denied. To change this, refer to the attached Provisioning Profile <code>profile_name</code> (controls are Read-Only, configured by profile)</td>
</tr>
</tbody>
</table>
| Centrally       | Override allowed | Select override method:  
- **Manage settings locally on the device**: Local management. Override provisioning configurations with local settings.  
- **Use profile settings**: Enforce profile settings on this gateway.  
- **Use the following settings**: Manage these settings on this gateway individually with the values given here.  
| Centrally       | Override mandatory | Overriding profile settings is mandatory: configure settings here. To change this, refer to Provisioning Profile `profile_name` (Each gateway is configured separately)  
- **Manage settings locally on the device**: Manage these settings on this gateway locally.  
- **Use the following settings**: Manage these settings on this gateway individually with the values given here. |

For example, if you set Hosts configuration to **Central** and **Allowed**: The **Hosts** tab on the gateway enables you to manage the Host List of a gateway if you:

- Define the Host List locally on the device (even if it has an assigned Provisioning Profile)  
- Provision gateways with the Host List of the Provisioning Profile  
- Define a New Host List (in the Gateway window) that overrides the Provisioning Profile on this gateway

**Warning** - If you select **Use the following settings** and do not enter values for a specified topic, the current settings on the device are deleted.
First Time Deployment Options

In This Section:

Zero Touch Cloud Service ........................................................................................................... 38
Deploying from a USB Drive or SD Card ....................................................................................... 40

There are different options for first time deployment of your Small and Medium Business (SMB) gateways:

- First Time Configuration Wizard - For more information, see the Getting Started Guide for your appliance model.
- Zero Touch Cloud Service
- USB Drive
- SD Card

Zero Touch Cloud Service

The Zero Touch Cloud Service lets you easily manage the initial deployment of your gateways in the Zero Touch portal https://zerotouch.checkpoint.com.

Note - You cannot use Zero Touch if you connect to the internet through a proxy server.

Zero Touch enables a gateway to automatically fetch settings from the cloud when it is connected to the internet for the first time.

Note - The appliance is fully configured after you complete the First Time Configuration Wizard (click Finish on the final screen or click Quit on an earlier screen after you enter a username and password). To use the Zero Touch Cloud Service after this point, you must first restore the factory defaults.

If the gateway connects to the internet using DHCP, the gateway fetches the Zero Touch settings without any additional action. If no DHCP service is available, you must run the First Time Configuration Wizard, configure the Internet Connection settings, and then fetch the settings from the Zero Touch server.
To connect to the Zero Touch server from the First Time Configuration Wizard:

1. In the Welcome page of the First Time Configuration Wizard, click Fetch Settings from the cloud.

2. In the window that opens, click Yes to confirm that you want to proceed.

3. The Internet connection page of First Time Configuration Wizard opens. Configure your Internet connection and click Connect.

4. The settings are automatically downloaded and installed.

5. A new window opens and shows the installation status. It may take several minutes until the installation is complete.

Note - If a collision is detected between an internal network (LAN) and an IP returned via DHCP (WAN), the conflicting LAN address is changed automatically. If a colliding LAN IP address is changed, a message appears in the system logs.

When you reconnect to the WebUI or click Refresh, the browser opens to show the status of the installation process.

After the gateway downloads and successfully applies the settings, it does not connect to the Zero Touch server again.

Deploying from a USB Drive or SD Card

In This Section:

Sample Configuration File ................................................................................... 40
Preparing the Configuration Files ........................................................................ 41
Deploying the Configuration File - Initial Configuration ........................................ 41
Deploying the Configuration File - Existing Configuration .............................. 41
Viewing Configuration Logs ................................................................................. 42
Troubleshooting Configuration Files .................................................................... 42
Using the set property Command ...................................................................... 44

You can deploy the Check Point Appliance configuration files from a USB drive or SD card and quickly configure many appliances without using the First Time Configuration Wizard. The configuration file lets you configure more settings and parameters than are available in the First Time Configuration Wizard.

You can deploy configuration files in these conditions:

- An appliance with default settings is not configured at all.
- An appliance that already has an existing configuration.

The Check Point Appliance starts, automatically mounts the USB drive or SD card, and searches the root directory for a configuration file.

Note - The USB drive must be formatted in FAT32.

Sample Configuration File

This is a sample Check Point Appliance configuration file for USB deployment.

```plaintext
set time-zone GMT+01:00(Amsterdam/Berlin/Bern/Rome/Stockholm/Vienna)
set ntp server primary 10.1.1.10
set ntp server secondary

set user admin type admin password aaaa
set interface WAN ipv4-address 10.1.1.134 subnet-mask 255.255.255.192 default-gw 10.1.1.129

delete interface LAN1_Switch

set dhcp server interface LAN1 disable
set interface LAN1 ipv4-address 10.4.6.3 subnet-mask 255.255.255.0
add interface LAN1 vlan 2
set dhcp server interface LAN1:2 disable
set interface LAN1:2 ipv4-address 10.4.3.3 subnet-mask 255.255.255.0

set dhcp server interface LAN2 disable
set interface LAN2 ipv4-address 192.168.254.254 subnet-mask 255.255.255.248
set interface LAN2 state on

set admin-access interfaces WAN access allow

set hostname DEMOgw01
```
Preparing the Configuration Files

The Check Point Appliance Massive Deployment configuration files are composed of CLiSh commands. These are the file names that can be used:

- `autoconf.clish`
- `autoconf.XX-XX-XX-XX-XX.clish`

You can create multiple configuration files for different Check Point Appliance gateways. Name each file based on the MAC address of each appliance. The Check Point Appliance first searches for a configuration file with the same MAC address. If there is no file that matches the MAC address of the appliance, the `autoconf.clish` configuration file is loaded.

Deploying the Configuration File - Initial Configuration

This section describes how to deploy a configuration file on a USB drive to the Check Point Appliance. You must configure and format the file correctly before you deploy it. You can insert the USB drive in the front or rear USB port. Make sure the USB drive is formatted in FAT32.

You can deploy the configuration file to the Check Point Appliance when the appliance is off or when it is powered on.

**Important** - Do not remove the USB drive or insert a second USB drive while the configuration script runs. This may cause a configuration error.

To deploy the configuration file from a USB drive for the initial configuration:

1. Insert the USB drive into a Check Point Appliance.
   - Check Point Appliance is OFF - Turn on the appliance. The Power LED comes on and is green.
   - Check Point Appliance is ON - The appliance automatically detects the USB drive. The USB LED comes on and is a constant orange.
2. The Check Point Appliance locates the USB configuration file and begins to run the script. The USB LED blinks green while the script runs.
3. The configuration script finishes and the Check Point Appliance USB LED is a constant green.
4. Remove the USB drive from the Check Point Appliance.

**Note** - The USB LED is red when there is a problem running the configuration script. Turn off the Check Point Appliance and confirm that the configuration files are formatted correctly ("Preparing the Configuration Files" on page 41).

For more information about errors with configuration files, see Troubleshooting Configuration Files (on page 42).

Deploying the Configuration File - Existing Configuration

To edit or upgrade the existing configuration of a Check Point Appliance, deploy a configuration file. Use the `set property` command to set the appliance to use a configuration file on a USB drive. The USB drive can be inserted in the front or the rear USB port.

You can deploy the configuration file to the Check Point Appliance either when the appliance is off or when it is powered on.
**Important** - Do not remove the USB drive or insert a second USB drive while the Check Point Appliance configuration script runs. This may cause a configuration error.

To deploy the configuration file from a USB drive to a configured appliance:

1. From the CLI, enter the command: `set property USB_auto_configuration once`
   The appliance is set to use a configuration script from a USB drive.
2. Insert the USB drive in the appliance (the appliance automatically detects the USB drive).
   The USB LED comes on and is a constant orange.
3. The appliance locates the USB configuration file and begins to run the script. The USB LED blinks green while the script runs.
4. The configuration script finishes.
   The USB LED is a constant green and the screen displays: **System Started**.
5. Remove the USB drive from the appliance.

**Note** - The USB LED is red when there is a problem running the configuration script. Turn off the appliance and confirm that the configuration files are formatted correctly ["Preparing the Configuration Files" on page 41].

For more information about errors with configuration files, see Troubleshooting Configuration Files [on page 42].

**Viewing Configuration Logs**

After the Check Point Appliance is successfully configured from a USB drive, a log is created.

- The log file is called `autonconf.<MAC>.<timestamp>.<log>`
- The log file is created in the USB root directory and in `/tmp` on the appliance.

**Troubleshooting Configuration Files**

This section discusses the scenario where the configuration file fails and the Check Point Appliance is not fully configured.

**Configuration File Error**

If there is an error and the configuration file fails, the appliance is not fully configured and is no longer in the initial default condition. The commands in the configuration file that show before the error are applied to the appliance. You can examine the configuration log to find where the error occurred.

When the appliance is not fully configured, the First Time Configuration Wizard shows in the Web UI. However, not all of the settings from the failed configuration file show in the First Time Configuration Wizard.

**Best Practice** - Check Point recommends that you do not use the First Time Configuration Wizard to configure an appliance when the configuration file fails. Restore the default settings to a partially configured appliance before you use the First Time Configuration Wizard to ensure that the appliance is configured correctly.
Suggested Workflow - Configuration File Error

This section contains a suggested workflow that explains what to do if there is an error with the configuration file on a USB drive. Use the set property USB_auto_configuration ("Using the set property Command" on page 44) command when you run a configuration file script on a configured appliance.

1. The USB drive with the configuration file is inserted into a USB port on the Check Point Appliance.
2. The USB LED on the front panel blinks red. There is a problem with the configuration file script.

Sample console output displaying an error
Booting Check Point RD-6281-A User Space...
INIT: Entering runlevel: 3
........sd 2:0:0:0: [sda] Assuming drive cache: write through
sd 2:0:0:0: [sda] Assuming drive cache: write through
.........................................................
System Started...
Start running autoconfiguration CLI script from USB2 ... Error.
autoconf.00-1C-7F-21-07-94.2011-07-21.1248.log was copied to USB2

3. The log file is created and contains the configuration details.
   • The log file is called autonconf.<MAC>.<timestamp>.<log>
   • The log file is created in the USB root directory and in /tmp on the appliance.

4. Analyze the log file to find the problem.

If you cannot repair the configuration file:
1. Remove the USB drive.
2. Run the CLI command: restore default-settings.
3. Connect to the Web UI and use the First Time Configuration Wizard to configure the appliance.

If you understand the error and know how to repair the configuration file:
1. Remove the USB drive.
2. Run the CLI command: restore default-settings.
3. Insert the USB drive and run the repaired configuration script again.

Sample Configuration Log with Error

This is a sample configuration log file for a configuration script that fails.

```
set hostname Demo1
set hostname: Setting hostname to 'Demo1'
OK

set interface WAN internet primary ipv4-address 66.66.66.11
Error: missing argument 'subnet-mask' for a new connection
Autoconfiguration CLI script failed, clish return code = 1
```
Using the set property Command

The `set property` CLI command controls how the Check Point Appliance runs configuration scripts from a USB drive. These commands do not change how the First Time Configuration Wizard in the Web UI configures the appliance.

- `set propert USB_auto_configuration off` - The appliance does not run configuration scripts from a USB drive.
- `set propert USB_auto_configuration once` - The appliance only runs the next configuration script from a USB drive.
- `set propert USB_auto_configuration any` - The appliance always runs configuration scripts from a USB drive.
Appliance Configuration

In This Section:

- Introduction to the WebUI Application ......................................................... 45
- The Home Tab ................................................................................................. 46
- Managing the Device ....................................................................................... 56
- Managing Users and Objects ........................................................................... 96
- Logs and Monitoring ......................................................................................... 110

This chapter contains instructions for special Check Point Appliance features.

Introduction to the WebUI Application

The Check Point Appliance uses a web application to configure the appliance.

After you use the First Time Configuration Wizard [see the Check Point Appliance Getting Started Guide], when you connect to the appliance with a browser (with the appliance’s IP or, if the appliance is used as a DNS proxy or DHCP server, to “my.firewall”), it redirects the web page to a secure https site and asks for administrator credentials. When you log in, you can select the Save user name checkbox to save the administrator’s user name. The name is saved until you clear the browser’s cookies.

When you log in correctly, the WebUI opens to Home > System. The left pane lets you navigate between the different pages of each of these tabs:

- Home
- Device
- Access Policy
- Threat Prevention
- VPN
- Users & Objects
- Logs & Monitoring

To log in to the WebUI in a different language:

In the browser page that shows the Login window, select the language link at the bottom of the page.

The log in page changes immediately to the selected language. The next login from the same computer is in the selected language (saved in a browser cookie). The language is kept until you clear the browser’s cookies.

Note - If the locale of a user matches a localized WebUI, the Login window automatically loads in the specified language. Only English is supported as the input language.
The Home Tab

Viewing System Information

The Home > System page shows an overview of the Check Point Appliance.

The Check Point Appliance requires only minimal user input of basic configuration elements, such as IP addresses, routing information, and blade configuration. The initial configuration of the Check Point Appliance can be done through a First Time Configuration Wizard. When initial configuration is completed, every entry that uses http://my.firewall shows the WebUI Home > System page.

- **System Information** - Shows the appliance model, installed software version, name, MAC address, system date and time (with the GMT setting), and system uptime.

- **Network** - Shows Internet information and (where applicable) the wireless network status. Click the links to configure these options.


- **Network Activity** - Shows live data graphs of packet rate and throughput.

Controlling and Monitoring Software Blades

The Home > Security Dashboard page shows you the active blades and lets you quickly navigate to the blade configuration page.

It also gives you:

- Access to the basic settings of the blades with the Settings button (cogwheel icon) and lets you activate the blades.

- Access to statistics for each blade (graph icon)

- Alerts you if there are blades that are missing licenses, service blades which are not up-to-date, and active blades which require additional configuration (for example, site-to-site VPN where the user did not configure any sites). When applicable, there is a triangle in the upper right hand corner of the specified blade.

The software blades are shown in these groups on this page based on where they are configured in the WebUI:

- **Access Policy** - Contains the Firewall, Applications & URL Filtering, User Awareness, and QoS blades.

- **Threat Prevention** - Contains the Intrusion Prevention (IPS), Anti-Virus, Anti-Bot, Threat Emulation, and Anti-Spam blades.

- **VPN** - Contains the Remote Access and Site to Site VPN blades. It also contains certificate options.

You can click the tab name link or software blade link to access the tab for further configuration.

To turn a software blade on or off:

Slide the lever of the specified blade to the necessary **ON** or **OFF** position. When you turn off the Firewall blade, click **Yes** in the confirmation message.
**Note** - Software blades that are managed by Cloud Services show a lock icon. You cannot toggle between on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

**To see or edit setting information:**
1. Click the cogwheel icon next to the On/Off lever.
   The blade settings window opens.
2. View the details or select options to change current settings.
3. Click **Apply**.

**To view statistics:**
1. Click the bar graph icon.
   The blade statistics window opens.
2. If the blade is turned on:
   a) View the graph and details.
   b) To go to other blade statistics, click the arrows in the header.
3. If the blade is turned off:
   a) Click **View demo** to see an example of the statistics shown.
   b) Click the X icon to close the demo.

**To view an alert:**
1. Hover over the alert triangle.
2. Click the applicable link.

**Setting the Management Mode**

The **Home > Security Management** page shows information for the management mode of the Check Point Appliance. You can also test Internet Connectivity from this page.

**To set the management type:**
Select one of the options:
- **Locally** - To manage the Check Point Appliance using the local web application (WebUI). Click **Apply** and then **Yes** when asked to confirm.
- **Centrally** - To manage the Check Point Appliance using the Security Management Server.

When centrally managed, it shows the trust status between the Check Point Appliance and the Security Management Server. When a policy is prepared in SmartDashboard, you can fetch the policy from this window.
Security Management Server

In this section you can view the status of the management connection, last policy installation, adjust trust settings, and initialize a connection.

1. In the Security Management Server section, click **Settings** to adjust trust settings or **Setup** to initialize a connection. The Welcome to the Security Management Server Configuration Wizard shows.

2. Click **Next**. In the One Time Password (SIC) page, select an option for authenticating trusted communication:
   - Initiate trusted communication securely by using a one-time password - The one-time password is used to authenticate communication between the Check Point Appliance and the Security Management Server in a secure manner. Enter a one-time password and confirm it. This password is only used to establish the initial trust. When established, trust is based on security certificates.

   **Important** - This password must be identical to the Secure Communication authentication one-time password configured for the Check Point Appliance object in the SmartDashboard of the Security Management Server.

   - Initiate trusted communication without authentication (not secure) - Select this option only if you are sure that there is no risk of imposture (for example, when in a lab setting).

3. Click **Next**. In the Security Management Server Connection page, select a connection method:
   - To connect to the Security Management Server now, select **Connect to the Security Management Server now**, enter the Security Management Server IP or name and click **Connect**. When you successfully connect to the Security Management Server, the security policy is automatically fetched and installed.

   If the Security Management Server is deployed behind a 3rd party NAT device, select **Always use this IP address** and manually enter the IP address the appliance used to reach the Security Management Server. This IP address overrides, from this point on, the automatic calculating mechanism that determines the routeable IP address of the Security Management Server for each appliance.

   If trust was established but the gateway could not fetch the policy, you can investigate the issue with the Security Management Server administrator. When the issue is resolved, click the **Fetch Policy** button that shows instead of the **Connect** button.

   - To connect to the Security Management Server later, select **Connect to the Security Management Server later**.

4. Click **Finish**.

To reinitialize trusted communication with the Security Management Server:

1. In the Security Management Server section, click **Advanced** to reinitialize trusted communication.

2. Click **Reinitialize Trusted Communication**.

   A Warning message shows.

3. Click **Yes**.

   **Note** - You need to coordinate this operation with the Security Management Server administrator, as reinitialization is necessary on both sides.
Security Policy
To obtain the security policy from the Security Management Server, click **Fetch Policy**. This option is available only if trust is established with the Security Management Server.

Internet
To test connectivity, click **Test Connection Status**. A status message shows the results of the test. You can click **Settings** to configure Internet connections.

Managing Licenses
The **Home > License** page shows the license state for the software blades. From this page, the appliance can connect to the Check Point User Center with its credentials to pull the license information and activate the appliance.

In most cases, you must first register the appliance in your Check Point User Center account or create one if you don’t already have one. A User Center account is necessary to receive support and updates.

If you have Internet connectivity configured:
1. Click the **Activate License** link on this page to be directed to the registration form in the User Center.
2. If registration information is not successfully retrieved, browse to: https://smbregistration.checkpoint.com
3. Complete the applicable fields in the User Center registration.
   - Appliance MAC address
   - Appliance registration key
   - Select **Hardware Platform**
   - Select **Hardware Model**
4. Return to this page and click **Activate License**.
   You are notified that you successfully activated the appliance. After initial activation, the Activate License button shows **Reactivate**. If changes are made to your license, click Reactivate to get the updated license information.

If you work offline while configuring the appliance:
1. Browse to https://usercenter.checkpoint.com and fill out the requested information. You must enter the appliance’s credentials, MAC address and registration key, that can be found on the **Home > License** page.
2. After you complete the registration wizard, you are prompted to download the activation file. Download it to a local location. This is needed for the next step.
3. In the **Home > License** page, click **Offline**.
   The Import Activation File window opens.
4. **Browse** to the activation file you downloaded and click **Import**. The activation process starts.

If there is a proxy between your appliance and the Internet, you must configure the proxy details before you can activate your license.
To configure the proxy details:

1. Click **Set proxy**.
2. Select **Use proxy server** and enter the proxy server **Address** and **Port**.
3. Click **Apply**.
4. Click **Activate License**.
5. Click **Activate License**.

**Viewing the Site Map**

The **Home > Site Map** page shows a site map of the WebUI. It shows all of the tabs and the pages they contain.

Click the link to any page directly from the Site Map page.

**Managing Active Devices**

The **Active Devices** page shows a list of the devices identified in internal networks. The information includes:

- Object name
- MAC Address
- IP addresses
  
  **Note** - 1200R and 1400 appliances support both IPv4 and IPv6 addresses. If a host has both IPv4 and IPv6 addresses, there will be a single entry in the table.
- Device/User Name - Shows a device/user name if the information is available to the Check Point Appliance through DHCP or user awareness.
- Services - Shows incoming and outgoing services. Incoming services usually indicate servers.
- Zone - Shows if the appliance is connected physically or through a wireless connection.
- Traffic - Shows upload and download packet rates for all IP addresses when traffic monitoring is active. **Note** - Traffic monitoring does not differentiate between IPv4 and IPv6 addresses.

Manage the display:

- **Save as** - Save a selected device as a network object or server.
  
  When you select this option, the New Network Object ["Managing Network Objects" on page 106] window or New Server Wizard opens. Enter the information in the fields and click **Apply**. Use these objects to reserve IP addresses to MAC addresses in the DHCP server and also add this object name as a host in the local DNS service. Network objects and server objects can be used in the security configurations, for example in the Access Policy and IPS exceptions.
  
  A server object also allows you to configure access and NAT if applicable as part of the object. If access and/or NAT are configured, automatic access rules are created in the Access Policy Rule Base.
- **Filter** - Filter the list by servers, active devices, or known devices.
- **Details** - Select a row in the list and click **Details** to show additional properties of the device.
- **Refresh** - Refresh the information in the list.
• **Start/Stop Traffic Monitor** - Gather upload and download packet rates for active devices. The information is shown in the added Traffic column in the table.

  This operation may affect performance.

  To stop, click **Stop Traffic Monitoring**.

The display shows the devices connected to the gateway through a Hotspot. You can revoke the Hotspot access for one or more devices. This disconnects the device from the gateway and requires the device to log in again through the Hotspot.

**To revoke the Hotspot access:**

1. Click the record for the relevant device.
2. Click **Revoke Hotspot Access**.

   The access for that device is revoked. You must log in again through the Hotspot to reconnect the device to the gateway.

**Note** - If there is no IPv6 activity in a dual stack host, the Active devices do not show the IPv6 address.

**Note** - This page is available from the **Home** and **Logs & Monitoring** tabs.

---

### Viewing Monitoring Data

The **Monitoring** page shows network, security, and troubleshooting information. When you enter this page, the latest data shows. You can click **Refresh** to update information. To see a sample monitoring report, click **Demo**. To close the sample reports, click **Back**.

The number of current connections in the system is shown for **VPN Tunnels**, **Active Devices**, and **Connections**. You can click the links to open the corresponding WebUI pages.

The Monitoring page is divided into these sections:

- **Network**
- **Security**
- **Troubleshooting**

To expand or collapse the sections, click the arrow icon in the section's title bar.

#### Network

By default, network statistics are shown for the last hour. You can also see statistics for the last day. Select the applicable option **Last hour** or **Last day** from the Network section’s title bar.

The data is automatically refreshed for the time period:

- **Last hour** - At one minute intervals. For example, if you generate a report at 10:15:45 AM, the report represents data from 9:15 to 10:15 AM.
- **Last day** - At hourly intervals. For example, if you generate a report at 10:15 AM, the report represents data from the last 24 hours ending at 10:00 AM of the current day.

- **Bandwidth Usage** - The doughnut chart shows the top 10 applications or users that consumed the most bandwidth in the selected time frame (last hour or last day). Click the **Applications** or **Users** links to toggle between the statistics. To show user information the User Awareness blade must be activated.

- **Top Bandwidth Consuming** - Shows statistics for the top bandwidth consuming application, category, site, and user in percentages and the amount of traffic (MB or GB).
**Traffic** - By default, shows the total amount of traffic received and sent in an area graph. The time axis reflects the time frame (last hour or last day) selected for the Network section. For last hour, the graph shows 5 minute intervals and for last day, hourly intervals. You can click the **Received** and **Sent** links to see only the amount of traffic received or sent. The orange area on the graph represents sent traffic. The blue area represents received traffic.

If you hover over a time interval, a popup box shows:
- The date and time
- The traffic sent or received
- The total traffic for that time interval

**Total traffic statistics** - Next to the area graph you can see total traffic statistics for the last day or hour.

**Security**

- **Infected hosts** - Shows the number of:
  - Infected hosts
  - Infected servers
  - Recently active infected hosts

  You can click **All Infected Hosts** to open the **Logs & Monitoring > Infected Hosts** page.

- **High risk applications** - Shows:
  - The number of high risk applications
  - The most used high risk applications
  - The top users of high risk applications.

  You can click **Applications Blade Control** to open the **Access Policy > Firewall Blade Control** page to see Applications and URL Filtering settings.

- **Security events** - Shows the number of:
  - Anti-Bot - Malwares detected by the Security Gateway.
  - Anti-Virus - Malwares detected by the Security Gateway.
  - Threat Emulation - Malicious files found since the last reboot and how many files scanned.
  - The number of IPS attacks.

  You can click the links to open the **Threat Prevention > Blade Control** page.

**Troubleshooting**

- **System Resources** - Click **CPU, memory and disk usage** to see CPU, memory, and disk usage information.

- **Device Info** - Shows Security Gateway information.

- Links to pages that can be useful for monitoring and troubleshooting purposes.

**Note** - This page is available from the **Home** and **Logs & Monitoring** tabs.
Viewing Reports

The Reports page shows network analysis, security analysis, and infected hosts reports by a selected time frame (monthly, weekly, daily, and hourly).

These elements influence the times shown in reports:

- Rounding off of time
- System reboot

**Rounding Off of Time**

The times shown in generated reports are rounded down:

- For hourly reports - At one minute intervals. For example, if you generate a report at 10:15:45 AM, the report represents data from 9:15 to 10:15.
- For daily reports - At hourly intervals. For example, if you generate a report at 10:15 AM, the report represents data from the last 24 hours ending at 10:00 AM of the current day.
- For weekly reports - At four hour intervals, starting with 00:00, 04:00, 08:00 and so on. For example, if you generate a report at 11:55 AM, the report represents data from the last week ending at 08:00 AM of the current day.
- For monthly reports - At four hour intervals, starting with 00:00, 04:00, 08:00, 12:00 and so on. For example, if you generate a report at 11:15 AM, the report represents data from the last month ending at 08:00 AM of the current day.

**System Reboot**

In the first 24 hour cycle after an appliance starts up (after installation or an update), the system adds one more time interval to the delta of the next applicable report interval.

For example, for weekly reports that are generated at pair hour intervals, the appliance requires 1 more hours plus the delta for the first applicable pair hour.

- For an appliance that started at 00:00 AM - The first weekly report is generated at 04:00 AM. The total of 4 hours derives from the first delta of the first applicable pair hour which is 02:00 and the added 2 hours. The total wait is 4 hours.
- For an appliance that started at 01:59 AM - The first weekly report is generated at 04:00 AM. The generated time derives from the delta of the first applicable pair hour which is 02:00 and the added 2 hours. The total wait is 2 hours.

After you start up an appliance, reports are generated:

- Hourly reports - 2-3 minutes from startup.
- Daily reports - 1-2 hours from startup.
- Weekly reports - 2-4 hours from startup.
- Monthly reports - 4-8 hours from startup.

**Note** - Only the last generated report for each report type is saved in the appliance. When you generate a new report, you override the last saved report for the specified type.

**To generate a report:**

Click the applicable time frame link at the top of the page ([Monthly, Weekly, Daily] or [Hourly]).

The line below the links shows the selected report and its time frame. To refresh the data shown, click Generate.
The report includes these sections:

- Executive Summary
- Table of Contents
- Report Pages

**Executive Summary**

The first page of the report is the executive summary and shows:

- The number of Anti-Bot and Anti-Virus malware detected by the Security Gateway and the number of IPS attacks.
- Top bandwidth consuming statistics by category, site, and user. You can click the **Top category**, **Top site**, or **Top user** link to get to the applicable report page. It also shows **Bandwidth Usage by Applications** statistics for the top 5 applications in a doughnut chart and total traffic received and sent.
- The number of infected hosts, servers, and recently active infected hosts.
- The number of high risk applications, the most used high risk applications, and the top users of high risk applications.
- The Security Gateway name, version, and MAC address.

**Table of Contents**

The table of contents contains links to the network analysis, security analysis, and infected hosts reports. Click a link to go directly to the selected section.

**Report Pages**

Each report page shows a detailed graph, table, and descriptions.

**Note** - This page is available from the **Home** and **Logs & Monitoring** tabs.

**Using System Tools**

On the **Tools** page you can:

- Monitor system resources.
- Show the routing table.
- Verify the appliance connectivity to Cloud Services.
- Display DSL Statistics (DSL models only)
- Generate a CPInfo file.
- Ping or trace an IP address.
- Perform a DNS lookup.
- Capture packets.
- Download the console-USB driver (1400 appliances only)
To monitor system resources:

1. Click Monitor System Resources. The System Resources page opens and shows the following information:
   - **CPU Usage History** (automatically refreshed)
   - **Memory Usage History** - memory is calculated without memory that was preallocated to handle traffic and without cache memory. This gives a more accurate picture of the actual memory usage in the appliance but it may differ from figures you receive from Linux tools. The information is automatically refreshed.
   - **Disk Usage** - click the Refresh button for the most updated disk usage information.

2. Click Close to return to the Tools page.

To show the routing table:

1. Click Show Routing Table. The output appears in the Command Output window.

2. Click Close to return to the Tools page.

To verify the appliance connectivity to Cloud Services:

Click Test Cloud Services Ports.

The Cloud Services Ports Test window opens and shows the available ports and their state.

To display DSL statistics:

Click DSL Statistics. A window opens and shows the statistic parameters.

To generate a CPInfo file:

1. Click Generate CPInfo File. A message next to the button shows the progress.

2. Click Download CPInfo File to view or save the CPInfo file.

To ping or trace an IP address:

1. Enter an IP or host name in the **Host Name or IP Address** field.

2. Click Ping or Trace Route. The output appears in the Command Output window.

3. Click Close to return to the Tools page.

To perform a DNS lookup:

1. Enter a **Host Name or IP Address**.

2. Click Lookup. The output appears in the Command Output window.

3. Click Close to return to the Tools page.

To capture packets:

If a packet capture file exists, a note shows the date of the file and you can download it before you start a new packet capture that overwrites the existing file.

1. Select an option from the **Select Network** list.

2. Click Start and then Stop when you want to stop packet capturing.

3. Click Download File to view or save the capture file.
You can activate packet capture and go to other WebUI application pages while the packet capture runs in the background. However, the packet capture stops automatically if the WebUI session ends. Make sure you return to the packet capture page, stop and download the capture result before you end the WebUI session.

**Note** - The capture utility uses tcpdump. "fw monitor" is available through the command line interface.

When the mini-USB is used as a console connector in 1400 appliances, Windows does not automatically detect and download the driver needed for serial communication. You must manually install the driver. For more information, see sk111713 https://supportcontent.checkpoint.com/solutions?id=sk111713.

To download the Windows driver for Mini-USB console socket (1400 appliances only):

Click the Download link.

**Note** - This page is available from the Home, Device, and Logs & Monitoring tabs.

---

### Managing the Device

This section describes how to set up and manage your Check Point Appliance.

#### Configuring Internet Connectivity

The Device > Internet page shows how the Check Point Appliance connects to the Internet. You can configure a single Internet connection or multiple connections in High Availability or Load Balancing configurations. When multiple Internet connections are defined, the page shows them in a table. You can add a new connection and edit, delete, or disable existing connections. When there are multiple Internet connections, you can select which mode to use - **High Availability** or **Load Balancing**.

We recommend you contact your local Internet Service Provider (ISP) to understand how to configure your specific Internet connection.

**Note** - ADSL/VDSL settings are relevant only for devices that have a DSL port.

To configure Internet connectivity:

1. Click **Configure Internet** (if not configured at all), **Add** (for another Internet connection), or **Edit**.
   
   The New or Edit Internet Connection window opens.

2. Configure the fields in the tabs:

   **Configuration tab**

   **Note** - When you change the connection type, the appliance may disconnect from the Internet.

   - **Connection name** - Enter a name for the connection or leave the default “InternetN” label (where N indicates an incrementing number).

   - **Interface name** -
     - **WAN** or **DMZ** is for most types of Internet connections.
     - **LAN**. You can also use unassigned LAN ports with no VLANs for Internet connections. When you delete the internet connection, the port reverts to an unassigned LAN.

   **Note** - This option is not supported in 1200R appliances.
Appliance Configuration

- **USB/Serial** is for cellular or analog modems.
- **ADSL/VDSL**. If you select the ADSL/VDSL interface, you must select one of these for the connection type: PPPoE, IPoE - static IP, or IPoE - dynamic IP.

You can create a maximum of 32 internet connections.

**Unassigned LAN ports use case** - If your company is in a region where internet connections supplied by ISPs are unreliable and experience multiple disconnections, you can connect your appliances to multiple internet connections from different ISPs.

**IPv4 connection types:**

- **Connection type** - Select the connection type:
  - **DHCP** - Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses within a specified range to devices on a network. The device retains the assigned address for a specified administrator-defined period. This does not apply to the ADSL/VDSL interface.
  - **Static IP** - A fixed (non-dynamic) IP address.
  - **PPPoE** - A network protocol to encapsulate Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly in DSL systems. PPPoE can run directly over the ADSL/VDSL interface. It can also run over WAN or DMZ interfaces that are typically connected to an external DSL modem. You must enter the **IP address**, the **subnet mask**, **default gateway** and **DNS Server Settings**.
  - **IPoE - dynamic IP** (DSL only) - The Internet IP of the appliance is imported through DHCP.
  - **IPoE - static IP** (DSL) - The Internet IP of the appliance is determined statically. You must enter the **IP address**, the **subnet mask**, **default gateway** and **DNS Server Settings**.
  - **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
  - **L2TP** - Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol. It does not provide any encryption or confidentiality but relies on an encryption protocol that it passes within the tunnel to provide privacy.
  - **Bridge** - Connects multiple network segments at the data link layer (Layer 2).
  - **Cellular Modem** - Connect to the Internet with a cellular modem to the ISP through a 3G or 4G network. For this option, select the USB/Serial option in the Interface name.
  - **Analog Modem** - Connect to the Internet with an analog modem through a USB or serial port. For this option, select the USB/Serial option in Interface name.

**Note** - If you use an analog modem through the serial port, you cannot connect to the appliance with the serial port or get terminal server functionality. For more on the terminal server, go to **Device > Advanced Settings**.

Fill in the fields that are shown for the connection type.

**Note** - You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | " # + \
IPv6 connection types:

**Note** - The device can have only a single IPv6 Internet connection.

- **Static IPv6** - A fixed (non-dynamic) IP address.
- **Obtain automatically (DHCPv6/SLAAC)** - In both Dynamic Host Configuration Protocol (DHCP) and Stateless Address Auto Configuration (SLAAC) the user does not set the IP as this is handled by the router/DHCP server. DHCPv6 issues a full IP address. SLAAC issues an IP address prefix, and the gateway completes the rest of the address according to discovery protocols.
- **PPPoE (IPv6 only)** - A network protocol to encapsulate Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and Metro Ethernet networks.
- **PPPoE (IPv4/IPv6)** - Same as **PPPoE (IPv6 only)**, but the user must first configure a type IPv4 PPPoE internet connection on the same interface. Use this option when the ISP provides both IPv4 and IPv6 addresses through the same PPPoE connection. This prevents the need to define the same dialer connection details more than once.
- **IPv6 Bridge** - A Layer 2 bridge between internal and external networks, containing both IPv4 and IPv6 addresses (or just IPv6) to make the gateway reachable through the bridge in a dual stack/pure IPv6 network.

For PPPoE over ATM over VDSL/ADSL or IPoE over ATM over VDSL/ADSL or for an ADSL interface:

Enter the **VPI number** and **VCI number** you received from your service provider, and the **Encapsulation type** (LLC or VC_MUX).

For WAN/DMZ interfaces and static, DHCP, PPPoE, PPTP, and L2TP connection types

Or

For VDSL/ADSL interfaces and IPoE - dynamic IP and IPoE - static IP connection types over PTM:

- **Use connection as VLAN** - Select this checkbox to add a virtual Internet interface.
- **VLAN ID** - Enter a VLAN ID between 1 and 4094.

If you are in an Annex L system, in Advanced Settings, you must enable the Annex L and disable the Annex J/M.

If you are in an Annex M system, in Advanced Settings, you must enable Annex J/M and disable the Annex L. In all other Annex systems, no changes are needed to the default configuration.

**Notes:**

- Multiple internet connections can be established over a single VDSL/ADSL connection carrying PTM traffic or in the case of WAN and DMZ interfaces.
- Only one internet connection can be established over a VDSL/ADSL interface carrying ATM traffic or a USB interface.
- One IPoE or PPPoE connection can be established over ATM running over the DSL interface.
- A single IPoE connection or multiple PPPoE connections can be established over one untagged DSL interface carrying PTM traffic.
- A single IPoE connection or multiple PPPoE connections can be established over one VLAN tagged DSL interface carrying PTM traffic.
- A single DHCP or Static IP connection can be established over a USB interface.
A single DHCP or Static IP connection or multiple PPPoE connections can be established over one untagged or one VLAN tagged WAN or DMZ interface.

When all the ADSL standards are turned off in the Advanced Settings and you can only connect using the VDSL2 standard, the VPI, the VCI and the encapsulation options still appear even though they are not used to open an internet connection.

**Connection Monitoring tab**

- **Automatically detect loss of connectivity to the default gateway** - Select this option to detect connectivity loss by sending ARP requests (pinging) to the default gateway and expecting responses.

- **Monitor connection state by sending probe packets to one or more servers on the Internet** - Select this option to detect connectivity loss by using more methods and servers.
  - **Connection probing method** - Select one of the options.
    - **Ping addresses** - When you select this option, you can configure up to three servers by IP address or host name.
    - **Probe DNS servers** - When you select this option, the appliance probes the DNS servers as defined in the Internet connection and expects responses.

**Advanced tab**

For PPPoE

- **IP Address Assignment** (PPPoE IPv4 only) - In **Local tunnel IP address**, select if the IP address is obtained automatically or manually configured. If manually configured, enter the **IP address**.

- **Service Provider Settings** - In **Service**, enter a service name (optional) and select the **Authentication method**.

- **Connect on demand** - Select the **Connect on demand** checkbox if necessary. This is relevant only when you are in high availability mode.

For PPTP and L2TP

- **IP Address Assignment** -
  - In **Local tunnel IP address**, select if the IP address is obtained automatically or manually configured. If manually configured, enter the **IP address**.
  - In **WAN IP assignment**, select if the WAN IP address is obtained automatically or manually configured. If manually configured, enter the **IP address**, **Subnet mask**, and **Default gateway**.

- **Service Provider Settings** - In **Service**, enter a service name (optional) and select the **Authentication method**.

- **Connect on demand** - Select the **Connect on demand** checkbox if necessary. This is relevant only when you are in high availability mode.

**Port Settings**

- If necessary, select **Use custom MTU value** and set the **MTU size**.

  **Note** - For a DMZ interface the MTU value is applied to all LAN ports.

  To avoid fragmentation (which slows transmission), set the MTU according to the smallest MTU of all the network devices between your gateway and the packet destination.

  For static and DHCP mode, set MTU to 1500 or lower.

  For PPPoE connections, set MTU to 1492 or lower.
Appliance Configuration

**Note** - When the gateway is behind a modem that works as a NAT device, the MTU value of the gateway must be the same value as in the modem. If the modem has a PPPoE connection, set the MTU in the gateway to 1492 or lower.

- **MAC address clone** - If you select *Override default MAC address*, you can override the default MAC address used by the Internet connection. This is useful when the appliance replaces another device and wants to mimic its MAC address.
- If necessary, select *Disable auto negotiation*. This lets you manually define the link speed of the Internet connection.
  - Select the *Link Speed*.

**QoS Settings (bandwidth control) - supported in IPv4 connections only**

To enable QoS bandwidth control for download and upload for this specified connection, select the applicable *Enable QoS (download)* and/or *Enable QoS (upload)* checkboxes. Enter the maximum Kbps rates for the selected options as provided by your ISP for the Internet upload and download bandwidth.

Make sure that the QoS blade is turned on. You can do this from Home > Security Dashboard > QoS > ON.

**ISP Redundancy - supported in IPv4 connections only**

Multiple Internet connections can be configured in High Availability or Load Sharing modes. When you configure more than one Internet connection, the Device > Internet page lets you toggle between these options. The Advanced setting of each Internet connection lets you configure each connection’s priority or weights based on the set mode.

- Clear the *Route traffic through this connection by default* checkbox when you do not want this Internet connection used as a default route for this gateway. The connection is used by the device only if specific, usually service-based, routing rules are defined for it. This is commonly used when you have a connection that is used for dedicated traffic. When you clear this option, this connection does not participate in High Availability or Load Balancing.
- **High Availability** - *Priority* - Select the priority for the connection. Lower priority connections are only used if higher priority connections are unavailable.
- **Load Balancing** - *Weight* - The traffic to the Internet is divided between all available connections based on their weights.

**NAT Settings**

If the gateway’s global hide NAT is turned on in the Access Policy > NAT page, you can disable NAT settings for specified internet connections.

**To disable NAT settings:**

1. Go to Device > Internet.
2. Select an internet connection and click **Edit**.
   The Edit Internet Connection window opens.
3. Click Advanced > NAT Settings.
4. Select *Do not hide internal networks behind this internet connection*.
5. Click **Apply**.
Configuring the Wireless Network

The Device > Wireless page shows the wireless network settings (if applicable). You can configure your main wireless network and also additional guest or standard wireless networks (VAPs - Virtual Access Points).

- **Guest** wireless network - Uses hotspot by default and is unprotected (no password required).
- **Standard** wireless network - Is a protected wireless network that requires a password and does not use a hotspot by default.

To delete the wireless network, go to Device > Local Network.

If multiple wireless networks (VAPs) are defined, the page shows them in a table, where you can add a new guest or standard wireless network and edit, delete, or disable existing ones.

**To turn the Wireless network on or off:**

- Move the slider to select the **On** or **Off** option. If you configured multiple VAPs, selecting Off turns them all off.
  
  **Note** - If you turn off the wireless radio and then turn it back on, the VAPs remain disabled. To enable the VAPs, you must select the relevant entries in the table and click **Enable**.

- To disable or enable the Wireless network, click **Disable/Enable**.

**To edit the radio settings:**

1. Click **Radio settings**.
2. Select the correct **Operation mode, Channel, Channel width, and Transmitter power**.
3. Click **Advanced** to set the **Guard Interval** and **Antenna control**.
4. Click **Apply**.

This configuration is global for all wireless networks. Some options may not be available or allowed depending on your country’s wireless standards.

**1430/1450 appliances only:** The wireless client search options depend on the frequency that the appliance is set to. The Check Point Appliance can be configured to only one frequency at a time and is set to 2.4 GHz by default. If you change the radio settings to 802.11 ac or 802.11 ac/n, the frequency automatically changes to 5 GHz. The Home > System page shows the wireless radio status.

**1470/1490 appliances only:** There are two radio transmitters: 2.4 GHz and 5 GHz. Each network is configured separately under a specified transmitter.

Dynamic Frequency Selection (DFS) detects radar signals that must be protected against interference from 5.0 GHz (802.11ac/n) radios. When these signals are detected, the operating frequency of the 5.0 GHz (802.11ac/n) radio switches to one that does not interfere with the radar systems. DFS is enabled by default.

**To edit a wireless network:**

Click **Edit Settings**.

The **Edit** window opens in the **Configuration** tab.
Configuration tab

- **Network name (SSID)** - Enter a name for the wireless network or use the default name. This is the name shown to clients that look for access points in the transmission area.
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the Device > Hotspot page.

**Wireless Security**

- **Protected network (recommended)** - This is the recommended wireless security setting.
- **Security type** - Select the security technology used in your wireless network. WPA/WPA2 is the most compatible option. WPA2 is the most secure.
- **Encryption type** - Select the encryption method.
- **Authenticate using** - Select Password or RADIUS server (Enterprise mode) to determine how the users authenticate.
  
  The Password option allows a single password for all users. This option is known as **WPA Personal**.
  
  The RADIUS servers (Enterprise mode) option requires defining RADIUS servers in the Users & Objects > Authentication Servers page. Each user that tries to connect to the wireless network is authenticated through the RADIUS server. This option is also known as **WPA Enterprise**.

- **Network password** - When authenticating using a password, enter a password or click Generate for an automatically generated password.
  
  - **Show** - To see the password, select this option. To hide it, clear the checkbox.

- **Unprotected network (not recommended)** - Without a password, any wireless client can connect to this network. This option is not recommended.

**Advanced Settings**

- **Hide the Network Name (SSID)** - When selected, this wireless network name is not automatically shown to users scanning for them. Connecting to the wireless network can be done manually by adding the specified network name.
- **Allow Station-to-Station Traffic** - When selected, allows wireless stations on this network to communicate with each other. When cleared, traffic between wireless stations is blocked.
- **Enable MAC address filtering** - When selected, by default, all wireless devices are not allowed to connect to the wireless network. To allow a specific device to connect, add a new MAC address to the table. Click **New**, enter the device’s **MAC address** and click **Apply**.

Wireless Network tab

**Interface Configuration**

- **Assigned to** - Select Separate network or one of the existing configured networks. When selecting a separate network configure this information:
  
  - **IP address**
    
    - **Note** - 1200R and 1400 appliances support both IPv4 and IPv6 addresses.

  - **Subnet mask** - for IPv4 addresses

  - **Prefix length** - for IPv6 addresses
DHCPv4 Server section
Select one of the options:

- **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance’s own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the Users & Objects > Network Objects page. Reserving specific IP addresses requires the MAC address of the device.
- **Relay** - Enter the DHCP server IP address.
- **Disabled**

IPv6 Auto Assignment section
Select one of the options:

- **SLAAC (Stateless Address Autoconfiguration)**
- **DHCPv6 Server** - Enter the IP address range and the IP addresses exclude range
- **DHCPv6 Server Relay** - Enter the DHCPv6 server IP address and the Secondary DHCPv6 server IP address

Access Policy tab
These options create automatic rules that are shown in the Access Policy > Firewall Policy page.

- **Allow access from this network to local networks (Wireless network is trusted)**
- **Log traffic from this network to local networks**

Advanced tab
Click the checkbox to exclude from DNS proxy.

Advanced IPv6 Settings
Configure the Router Advisement fields.

DHCP/SLAAC Settings tab
Note - In IPv4-only mode, this tab is called DHCP4 Settings.
The values for the DHCP options configured on this tab will be distributed by the DHCP server to the DHCP clients.

DHCP Server Settings (For DHCPv6/SLAAC)
Select one of these options:

- **Auto** - Use the DNS configuration of the device.
- **Use the following IP addresses** - Enter the first, second and third DNS servers.

DNS Server Settings (For DHCPv4)
These settings are effective only if a DHCPv4 server is enabled.
Select one of these options:

- **Auto** - This uses the DNS configuration of the appliance as configured in the Device > DNS and Device > Internet pages.
- **Use the following IP addresses** - Enter the IP addresses for the First DNS server, Second DNS server, and Third DNS server.
**Default Gateway**

Select one of these options:

- **Use this gateway's IP address as the default gateway**
- **Use the following IP address** - Enter an IP address to use as the default gateway.

**WINS**

Select one of these options:

- **Use the WINS servers configured for the internet connection**
- **Use the following WINS servers** - Enter the IP addresses of the **First** and **Second** WINS servers.

**Lease**

- **Lease time** - Configure the timeout in hours for a single device to retain a dynamically acquired IP address.

**Other Settings**

You can optionally configure these additional parameters so they will be distributed to DHCP clients:

- **Time servers**
- **Call manager**
- **TFTP server**
- **TFTP boot file**
- **X-Windows display manager**
- **Avaya IP phone**
- **Nortel IP phone**
- **Thomson IP phone**

**Custom Options**

Lets you add custom options that are not listed above. For each custom option, you must configure the name, tag, type, and data fields.

When you finish editing the network, click **Apply**.

**Configuring the Local Network**

The **Device > Local Network** page lets you set and enable the local network connections, switches, bridge or wireless network (on wireless devices only).

**Note** - 1200R and 1400 appliances support both IPv4 and IPv6 addresses.

The Network table shows all available network connections.

The page also lets you:

- Configure multiple **switches** (port based VLANs) between the available local LAN interfaces and wireless networks. Between the LAN ports of a switch, traffic is not monitored or inspected. **Note** - MAC filtering is disabled on switch networks. To enforce MAC filtering on a network with several ports, use bridge.
- Configure multiple bridges between interfaces. Traffic in a bridge is always monitored and inspected by the appliance.
- Create and configure tag based VLANs (802.1q) on any of the LAN interfaces or DMZ.
- Create and configure VPN tunnels (VTI) which can be used to create routing rules which determine which traffic is routed through the tunnel and therefore also encrypted (Route based VPN).
- On wireless devices - Add new wireless networks (Virtual Access Points). This can also be done through the Device > Wireless page.
  1400 appliances only: There are two radio transmitters: 2.4 GHz and 5 GHz. Each network is configured separately under a specified transmitter.

For 1400 appliances: You can also use unassigned LAN ports to create an internet connection. In the table, these ports have the status Assigned to Internet.

Notes:
- LAN ports assigned to internet connections can only be disabled from the Internet page.
- You cannot edit a LAN port assigned to an internet connection. When you click Edit, the window opens, but when you click Apply, a warning shows that this deletes the connection.
- When you create a bridge or switch surface, these LAN ports do not appear in the selection box as optional ports.

To create any of the above options:
Click New and choose the option you want.

To edit/delete/enable/disable any of the above options:
Select the relevant row and click Edit/Delete/Enable/Disable.

Notes:
- Physical interfaces cannot be deleted.
- Editing an interface that is part of a switch or a bridge lets you remove it from the switch or bridge.
- When a LAN or DMZ interface is part of an Internet connection, it is still visible on this page, but can be only be configured through the Device > Internet page.
- For each network, the table on this page shows you:
  - Name - Name of the network, interfaces that participate (if there are multiple interfaces), and a description (optional)
  - Local IP Address
  - Subnet Mask
  - MAC Address
  - Status - Shows a status for physical interfaces and wireless networks:
    - Physical interfaces - Shows cable connection status of each physical interface that is enabled. Otherwise, it shows disabled.
    - Wireless networks - Shows if the wireless network is up or disabled.
To create/edit a switch:

**Note** - Between the LAN ports of a switch, traffic is not monitored or inspected. MAC filtering is disabled.

Configure the fields in the tabs:

**Configuration tab**

1. In **Switch Configuration**, select or clear the interfaces you want to be part of the switch. The table shows you which interfaces are already part of the switch (shown with checkmarks in the table) and which interfaces are not assigned yet and can be added to the switch (empty checkboxes in the table). For example, if LAN8 is already part of another switch, it does not show in this table.

2. From **Assigned to**, select an option:
   - **Unassigned** - The switch is not part of any network and cannot be used
   - **Separate network** - When you select a separate network, configure the settings for the switch
   - **Monitor Mode** - See below

3. Choose the **IP address** and **Subnet mask** the switch uses.

4. **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device > Hotspot** page.

5. In **DHCP Server**:

   Select one of the options:
   - **Enabled** - Enter the **IP address range** and if necessary the **IP address exclude range**. The appliance’s own IP address is automatically excluded from this range. You can also exclude or reserve specified IP addresses if you define network objects in the **Users & Objects > Network Objects** page. To reserve specified IP addresses, you must have the device MAC address.
   - **Relay** - Enter the DHCP server IP address.
   - **Disabled**

**IPv6 Auto Assignment for IPv6 configurations:**

- **SLAAC (Stateless Address Autoconfiguration)** - The host selects its own full IPv6 address after it receives the IPv6 address prefix from the gateway. The appliance cannot reserve an IPv6 address for a specific host (Mac Address).
  
  **Note** - The common use case is a prefix length of 64. If you change it from 64, make sure the internal hosts support the new length.

- **DHCPv6 Server** - Same as the DHCPv4. You can reserve an IP address for a specified host.

- **DHCPv6 Server Relay** - Same as in IPv4.

- **Disabled (Static)**

**Monitor Mode**

Security Gateways can monitor traffic from a Mirror Port or Span Port on a switch.

With Monitor Mode, the appliance uses Automatic Learning or user-defined networks to identify internal and external traffic, and to enforce policy.

**Automatic Learning** - The appliance automatically recognizes external networks by identifying the default gateway’s network from requests to the Internet (specifically, requests to Google). The rest of the networks are considered internal.
**User-Defined Networks** - You can manually define internal networks. If a network is not defined as internal, it is considered external.

In both Automatic Learning and user-defined networks:

- Traffic to internal hosts is inspected by the Incoming/Internal/VPN Rule Base.
- Traffic to external hosts is inspected by the Outgoing Rule Base.
- Threat prevention's default configuration is optimized to inspect suspicious traffic from external hosts to internal hosts.

**To configure monitor mode in the WebUI:**

1. Go to **Device > Local Network**.
2. Select an interface and double-click. The **Edit** window opens in the **Configuration** tab.
3. In the **Assigned To** drop-down menu, select **Monitor Mode**. The **Manually define internal networks** checkbox shows.
4. To use Automatic Learning, do not select **Manually define internal networks** and click **Apply**.
5. To use your own network definitions, select **Manually define internal networks**. The network definition features and table show.
6. Click **New**.
7. Enter the network **IP address**.
8. Enter the **subnet**. An internal network can be a 255.255.255.255 subnet, for one host. For example, to monitor the traffic after the router, enter the IP address of the Default Gateway and the 255.255.255.255 subnet.
9. Click **Apply**. The Internal network you defined (with Monitor Mode in the name) shows in the list of interfaces.

**Note** - You can configure multiple local networks to be in monitor mode at the same time (1200R and 1400 appliances).

**After you configure monitor mode:**

1. Go to **Device > Advanced Settings**.
2. Turn off **Anti-Spoofing**.

**To configure monitor mode in CLI:**

1. To define a port for Monitor Mode:
   
   ```
   > set interface <portName> monitor-mode
   ```

2. To configure Monitor Mode Automatic Learning, disable user-defined networks:
   
   ```
   > set monitor-mode-configuration use-defined-networks false
   ```

3. To configure Monitor Mode with user-defined networks:
   
   ```
   > add monitor-mode-network ipv4-address <IP> subnet-mask <mask> > set monitor-mode-configuration use-defined-networks true
   ```

4. To see user-defined Internal networks:
   
   ```
   > show monitor-mode-network
   ```

5. To disable Anti-Spoofing:
   
   ```
   > set antispoofting advanced-settings global-activation false
   ```
If you do not see the Monitor Mode option:

1. Run this CLI command:
   
   set monitor-mode-configuration allow-monitor-mode true

2. Select an interface and click **Edit**.

   Monitor Mode is now added to the options list.

For more information on monitor mode, see sk112572

To edit a physical interface:

Configure the fields in the tabs. Note that for the DMZ there is an additional tab **Access Policy**:

**Configuration tab**

- **Assigned to** - Select the required option:
  - **Unassigned** - The physical interface is not part of any network and cannot be used.
  - One of the existing configured **switches** or **bridges**

- **Separate network** - When selecting a separate network configure this information:
  - **IP address**
  - **Subnet mask**
  - **DHCP Server settings**
    
    Select one of the options:
    - **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance’s own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects > Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
    - **Relay** - Enter the DHCP server IP address.
    - **Disabled**

**Note** - When you create a switch, you cannot remove the first interface inside unless you delete the switch.

**Advanced tab**

The options that are shown vary based on interface type and status. Configure the options that are applicable:

- **Description** - Enter an optional description. The description is shown in the local network table next to the name.

- **MTU size** - Configure the Maximum Transmission Unit size for an interface. Note that in the Check Point Appliance, the value is global for all physical LAN and DMZ ports.

- **Disable auto negotiation** - Select this option to manually configure the link speed of the interface.

- **Override default MAC address** – This option is for local networks except those on VLANs and wireless networks. Use this option to override the default MAC address of the network’s interface, when the device has two separate local networks connected to the same external switch.

**Best Practice** - This is a rare configuration. Do not select this option unless you are sure you need it.
• **Exclude from DNS proxy** – Select this checkbox for any network that you do not want exposed to internal domains. In guest VAPs (wireless network for guests), this is selected by default.

**Access Policy tab (only for DMZ)**

These options create automatic rules that are shown in the **Access Policy > Firewall Policy** page.

- **Allow access from this network to local networks**
- **Log traffic from this network to local networks**

**To create/edit a tag based VLAN:**

You can create a new VLAN only if you have at least one physical interface that is not part of an existing network (switch or bridge).

**Note** - For more information on the maximum number of VLANs that you can configure for each appliance, refer to sk113247 http://supportcontent.checkpoint.com/solutions?id=sk113247.

Configure the fields in the tabs:

**Configuration tab**

- **VLAN ID** - Enter a number that is the virtual identifier.
- **Assigned to** - Select the physical interface where the new virtual network is created.
- **IP address**
- **Subnet mask**
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device > Hotspot** page.

- **DHCP Server settings**

  Select one of the options:

  - **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance’s own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects > Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
  - **Relay** - Enter the DHCP server IP address.
  - **Disabled**

**To create/edit a VPN Tunnel (VTI):**

A Virtual Tunnel Interface (VTI) is a virtual interface on a Security Gateway that is related to an existing, Route Based VPN tunnel. The Route Based VPN tunnel works as a point-to-point connection between two peer Security Gateways in a VPN community. Each peer Security Gateway has one VTI that connects to the tunnel.
The VPN tunnel and its properties are defined by the VPN community that contains the two gateways. You must define the VPN community and its member Security Gateways before you can create a VTI.

Configure the fields in the tab:

**Configuration tab**

- **VPN Tunnel ID** - A number identifying the VTI.
- **Peer** - The name of the remote VPN site. See Configuring VPN Sites.

The VPN tunnel interface can be numbered or unnumbered. Select the applicable option:

- **Numbered VTI** - You configure a local and remote IP address for a numbered VTI:
  - **Local IPv4 address** - The IP address to be used for the local point-to-point virtual interface.
  - **Remote IP address** - The IP address to be used at the peer gateway’s point-to-point virtual interface.

- **Unnumbered VTI** - When the VTI is unnumbered, it is not necessary to configure local and remote IP addresses. You define a local interface to use as the source IP address for outbound traffic.
  - **Internet connection** - Select from the list.
  - **Local bridge interface** - Select the local interface from the list.

To create/edit a bridge:

Configure the fields in the tabs:

**Configuration tab**

- In **Bridge Configuration**, select the networks you want to be part of the bridge.
- **Enable Spanning Tree Protocol** - When Spanning Tree Protocol (STP - IEEE 802.1d) is enabled, each bridge communicates with its neighboring bridges or switches to discover how they are interconnected. This information is then used to eliminate loops, while providing optimal routing of packets. STP also uses this information to provide fault tolerance, by re-computing the topology in the event that a bridge or a network link fails.
- Enter a **Name** for the bridge interface. Note that you can only enter "brN" where N is a number between 0 and 9. For example, br2.
- Choose the **IP address** and **Subnet mask** the switch uses.
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device > Hotspot** page.
- **DHCP Server**
  Select one of the options:
  - **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance’s own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects > Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
  - **Relay** - Enter the DHCP server IP address.
  - **Disabled**
Advanced tab

- **MTU size** - Configure the Maximum Transmission Unit size for an interface.
- **Disable auto negotiation** - Select this option to manually configure the link speed of the interface.
- **Override default MAC address** – This option is for local networks except those on VLANs and wireless networks. Use this option to override the default MAC address used by the network’s interface, when the device has two separate local networks connected to the same external switch.
  
  **Best Practice** - This is a rare configuration. Do not select this option unless you are sure you need it.
- **Exclude from DNS proxy** – Select this checkbox for any network that you do not want exposed to internal domains. In guest VAPs (wireless network for guests), this is selected by default.

Advanced IPv6 Settings

Configure the Router Advisement fields.

**To create/edit a Virtual Access Point (VAP):**

See the Device > Wireless Network help page.

DHCP/SLAAC Settings tab

**Note** - In IPv4-only mode, this tab is called DHCPv4 Settings.

The values for the DHCP options configured on this tab will be distributed by the DHCP server to the DHCP clients.

**DNS Server Settings (For DHCPv6/SLAAC)**

Select one of these options:

- **Auto** - Use the DNS configuration of the device.
- **Use the following IP addresses** - Enter the first, second and third DNS servers.

**DNS Server Settings (For DHCPv4)**

These settings are effective only if a DHCPv4 server is enabled.

Select one of these options:

- **Auto** - This uses the DNS configuration of the appliance as configured in the Device > DNS and Device > Internet pages.
- **Use the following IP addresses** - Enter the IP addresses for the First DNS server, Second DNS server, and Third DNS server.

**Default Gateway**

Select one of these options:

- **Use this gateway’s IP address as the default gateway**
- **Use the following IP address** - Enter an IP address to use as the default gateway.
WINS

Select one of these options:

- **Use the WINS servers configured for the internet connection**
- **Use the following WINS servers** - Enter the IP addresses of the First and Second WINS servers.

*Lease section*

- **Lease time** - Configure the timeout in hours for a single device to retain a dynamically acquired IP address.

*Other Settings*

You can optionally configure these additional parameters so they will be distributed to DHCP clients:

- Time servers
- Call manager
- TFTP server
- TFTP boot file
- X-Windows display manager
- Avaya IP phone
- Nortel IP phone
- Thomson IP phone

*Custom Options*

Lets you add custom options that are not listed above. For each custom option, you must configure the name, tag, type, and data fields.

Configuring a Hotspot

In the **Device > Hotspot** page, if a network interface was defined for hotspot, you can configure:

- **Guest access** - A session is created for an IP address when a user accepts terms or authenticates in the Hotspot portal. The session expires after the configured timeout (240 minutes by default).
- **Hotspot portal** - Customize the portal’s appearance.
- **Hotspot exceptions** - Define specified IP addresses, IP ranges or networks to exclude from the Hotspot.

If no network interface was defined for the Hotspot, click **Configure in Local Network**.

In the **Access** section of the page, you can configure if authentication is required and allow access to all users or to a specified user group (Active Directory, RADIUS or local).

Hotspot is automatically activated in the system.
To turn off Hotspot:
1. Go to Device > Advanced Settings.
2. Search for Hotspot and double-click the entry.
3. Select Disabled.
4. Click Apply.

To configure Hotspot for an interface:
1. Click Configure in Local Network.
The Local Network window opens.
2. Select interface and click Edit.
The Edit <interface> window opens.
3. Select Use Hotspot.
4. Click Apply.

Any user that browses from configured interfaces is redirected to the Check Point Hotspot portal.

To configure Hotspot exceptions:
1. Click Manage Exceptions.
The Manage Hotspot Network Objects Exceptions window opens.
2. Select the objects to add as exceptions.
The Selected Network Objects window shows the selected objects. To remove an object from the list, click the x next to it.
3. To filter the object list, enter the filter value. The list shows the objects that match the filter.
4. If necessary, click New to add new objects to the list. For information on how to create a new object, see the Users & Objects > Network Objects page.
5. Click Apply.
The added objects are excluded from the Hotspot.

To require user authentication:
1. Select the Require Authentication checkbox.
2. You can allow access to All users or to a Specific user group.
3. If you selected Specific user group, enter the group’s name in the text box.
4. Click Apply.
Any user/user group that browses from configured interfaces is redirected to the Check Point Hotspot portal and must enter authentication credentials.

To configure the session timeout:
1. In Session timeout, enter the number of minutes that defines how long a user stays logged in to the session before it is ends.
2. Click Apply.

To customize the portal appearance:
1. Click Customize Hotspot portal.
2. For Portal title - Keep the default or enter a different title.
3. For Portal message - Keep the default or enter a different message.
4. For **Terms of use** - Select this checkbox to add an "I agree with the following terms and conditions" checkbox on the Hotspot portal page. Enter the terms and conditions text in the text box. When users click the "terms and conditions" link, this text shows.

5. To customize a logo for all portals shown by the appliance (Hotspot and captive portal used by User Awareness), click **Upload**, browse to the logo file and click **Apply**. If necessary, click **Use Default** to revert to the default logo.

6. Click **Apply**.

To prevent simultaneous login to the Hotspot portal:

1. Go to **Device > Advanced Settings**.
2. Select **Hotspot**.
3. Click **Edit**.
   
   The **Hotspot** window opens.

4. Click the checkbox for **Prevent simultaneous login**.

5. Click **Apply**.

   The same user cannot log in to the Hotspot portal from more than one computer at a time.

On the **Active Devices** page (available through the **Home** and **Logs & Monitoring** tabs), you can revoke Hotspot access for connected users.

### Configuring the Routing Table

The **Device > Routing** page shows routing tables with the routes added on your appliance.

On this page:

- You can add or edit routes and configure manual routing rules. You cannot edit system defined routes.

- You can specify routes for and associate IP addresses with selected VPN tunnels. To add, delete, and modify the IP addresses, use dynamic routing protocols.
For every route:

<table>
<thead>
<tr>
<th>Table Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>The route rule applies only to traffic whose destination matches the destination IP address/network.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>IPv4 only. The route rule applies only to traffic whose source matches the source IP address/network.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>IPv4 only. The route rule applies only to traffic whose service matches the service IP protocol and ports or service group.</td>
</tr>
<tr>
<td><strong>Next Hop</strong></td>
<td>The next hop gateway for this route, with these options:</td>
</tr>
<tr>
<td></td>
<td>• Specified IP address of the next hop gateway</td>
</tr>
<tr>
<td></td>
<td>• Specified Internet connection from the connections configured in the appliance</td>
</tr>
<tr>
<td></td>
<td>• Specified VPN Tunnel Interface (VTI)</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is selected.</td>
</tr>
</tbody>
</table>

To add a new static route (IPv4 addresses):

1. In **Device > Routing**, above the **Routing Table**, click **New**. The New Routing Rule window opens with this message: Traffic from **any source** to **any destination** that belongs to **any service** should be routed through the **next hop**.
2. Click **next hop** and select an option in the new window that opens:
   - **IP Address** - Enter the IP address.
   - **Internet connection** - Select an internet connection.
   - **VPN Tunnel (VTI)** - Select the VPN Tunnel.
3. Click **OK**.
4. Click **any source** and select an option in the new window that opens:
   - Any
   - **Specified IP address** - Enter the **IP Address** and **Mask**
5. Click **any destination** and select an option in the new window that opens:
   - Any
   - **Specified IP address** - Enter the **IP Address** and **Mask**
6. Click **OK**.
7. Click **any service** and select a service name or enter a service name in the search field. You can create a new service or service group.
   **Note** - Static routes are not supported for source based or service based routes.
8. **Optional** - Enter a comment.
9. Enter a **Metric** between 0 and 100. The default is 0.
10. Click **Apply**.
To configure a default route:
1. Go to Device > Local Network page.
2. Select an interface and click Edit.
   The Edit window opens in the Configuration tab.
3. Click the DHCP Server options tab.
4. In the Default Gateway section,
   - Click Use this gateway's IP address as the default gateway.
     Or
   - Select Use the following IP address and enter an IP address.
5. Click Apply.

To edit a default route:
1. In Device > Internet, click the Internet connection.
2. Click Edit.
   The Edit Internet Connection window opens in the Configuration tab.
3. Set the Default gateway (next hop) to a different IP address.
4. Click Apply.

When no default route is active, this message shows: "Note - No default route is configured. Internet connections might be down or not configured."

For Internet Connection High Availability, the default route changes automatically on failover (based on the active Internet connection).

When a network interface is disabled, all routes that lead to it show as inactive in the routing page. A route automatically becomes active when the interface is enabled. Traffic for an inactive route is routed based on active routing rules (usually to the default route).

The edit, delete, enable, and disable options (on the Device > Local Network page) are only available for manually defined routing rules created on this page. You cannot edit, delete, enable, and disable routing rules created by the operating system for directly attached networks or rules defined by the dynamic routing protocol.

To edit an existing route:
Select the route and click Edit.

To delete an existing route:
Select the route and click Delete.

To enable/disable an existing route:
Select the route and click Enable or Disable.
Configuring MAC Filtering

MAC Filtering

MAC Filtering lets you manage a whitelist of MAC addresses that can access the LAN. All others are blocked. The list is global for all interfaces defined on physical LAN ports.

To enable MAC filtering:

1. Turn the slider to **ON**.
2. Add a MAC address to the LAN MAC Filter whitelist.

   **Note** - MAC filtering is not active when no MAC addresses are defined.

After MAC filtering is enabled, you can disable the feature for specified networks.

To edit the LAN MAC Filter whitelist:

1. Go to **Device > MAC Filtering > LAN MAC Filter**.
2. To add a new MAC Address, click **Add > New**.
3. To select MAC addresses from the list of Active Devices, click **Add > Select**.
4. To edit a MAC address, select it from the list and click **Edit**.
5. To delete a MAC address, select it from the list and click **Delete**.

To disable MAC filtering for a specific interface:

1. Go to **Device > Local Network**.
2. Select a LAN interface and click **Edit**
   The Edit LAN window opens.
3. Click **Advanced**.
4. Select **Disable MAC filtering**.
   To enable, clear this option.
5. Click **Apply**.

Limitations:

- MAC filtering is not supported on external interfaces and over switches between physical LAN ports (port-based VLANs). If you configure a physical switch between multiple LAN ports, you cannot activate MAC filtering on this network. Replace the switch with a bridge configuration.
- To disable MAC filtering for a bridged LAN interface, you must reboot.
- Traffic from a remote encryption domain is not MAC filtered.
- Broadcast traffic such as ARP and DHCP is not blocked.
- To configure MAC filtering for a DMZ interface, you must use CLI. You cannot configure MAC filtering in the WebUI.

802.1x Authentication Protocol

IEEE 802.1x is a port-based network access protocol that provides an authentication mechanism for devices that are physically attached to the network.

802.1x authentication is enabled only when you define a LAN or a DMZ network as a separate network and a RADIUS server is defined.
Workflow:
2. Define it on the appliance
3. Activate 802.1x authentication on a separate LAN interface (includes the DMZ when not used as an internet connection), or a tag-based VLAN interface defined on one of the LAN physical ports.

If you configure a physical switch (port-based VLAN) between multiple LAN ports, you cannot activate the 802.1x protocol on this network. Replace the switch with a bridge configuration.

To enable 802.1x authentication on a separate LAN interface:
1. Go to Device > Local Network.
2. Select the LAN interface and click Edit.
   The Edit window opens in the Configuration tab.
3. For Assigned to: select Separate network.
4. In the Advanced tab, select Activate 802.1x authentication.
5. Enter a time for Re-authentication frequency (in seconds).
6. Click Apply.

To enable 802.1x authentication on a tag based VLAN interface:
1. Go to Device > Local Network.
2. Select the LAN and click New > VLAN.
   The New VLAN window opens in the Configuration tab.
3. For Assigned to: select the LAN ID.
4. In the Advanced tab, select Activate 802.1x authentication.
5. Enter a time for Re-authentication frequency (in seconds).
6. Click Apply.

To disable 802.1x authentication on an interface:
1. Go to Device > Local Network.
   Select the LAN interface and click Edit.
2. The Edit window opens in the Configuration tab.
3. Click the Advanced tab.
4. Clear Activate 802.1x authentication.
5. Click Apply.

To configure logging for MAC filtering and 802.1x authentication:
1. Go to Device > Advanced Settings.
2. Set the value of the MAC Filtering settings - Log blocked MAC addresses attribute to
   - Enabled - To enable logging
   - Disabled - To disable logging.
   Note - This attribute is available only in Locally Managed mode. In Centrally Managed mode, configure logging with CLI.
3. **Optional** -
   - To reduce the number of logs, specify the value of the **MAC Filtering settings - Log suspension** attribute in seconds.
   - To show all logs, set the value to “0”.

   **Note** - Traffic dropped in the WiFi driver is not logged.

### Configuring the DNS Server

In the **Device > DNS** page you can configure the DNS server configuration and define the domain name.

**To configure DNS:**

1. Select to define up to three DNS servers which is applied to all Internet connections or use the DNS configuration provided by the active Internet connection (Primary).
   
   If you select **Configure DNS servers**, make sure that you enter valid IP addresses.
   
   Use the first option if your DNS servers are located in the headquarters office. In this case, all DNS requests from this branch office are directed to these DNS servers.
   
   The second option allows a more dynamic definition of DNS servers. The gateway uses the DNS settings of the currently-active Internet connection (in case of static IP – the DNS manually provided under “Internet connection”-> Edit, in case of DHCP / Dialers – the DNS automatically provided by the ISP). If Internet Connection High Availability is enabled, the DNS servers switch automatically upon failover.

2. By default, the Check Point Appliance functions as your DNS proxy and provides DNS resolving services to internal hosts behind it (network objects). This option is global and applies to all internal networks.
   
   To get IP addresses directly from the DNS servers defined above, clear the **Enable DNS Proxy** checkbox.
   
   When DNS proxy is enabled, **Resolve Network Objects** controls if the DNS proxy treats the local network objects as a **hosts list**. When selected, the local DNS servers resolves network object names to their IP addresses for internal network clients.

3. Enter a **Domain Name**. There are two separate uses of the domain name:
   
   - Local hosts (the Security Gateway and network objects) are optionally appended with the domain name when DNS resolving is performed.
   
   - DNS queries that do not contain a domain name are automatically appended with the domain name.

   Note these syntax guidelines:
   
   - The domain name must start and end with an alphanumeric character.
   
   - The domain name can contain periods, hyphens, and alphanumeric characters.

4. Click **Apply**.
Configuring the Proxy Server

In the Device > Proxy page, you can configure a proxy server to use to connect to the Check Point update and license servers.

To configure a proxy server:
1. Select Use a proxy server.
2. Enter a Host name or IP address.
3. Enter a Port.
4. Click Apply.

Backup, Restore, Upgrade, and Other System Operations

In the Device > System Operations page you can:

- Reboot
- Restore factory default settings
- Revert to the factory default image and settings
- Automatically or manually upgrade ("Using the Software Upgrade Wizard" on page 82) the appliance firmware to the latest Check Point version
- Revert to earlier firmware image
- Backup appliance settings ("Backing up the System" on page 83) to a file stored on your desktop computer
- Restore a backed up configuration
- Enable IPv6 networking and enforce IPv6 security (1200R and 1400 appliances only)

To reboot the appliance:
1. Click Reboot.
2. Click OK in the confirmation message.
   The appliance reboots.

To restore factory default settings:
1. Click Default Settings.
2. Click OK in the confirmation message.
   The factory default settings are restored. The appliance reboots to complete the operation.
   **Note** - This does not change the software image. Only the settings are restored to their default values (IP address https://192.168.1.1:4434, the username: admin and password: admin).

To revert to the factory default image:
1. Click Factory Defaults.
2. Click OK in the confirmation message.
   The factory default settings are restored. The appliance reboots to complete the operation.
   **Note** - This restores the default software image which the appliance came with and also the default settings (IP address https://192.168.1.1:4434, the username: admin and password: admin).
To make sure you have the latest firmware version:
Click Check now.

To automatically upgrade your appliance firmware when Cloud Services is not configured:
1. Click Configure automatic upgrades.
   The Automatic Firmware Upgrades window opens.
2. Click Perform firmware upgrades automatically.
3. Select the upgrade option to use when new firmware is detected:
   • Upgrade immediately
   Or
   • Upgrade according to this frequency.
4. If you selected Upgrade according to this frequency, select one of the Occurs options:
   • Daily - Select the Time of day.
   • Weekly - Select the Day of week and Time of day.
   • Monthly - Select the Day of month and Time of day.
5. Click Apply.

Notes:
• When a new firmware upgrade is available, a note shows the version number. Click Upgrade Now to upgrade it immediately, or click More Information to see what is new in the firmware version.
• If the gateway is configured by Cloud Services, automatic firmware upgrades are locked. They can only be set by Cloud Services.

To manually upgrade your appliance firmware:
1. Click Manual Upgrade.
   The Upgrade Software Wizard opens.
2. Follow the Wizard instructions.
   Note - The firewall remains active while the upgrade is in process. Traffic disruption can only be caused by:
   • Saving a local image before the upgrade (this causes the Firewall daemon to shut down). This may lead to disruption in VPN connections.
   • The upgrade process automatically reboots the appliance.

To revert to an earlier firmware image:
1. Click Revert to Previous Image.
2. Click OK in the confirmation message.
   The appliance reboots to complete the operation.

To backup appliance settings:
1. Click Backup.
   The Backup Settings page opens.
2. To encrypt the backup file, select the Use File Encryption checkbox. Set and confirm a password.
3. To back up the security policy installed on the appliance, select the **Backup Security Policy** checkbox. You can add **Comments** about the specific backup file created.

4. Click **Save Backup**. The File Download dialog box appears. The file name format is `<current software version>-<YY-Month-day>-<HH_MM_Seconds>.zip`

5. Click **Save** and select a location.

**To restore a backed up configuration:**
1. Click **Restore**. The Restore Settings page appears.
2. Browse to the location of the backed up file.
3. Click **Upload File**.

**Important Notes**
- To **replace** an existing appliance with another one (for example, upon hardware failure) you can restore the settings saved on your previous appliance and reactivate your license (through **Device > License**).
- To **duplicate** an existing appliance you can restore the settings of the original appliance on the new one.
- Restoring settings of a different version is supported, but not automatically between every two versions. If the restore action is not supported between two versions, the gateway does not allow you to restore the settings.

**IPv6 Mode**

To enable IPv6 networking and enforce IPv6 security:
1. Click **IPv6 Enforcement Settings**.
   - The **IPv6 Enforcement Settings** window opens.
2. To enforce IPv6 security policy, click the checkbox.
3. To enable IPv6 networking, click the checkbox.
4. Click **Apply**.
   - **Note** - This causes the appliance to reboot.

**Using the Software Upgrade Wizard**

Follow the instructions in each page of the Software Upgrade Wizard.

During the wizard click **Cancel** to quit the wizard.

**Welcome**

Click the **Check Point Download Center** link to download an upgrade package as directed. If you already downloaded the file, you can skip this step.

**Upload Software**

Click **Browse** to select the upgrade package file.

Click **Upload**. This may take a few minutes. When the upload is complete, the wizard automatically validates the image. A progress indicator at the bottom of the page tells you the percentage completed. When there is successful image validation, an "Upload Finished" status shows.
Upgrade Settings

The system always performs an upgrade on a separate flash partition and your current-running partition is not affected. You can always switch back to the current image if there is an immediate failure in the upgrade process. If the appliance does not come up properly from the boot, disconnect the power cable and reconnect it. The appliance automatically reverts to the previous image.

Click the **Revert to Previous Image** button on the System Operations page to return to an earlier image. The backup contains the entire image, including the firmware, all system settings and the current security policy.

When you click **Next**, the upgrade process starts.

Upgrading

The Upgrading page shows an upgrade progress indicator and checks off each step as it is completed.

- Initializing upgrade process
- Installing new image

**Backing up the System**

In the **Device > System Operations** page you can backup and restore system settings.

To create a backup file:

1. Click **Create Backup File**.
   
   The **Backup Settings** window opens.
2. To encrypt the file, click **Use file encryption**.
   
   If you select this option, you must enter and confirm a password.
3. **Optional** - add a comment about the backup file.
4. Click **Create Backup**.
   
   System settings are backed up.

The backup file includes all your system settings such as network settings and DNS configuration. The backup file also contains the Secure Internal Communication certificate and your license.

If you want to **replace** an existing appliance with another one, you can restore the settings of your previous appliance and re-activate your license (through **License Page > Activate License**).

If you want to **duplicate** an existing appliance, you can restore the settings of the original appliance on the new one. Make sure to change the IP address of the duplicated appliance (**Device > Internet** page) and generate a new license.

To configure a periodic backup to the FTP server:

1. Go to **Device > System Operations > Backup and Restore System Settings**.
2. Click **Settings**.
   
   The **Periodic Backup Settings** window opens.
3. Click **Enable scheduled backups**.
4. Configure the file storage destination (see below).
5. **Optional** - Select **Use file encryption**.
   
   If you select this option, you must enter and confirm a password.
6. In **Schedule Periodic Backup**, select frequency:
   - **Daily** - Select time of day (hour range).
   - **Weekly** - Select day of week and time of day.
   - **Monthly** - Select day of month and time of day. **Note** - If a month doesn’t include the selected day, the backup is executed on the last day of the month.

7. Click **Apply**.

To configure a file storage destination:

1. In **Device > System Operations > Backup and Restore System Settings**, click **Settings**.
   - The **Periodic Backup Settings** window opens.
2. Click **Enable scheduled backups**.
3. Enter a **Backup server path**.
4. Enter a username and password.
5. Click **Apply**.

### Configuring Local and Remote System Administrators

The **Device > Administrators** page lists the Check Point Appliance administrators and lets you:

- Create new local administrators
- Configure the session timeout
- Limit login failure attempts

Administrators can also be defined in a remote RADIUS server and you can configure the appliance to allow them access. Authentication of those remotely defined administrators is done by the same RADIUS server.

**Administrator Roles:**

- **Super Administrator** - All permissions. Super Administrators can create new locally defined administrators and change permissions for others.
- **Read Only Administrator** - Limited permissions. Read Only Administrators cannot update appliance configuration but can change their own passwords or run a traffic monitoring report from the Tools page.
- **Networking Administrator** - Limited permissions. Networking Administrators can update or modify operating system settings. They can select a service or network object but cannot create or modify it.

Two administrators with write permissions cannot log in at the same time. If an administrator is already logged in, a message shows. You can choose to log in with Read-Only permission or to continue. If you continue the login process, the first administrator session ends automatically.

The correct Administrator Role must be configured to perform the operations listed below. If not, a **Permission Error** message shows.
To create a local administrator:

1. Click **New**.
   
The **Add Administrator** page opens.

2. Configure the parameters [name, password, and password confirmation]. The hyphen (-) character is allowed in the administrator name. You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | ' " # + \n
3. Select the **Administrator Role**.

4. Click **Apply**.
   
The name and Administrator Role is added to the table. When logged in to the WebUI, the administrator name and role is shown at the top of the page.

To edit the details of locally defined administrators:

1. Select the administrator from the table and click **Edit**.

2. Make the relevant changes.

3. Click **Apply**.

To delete a locally defined administrator:

1. Select an administrator from the list.

2. Click **Delete**.

3. Click **Yes** in the confirmation message.

**Note** - You cannot delete an administrator who is currently logged in.

To allow access for administrators defined in a remote RADIUS server:

1. Make sure administrators are defined in the remote RADIUS server.

2. Make sure a RADIUS server is defined on the appliance. If there is no server, click the **RADIUS configuration** link at the top of this page. You must configure the IP address and shared secret used by the RADIUS server.

3. When you have a configured RADIUS server, click **edit permissions**.
   
The **RADIUS Authentication** window opens.

4. Click the **Enable RADIUS authentication for administrators** checkbox.

   **Use roles defined on RADIUS server** is selected by default.

5. Configure the role for each user on the RADIUS server. See additional details below.

   **Note** - A user without role definition will get a login error.

6. If you select **Use default role for RADIUS users**, select the **Administrators Role**:

   - Super Admin
   - Read only
   - Networking Admin

7. To define groups, click **Use specific RADIUS groups only** and enter the RADIUS groups separated by a comma.

8. Click **Apply**.
To set the Session Timeout value for both local and remotely defined administrators:

1. Click Security Settings.
   The Administrators Security Settings window opens.
2. Configure the session timeout (maximum time period of inactivity in minutes). The maximum value is 999 minutes.
3. To limit login failure attempts, click the Limit administrators login failure attempts checkbox.
4. Enter the number of Maximum consecutive login attempts allowed before an administrator is locked out.
5. In Lock period, enter the time (in seconds) that must pass before a locked out administrator can attempt to log in again.
6. To enforce password complexity on administrators, click the checkbox and enter the number of days for the password to expire.
7. Click Apply.

**Note** - This page is available from the Device and Users & Objects tabs.

Configuring a RADIUS Server for non-local Check Point Appliance users:
Non-local users can be defined on a RADIUS server and not in the Check Point Appliance. When a non-local user logs in to the appliance, the RADIUS server authenticates the user and assigns the applicable permissions. You must configure the RADIUS server to correctly authenticate and authorize non-local users.

**Note** - The configuration of the RADIUS Servers may change according to the type of operating system on which the RADIUS Server is installed.

**Note** - If you define a RADIUS user with a null password (on the RADIUS server), the appliance cannot authenticate that user.

To configure a Steel-Belted RADIUS server for non-local appliance users:

1. Create the dictionary file checkpoint.dct on the RADIUS server, in the default dictionary directory (that contains radius.dct). Add these lines to the file:

```plaintext
@radius.dct
MACRO CheckPoint-VSA(t,s) 26 [vid=2620 type1=%t% len1=+2 data=%s%]
ATTRIBUTE CP-Gaia-User-Role CheckPoint-VSA(229, string) r
ATTRIBUTE CP-Gaia-SuperUser-Access CheckPoint-VSA(230, integer) r
```
2. Add the following lines to the vendor.ini file on RADIUS server (keep in alphabetical order with the other vendor products in this file):

```plaintext
vendor-product = Check Point Appliance
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```
3. Add to the dictiona.dcm file the line:

```
"@checkpoint.dct"
```
4. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

\[
\text{CP-Gaia-User-Role} = \text{<role>}
\]

Where \text{<role>} allowed values are:

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>adminrole</td>
</tr>
<tr>
<td>Read only</td>
<td>monitorrole</td>
</tr>
<tr>
<td>Networking Admin</td>
<td>networkingrole</td>
</tr>
</tbody>
</table>

To configure a FreeRADIUS server for non-local appliance users:

1. Create the dictionary file \text{dictionary.checkpoint} in \text{/etc/freeradius/} on the RADIUS server:

```
# Check Point dictionary file for freeradius AAA server
# VENDOR CheckPoint 2620
ATTRIBUTE CP-Gaia-User-Role 229 string
ATTRIBUTE CP-Gaia-SuperUser-Access 230 integer
```

2. Add to \text{/etc/freeradius/dictionary} the line:

```
"$INCLUDE dictionary.checkpoint"
```

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

\[
\text{CP-Gaia-User-Role} = \text{<role>}
\]

Where \text{<role>} is the name of the administrator role that is defined in the WebUI.

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>adminrole</td>
</tr>
<tr>
<td>Read only</td>
<td>monitorrole</td>
</tr>
<tr>
<td>Networking Admin</td>
<td>networkingrole</td>
</tr>
</tbody>
</table>
To configure an OpenRADIUS server for non-local appliance users:

1. Create the dictionary file `dict.checkpoint` in 
   `/etc/openradius/subdicts/`
   on the RADIUS server:

   ```
   # Check Point Gaia vendor specific attributes
   # (Formatted for the OpenRADIUS RADIUS server.)
   # Add this file to etc/openradius/subdicts/ and add the line
   # "$include subdicts/dict.checkpoint" to etc/openradius/dictionaries
   # right after dict.ascend.

   $add vendor 2620 CheckPoint
   $set default vendor=CheckPoint
   space=RAD-VSA-STD
   len_ofs=1 len_size=1 len_adj=0
   val_ofs=2 val_size=-2 val_type=String
   nodec=0 noenc=0

   $add attribute 229 CP-Gaia-User-Role
   $add attribute 230 CP-Gaia-SuperUser-Access val_type=Integer
   val_size=4
   ```

2. Add the line
   `$include subdicts/dict.checkpoint`
   to
   `/etc/openradius/dictionaries`
   immediately after `dict.ascend`

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   ```
   CP-Gaia-User-Role = <role>
   ```
   Where `<role>` is the name of the administrator role that is defined in the WebUI.

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>adminrole</td>
</tr>
<tr>
<td>Read only</td>
<td>monitorrole</td>
</tr>
<tr>
<td>Networking Admin</td>
<td>networkingrole</td>
</tr>
</tbody>
</table>

To log in as a Super User:

A user with super user permissions can use the Check Point Appliance shell to do system-level operations, including working with the file system.

1. Connect to the Check Point Appliance platform using an SSH client or serial console client.
2. Log in to the Clish shell using your user name and password.
3. Run Expert
4. Enter the expert password.
Configuring Administrator Access

The Device > Administrator Access page lets you configure the IP addresses and interface sources that administrators can use to access the Check Point Appliance. You can also configure the Web and SSH ports.

First set the interface sources from which allowed IP addresses can access the appliance.

To set the interface sources from which administrator access is allowed:

Select one or more of the options:

- **LAN** - All internal physical ports
- **Trusted wireless** - Wireless networks that are allowed access to the LAN by default (only in Wireless Network models.)
- **VPN** - Uses encrypted traffic through VPN tunnels from a remote site or uses a remote access client
- **Internet** - Clear traffic from the Internet (not recommended to allow access from all IP addresses)

To allow administrator access from any IP address:

1. Select the **Any IP address** option. This option is less secure and not recommended. We recommend you allow access from the Internet to specific IP addresses only.
2. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
3. Click **Apply**. An administrator can access the Check Point Appliance using any IP address through the allowed interface sources.

To allow administrator access from specified IP addresses:

1. Select the **Specified IP addresses only** option.
2. Click **New**.
   The **IP Address Configuration** page shows.
3. Select **Type**:
   - IPv4 address
   - IPv4 network
   - IPv6 address
   - IPv6 network
4. Enter the IP address or click **Get IP from My Computer**.
5. Click **Apply**.
   The IP address is added to the table.
6. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
7. Click **Apply**. An administrator can access the Check Point Appliance using the configured IP addresses through the allowed interface sources.
To allow administrator access from both specified and any IP addresses:
Select this option when it is necessary to allow administrator access from the Internet (you must define the specified IP addresses). Access from other sources is allowed from any IP address.

1. Select the Internet source checkbox.
2. Select the **Specified IP addresses from the internet and any IP address from other sources** option.
3. Click **New**.
   The **IP Address Configuration** page shows.
4. Select **Type**:
   - IPv4 address
   - IPv4 network
   - IPv6 address
   - IPv6 network
5. Enter the IP address or click **Get IP from My Computer**.
6. Click **Apply**.
   The IP address is added to the table.
7. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
8. Click **Apply**. An administrator can access the Check Point Appliance using the configured IP addresses through the allowed interface sources.

To delete administrator access from a specific IP address:
1. Select the IP Address you want to delete from the IP Address table.
2. Click **Delete**.

**Important Notes:**
- Configuring different access permissions for LAN and Internet is not supported when your Internet Connection is configured in bridge mode (the option **Allow administration access from** does not show Internet or LAN).
- An automatic implied rule is defined to allow the access specified here. There is no need to add an explicit rule in the Access Policy page to allow this access.
- When you block the IP address or the interface group through which you are currently connected, you are not disconnected immediately. The access policy is applied immediately, but your current session remains active until you log out.

**Managing Device Details**
In the **Device > Device Details** page, you can:
- Enter an **Appliance Name** for the appliance to identify the Check Point Appliance.
  **Note** - The appliance name can only contain alphanumeric characters and the hyphen character. Do not use the hyphen character as the first or last character.

  **Important** - If the gateway’s Internet connection is assigned an IP address dynamically and the identifier option in SmartDashboard is set to Gateway name, the Appliance Name must be identical to the Check Point Appliance name defined for the Check Point Appliance object in SmartDashboard.
• **For wireless devices only** - Configure the **Country**. The allowed wireless radio settings vary based on the standard of each country.

• Assign a Web portal certificate.

**To assign a Web portal certificate:**
1. Click the downward arrow next to the **Web portal certificate** field. The list of uploaded certificates shows.
2. Select the desired certificate.
3. Click **Apply**.
4. Reload the page.

### Managing Date and Time

The **Device > Date and Time** page shows the current system time and lets you define the Check Point Appliance date and time, optionally using NTP.

**To manually configure date and time:**
1. Select the **Set Date and Time Manually** option.
2. Enter the current **Date** and **Time**. Click the calendar icon to enter the date. Specify whether the time is AM or PM.
3. Click **Apply**.

**To use Network Time Protocol (NTP) to synchronize the clocks of computers on the network:**
1. Select the **Set Date and Time Using a Network Time Protocol (NTP) Server** option.
2. Enter the Host name or IP addresses of the **Primary NTP Server** and **Secondary NTP Server**. If the Primary NTP Server fails to respond, the Secondary NTP Server is queried.
3. Set the **Update Interval (minutes)** field.
4. Select the **NTP Authentication** checkbox if you want to supply a **Shared Secret** and a **Shared Secret Identifier** (this is optional). You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | ' " # + \n
5. Click **Apply**.

### Time Zone

1. From the **Local Time Zone** list, select the correct time zone option.
2. Select the **Automatically adjust clock for daylight saving changes** checkbox to enable automatic daylight saving changes.
3. Click **Apply**.

### Configuring DDNS and Access Services

In the **Device > DDNS & Device Access** page, you can:

• Configure DDNS account details in one of the supported providers.

• Configure a service that lets you remotely connect to the appliance in instances where it is behind NAT, a firewall, or has a dynamically assigned IP address.
DDNS

When you configure DDNS, the appliance updates the provider with its IP addresses. Users can then connect to the device with a host name from the provider instead of IP addresses.

This is especially important for remote access users who connect to the device to the internal network through VPN.

To configure DDNS:

1. Select Connect to the appliance by name from the Internet (DDNS).
2. Enter the details of your account on the page:
   - Provider - Select the DDNS provider that you set up an account with.
   - User name - Enter the user name of the account.
   - Password - Enter the password of the account. You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | ' " # + \n   - Host name - Enter your routable host name as defined in your DDNS account.
   For more information about these details, refer to your provider's website.
3. Make sure Reinitialize internal certificates is selected. When you enable this feature or change settings, you must reinitialize the internal certificates for them to be valid for the new DNS.

Reach My Device

Reach My Device lets you remotely connect to the appliance from the Internet so that you can use the WebUI or CLI when necessary. This is done by tunneling the administrative UI or CLI connections through a Check Point Cloud Service. Such configuration is very useful in instances where the appliance is behind a NAT device or firewall, and cannot be reached directly. In addition, the feature makes it easier to access an appliance with a dynamically assigned IP address.

To register to the Reach My Device service:

1. Click Register.
   The Reach My Device window opens.
2. For Host Name, use the default host name or enter a name for this Check Point Appliance to enable remote access.
3. If the host name was already defined, select Register with an existing homename and enter the Validation token of the gateway. This token verifies that an existing name belongs to this appliance owner.
4. Click Apply.
   The validation token, web link, and shell link are shown on the page.
5. Go to Device > Administrator Access. Configure Internet as a source for administrator access and set specified IP addresses.

When the gateway participates in VPN, you can exclude the WAN interface (or any other interface used for the Internet connection) from the encryption domain and use Reach My Device traffic without a VPN tunnel.

In the VPN Site to Site global settings Advanced Setting, enable "Do not encrypt connections originating from the local gateway."
How to access the gateway with the Reach My Device service:
When registration is complete, an outgoing tunnel to the Check Point Cloud Service is established with the appliance’s IP address.

Remote Access to the WebUI
Web Link - Use this URL in a browser to remotely access the appliance. For example: https://my gateway-web.smbrelay.checkpoint.com. When the login page shows, enter the applicable user name and password.

Remote Access to the CLI
Shell Link - Use this URL in a browser to open an SSH connection to the appliance to use CLI commands. For example: https://mygateway-shell.smbrelay.checkpoint.com. Enter the administrator credentials.

Using System Tools
See Using System Tools [on page 54].

Managing Installed Certificates
On the Installed Certificates page, you can create and manage appliance certificates or upload a P12 certificate. Uploaded certificates and the default certificates are displayed in a table. To see certificate details, click the certificate name.

You can upload a certificate signed by an intermediate CA or root CA. All intermediate and root CAs found in the P12 file are automatically uploaded to the trusted CAs list.

On the Device > Device Details page, you can select and assign a Web portal certificate from the list of installed certificates (with the exception of the Default certificate).

Installed certificates are used in the Web portal.

These are the steps to create a signed certificate:

1. Create a signing request.
2. Export the signed request (download the signing request from the appliance).
3. Send the signing request to the CA.
4. When you receive the signed certificate from the CA, upload it to the appliance.

To create a new certificate to be signed by a CA:

2. Enter a Certificate name.
3. In the Subject DN enter a distinguished name (e.g. CN=myGateway).
4. Optional - to add alternate names for the certificate, click New. Select the Type and enter the Alternate name and click Apply.
5. Click Generate.

The new signing request is added to the table and the status shows “Waiting for signed certificate”. 

Note - You cannot edit the request after it is created.

If the new signing request is signed by the Internal CA and the Organization Name is not defined in the DN, the Internal CA automatically generates the Organization Name.
To export the signing request:
Click Export.

To upload the signed certificate when you receive the signed certificate from the CA:
1. Select the signing request entry from the table.
2. Click Upload Signed Certificate.
3. Browse to the signed certificate file (*.crt).
4. Click Complete.
   The status of the installed certificate record changes from "Waiting for signed certificate" to "Verified".

To upload a P12 file:
1. Click Upload P12 Certificate.
2. Browse to the file.
3. Edit the Certificate name if necessary.
4. Enter the certificate password.
5. Click Apply.

Configuring High Availability
The Security Gateway is not part of a Security Cluster. To define it as a cluster member, define a Security Cluster object in your Security Management Server and install a security policy.

Note - A cluster in bridge in Active/Standby mode is supported in 1200R and 1400 appliances.

Configuring Advanced Settings
The Device > Advanced Settings page is for advanced administrators or Check Point support. You can configure values for multiple advanced settings for the various blades.

⚠️ Important - Changing these advanced settings without fully understanding them can be harmful to the stability, security, and performance of this appliance. Continue only if you are certain that you understand the required changes.

For further details regarding the attributes, consult with Check Point support when necessary.

To filter the list of attributes:
1. Enter text in the Type to filter field.
   The search results are dynamically shown as you type.
2. To cancel the filter, click X next to the search string.

To configure the appliance attributes:
1. Select an attribute.
2. Click Edit.
   The attribute window opens.
3. Configure the settings, or click Restore Defaults to reset the attribute to the default settings.
   For more details on some of the attributes, see the below list of attributes.
4. Click **Apply**.

   The appliance attribute is configured.

**To reset all the appliance attributes to the default settings:**

1. From the **Advanced Settings** window, click **Restore Defaults**.
   
   The **Confirm** window opens.

2. Click **Yes**.

   All appliance attributes are reset to the default settings.

**Additional Information for Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP relay</td>
<td><strong>Use internal IP addresses as source</strong> Select <strong>Use internal IP addresses as source</strong> if DHCP relay packets from the appliance will originate from internal IP addresses. This may be required if the DHCP server is located behind a remote VPN site.</td>
</tr>
<tr>
<td>Hotspot</td>
<td><strong>Enable portal</strong> Select <strong>Disabled</strong> to disable the hotspot feature entirely.</td>
</tr>
<tr>
<td>Serial port</td>
<td><strong>Enable serial port</strong> <strong>Flow control Mode</strong> <strong>Port speed</strong> With the serial port parameters you can configure the console port on the back panel of the appliance. You can disable it completely [clear the Enable serial port checkbox] if necessary and configure <strong>port speed</strong> and <strong>flow control</strong> settings. Note that these settings must match the configuration of the device connected to the console port. There are three modes for working with this port: <strong>Console</strong> - This is the default mode configured. The port is used to access the appliance’s console. <strong>Active</strong> - Instead of connecting through the port to the appliance’s console, the data is relayed to a specified telnet server which can now be viewed through this port. Enter the <strong>Server TCP port</strong> of the telnet server and the IP address of the server. Two different IP server IP addresses can be configured (Primary server and Secondary server). <strong>Passive</strong> - In this mode the flow of data is reversed and the appliance connects through the serial port to the console of the connected device. This console will be accessible through a telnet connection to a configured port on the appliance. In <strong>Listen on TPC port</strong>, enter the port number. You must manually define an access rule in the Firewall Rule Base in SmartDashboard. Two appliances, one in active mode and the other in passive mode, can allow a client to remotely connect to a console connected to the appliance in passive mode over the internet using a telnet connection.</td>
</tr>
</tbody>
</table>
Managing Users and Objects

This section describes how to set up and manage users (User Awareness, users, administrators, and authentication servers) and network resources.

Configuring Local Users and User Groups

In the **Users & Objects > Users** page you can create local users and user groups. To use these objects in the Access Policy, make sure to activate User Awareness.

User objects are used to define the different terms under which users can operate. These include:

- The time frame during which users are allowed to access the network.
- If users can work remotely.

To add a new local user:

1. Click **New > Local User**.
2. Enter a **User name**, **Password**, and **Comments** (optional). You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | ' " # + \.
3. For temporary or guest users, click **Temporary user**.
   Enter the expiration date and time.
4. To give the user remote access permissions, select **Remote Access permissions**.
5. Click **Apply**.
   The user is added to the table on the page.

To add a new local users group with remote access permissions:

1. Click **New > Users Group**.
2. Enter a **Group name**.
3. To give the group remote access permissions, select **Remote Access permissions**.
4. To select initial users to add to the group, click the relevant checkboxes from the user list or click **New** to create new users.
   You can see a summary of the group members above the user list.
5. To remove a user, click the X next to the user name.
6. Click **Apply**.
   The group is added to the table on the page.

To automatically delete expired local users:

1. Go to **Device > Advanced Settings**.
2. Select **User Management**.
3. Click **Edit**.
   The **User Management** window opens.
4. Click the checkbox for **Automatically delete expired local users**.
5. Click **Apply**.
   Expired local users are automatically deleted every 24 hours (after midnight).

**To edit a user or group:**
1. Select the user or group from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

**To delete a user or group:**
1. Select the user or group from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.
   The user or group is deleted.

**Configuring Local and Remote System Administrators**

The **Device > Administrators** page lists the Check Point Appliance administrators and lets you:
- Create new local administrators
- Configure the session timeout
- Limit login failure attempts

Administrators can also be defined in a remote RADIUS server and you can configure the appliance to allow them access. Authentication of those remotely defined administrators is done by the same RADIUS server.

**Administrator Roles:**
- **Super Administrator** - All permissions. Super Administrators can create new locally defined administrators and change permissions for others.
- **Read Only Administrator** - Limited permissions. Read Only Administrators cannot update appliance configuration but can change their own passwords or run a traffic monitoring report from the Tools page.
- **Networking Administrator** - Limited permissions. Networking Administrators can update or modify operating system settings. They can select a service or network object but cannot create or modify it.

Two administrators with write permissions cannot log in at the same time. If an administrator is already logged in, a message shows. You can choose to log in with Read-Only permission or to continue. If you continue the login process, the first administrator session ends automatically.

The correct Administrator Role must be configured to perform the operations listed below. If not, a **Permission Error** message shows.

**To create a local administrator:**
1. Click **New**.
   The **Add Administrator** page opens.
2. Configure the parameters (name, password, and password confirmation). The hyphen (-) character is allowed in the administrator name. You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | ' " # + \
3. Select the **Administrator Role**.
4. Click **Apply**.
   The name and Administrator Role is added to the table. When logged in to the WebUI, the administrator name and role is shown at the top of the page.

**To edit the details of locally defined administrators:**
1. Select the administrator from the table and click **Edit**.
2. Make the relevant changes.
3. Click **Apply**.

**To delete a locally defined administrator:**
1. Select an administrator from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

**Note** - You cannot delete an administrator who is currently logged in.

**To allow access for administrators defined in a remote RADIUS server:**
1. Make sure administrators are defined in the remote RADIUS server.
2. Make sure a RADIUS server is defined on the appliance. If there is no server, click the **RADIUS configuration** link at the top of this page. You must configure the IP address and shared secret used by the RADIUS server.
3. When you have a configured RADIUS server, click **edit permissions**.
   The **RADIUS Authentication** window opens.
4. Click the **Enable RADIUS authentication for administrators** checkbox.
   **Use roles defined on RADIUS server** is selected by default.
5. Configure the role for each user on the RADIUS server. See additional details below.
   **Note** - A user without role definition will get a login error.
6. If you select **Use default role for RADIUS users**, select the **Administrators Role**:
   - Super Admin
   - Read only
   - Networking Admin
7. To define groups, click **Use specific RADIUS groups only** and enter the RADIUS groups separated by a comma.
8. Click **Apply**.

**To set the Session Timeout value for both local and remotely defined administrators:**
1. Click **Security Settings**.
   The **Administrators Security Settings** window opens.
2. Configure the session timeout (maximum time period of inactivity in minutes). The maximum value is 999 minutes.
3. To limit login failure attempts, click the **Limit administrators login failure attempts** checkbox.
4. Enter the number of **Maximum consecutive login attempts** allowed before an administrator is locked out.
5. In **Lock period**, enter the time (in seconds) that must pass before a locked out administrator can attempt to log in again.
6. To enforce password complexity on administrators, click the checkbox and enter the number of days for the password to expire.

7. Click **Apply**.

**Note** - This page is available from the **Device** and **Users & Objects** tabs.

**Configuring a RADIUS Server for non-local Check Point Appliance users:**

Non-local users can be defined on a RADIUS server and not in the Check Point Appliance. When a non-local user logs in to the appliance, the RADIUS server authenticates the user and assigns the applicable permissions. You must configure the RADIUS server to correctly authenticate and authorize non-local users.

**Note** - The configuration of the RADIUS Servers may change according to the type of operating system on which the RADIUS Server is installed.

**Note** - If you define a RADIUS user with a null password [on the RADIUS server], the appliance cannot authenticate that user.

**To configure a Steel-Belted RADIUS server for non-local appliance users:**

1. Create the dictionary file `checkpoint.dct` on the RADIUS server, in the default dictionary directory (that contains `radius.dct`). Add these lines to the file:

   ```
   @radius.dct
   MACRO CheckPoint-VSA(t,s) 26 [vid=2620 type1=%t% len1=+2 data=%s%]
   ATTRIBUTE CP-Gaia-User-Role  CheckPoint-VSA(229, string)  r
   ATTRIBUTE CP-Gaia-SuperUser-Access  CheckPoint-VSA(230, integer)  r
   ```

2. Add the following lines to the `vendor.ini` file on RADIUS server (keep in alphabetical order with the other vendor products in this file):

   ```
   vendor-product = Check Point Appliance
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
   ```

3. Add to the `dictionary.dcm` file the line:

   ```
   "@checkpoint.dct"
   ```

4. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   ```
   CP-Gaia-User-Role = <role>
   ```

   Where `<role>` allowed values are:

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>adminrole</td>
</tr>
<tr>
<td>Read only</td>
<td>monitorrole</td>
</tr>
<tr>
<td>Networking Admin</td>
<td>networkingrole</td>
</tr>
</tbody>
</table>
To configure a FreeRADIUS server for non-local appliance users:

1. Create the dictionary file `dictionary.checkpoint` in `/etc/freeradius/` on the RADIUS server:

   ```
   # Check Point dictionary file for freeradius AAA server
   #
   VENDOR CheckPoint 2620
   ATTRIBUTE CP-Gaia-User-Role 229 string
   CheckPoint
   ATTRIBUTE CP-Gaia-SuperUser-Access 230 integer
   CheckPoint
   ```

2. Add to `/etc/freeradius/dictionary` the line:
   ```
   "$INCLUDE dictionary.checkpoint"
   ```

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

   ```
   CP-Gaia-User-Role = <role>
   ```

   Where `<role>` is the name of the administrator role that is defined in the WebUI.

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>adminrole</td>
</tr>
<tr>
<td>Read only</td>
<td>monitorrole</td>
</tr>
<tr>
<td>Networking Admin</td>
<td>networkingrole</td>
</tr>
</tbody>
</table>
To configure an OpenRADIUS server for non-local appliance users:

1. Create the dictionary file `dict.checkpoint` in `/etc/openradius/subdicts/` on the RADIUS server:

   ```
   $add vendor 2620 CheckPoint
   $set default vendor=CheckPoint
   space=RAD-VSA-STD
   len_ofs=1 len_size=1 len_adj=0
   val_ofs=2 val_size=-2 val_type=String
   nodec=0 noenc=0
   $add attribute 229 CP-Gaia-User-Role
   $add attribute 230 CP-Gaia-SuperUser-Access val_type=Integer
   val_size=4
   ``

2. Add the line
   ```
   $include subdicts/dict.checkpoint
   ```
   to `/etc/openradius/dictionaries` immediately after `dict.ascend`

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:
   ```
   CP-Gaia-User-Role = <role>
   ```
   Where `<role>` is the name of the administrator role that is defined in the WebUI.

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>adminrole</td>
</tr>
<tr>
<td>Read only</td>
<td>monitorrole</td>
</tr>
<tr>
<td>Networking Admin</td>
<td>networkingrole</td>
</tr>
</tbody>
</table>

To log in as a Super User:

A user with super user permissions can use the Check Point Appliance shell to do system-level operations, including working with the file system.

1. Connect to the Check Point Appliance platform using an SSH client or serial console client.
2. Log in to the Clish shell using your user name and password.
3. Run Expert
4. Enter the expert password.
Managing Authentication Servers

In the **Authentication Servers** page you can define and view different authentication servers where users can define both an external user database and the authentication method for users in that database.

You can define these types of authentication servers:

- **RADIUS server** - Define the details of a primary and secondary RADIUS server. The Check Point Appliance can connect to these servers and recognize users defined in them and authenticated by them.

- **Active Directory domain** - Define the details of the Active Directory domain that contains your organization’s user information. The User Awareness feature can use these details to provide seamless recognition of users for logging purposes and user based policy configuration. This can be used for VPN remote access user authentication. When this is the case, additional configuration is necessary in the [VPN > Remote Access Users](#) page.

To add a RADIUS server:

1. Click **Configure**.
2. In the Primary tab, enter this information:
   - **IP address** - The IP address of the RADIUS server.
   - **Port** - The port number through which the RADIUS server communicates with clients. The default is 1812.
   - **Shared secret** - The secret (pre-shared information used for message "encryption") between the RADIUS server and the Check Point Appliance. You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | ' " # + \n   - **Show** - Displays the shared secret.
   - **Timeout** [seconds] - A timeout value in seconds for communication with the RADIUS server. The timeout default is 3 seconds.
3. Repeat step 2 for a Secondary RADIUS server if applicable.

   **Note** - If you want to remove information you entered in IP address and shared secret, you can click **Clear**.
4. Click **Apply**.

   The primary and secondary servers (if defined) are added to the RADIUS section on the page.

RADIUS servers can be used for:

- Defining a database of users with remote access privileges. Such users are both defined and authenticated by the RADIUS server.
- Defining administrators. See the [Users & Objects > Administrators](#) page.

To edit a RADIUS server:

1. Click the IP address link of the RADIUS server you want to edit.
2. Make the necessary changes.
3. Click **Apply**.

   The changes are updated in the RADIUS server.
To delete a RADIUS server:
Click the **Remove** link next to the RADIUS server you want to delete.
The RADIUS server is deleted.

To configure remote access permissions for users defined in the RADIUS server:
1. Click **permissions for RADIUS users**.
2. Select or clear the **Enable RADIUS authentication for remote access users** checkbox.
3. When selected, choose which users are given remote access permissions:
   - To allow all users defined in the RADIUS server to authenticate - Select **All users defined on RADIUS server**
   - Specific user groups defined in the RADIUS server - Select **For specific RADIUS groups only** and enter in the text field the names of the user groups separated by commas.
   - To allow administrators with Read-only permissions to authenticate - Select **Read-only Administrators**
4. Click **Apply**.

To add an Active Directory domain:
1. In the Active Directory section, click **New**.
The Add new Domain window opens.
2. Enter this information:
   - **Domain** - The domain name.
   - **IP address** - The IP address of one of the domain controllers of your domain.
   - **User name** - The user must have administrator privileges to ease the configuration process and create a user based policy using the users defined in the Active Directory.
   - **Password** - The user’s password. You cannot use these characters when you enter a password or shared secret: { } [ ] ` ~ | ' " # + \ 
   - **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually. For example: CN=John James,OU=RnD,OU=Germany,O=Europe,DC=Acme,DC=com
3. Select **Use user groups from specific branch only** if you want to use only part of the user database defined in the Active Directory. Enter the branch in the Branch full DN in the text field.
4. Click **Apply**.

When an Active Directory is defined, you can select it from the table and choose **Edit** or **Delete** when necessary.

When you edit, note that the Domain information is read-only and cannot be changed.

When you add a new Active Directory domain, you cannot create another object using an existing domain.
To configure remote access permissions for all users defined in Active Directory:

By default, users defined in the Active Directory are not given remote access permissions. Instead, in the **VPN > Remote Access Users** page all users defined locally or in Active Directories can be selected to be granted remote access permissions per user.

1. Click permissions for Active Directory users.
2. Select *All users in the Active Directory*. With this option, it is not necessary to go to the **VPN > Remote Access Users** page and select specific users.

   Note that most Active Directories contain a large list of users and you might not want to grant them all remote access permissions to your organization. Usually you keep the *Selected Active Directory user groups* option and configure remote access permissions through **VPN > Remote Access Users** page.

3. Click Apply.

To change synchronization mode with the defined Active Directories:

1. Click **Configure** in the toolbar of the Active Directory table.
2. Select one of the options - *Automatic synchronization* or *Manual synchronization*. When Manual synchronization is selected, you can sync the user database known to the appliance in all locations that this user database can be viewed. For example, the **Users & Objects > Users** page or the Source picker in the Firewall Rule Base in the **Access Policy > Firewall Policy** page.

3. Click Apply.

To edit an Active Directory:

1. Select the Active Directory from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

To delete an Active Directory:

1. Select the Active Directory from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

   The Active Directory is deleted.

*Note* - This page is available from the **VPN** and **Users & Objects** tabs.

**Managing System Services**

The **Users & Objects > Services** page lists the system services configured in the system. In this page you can add new services, edit services, and delete services.

You use service objects to easily define the different network protocols. This is usually with IP protocol and ports (used by the TCP and UDP IP protocols).

You can use these objects to define policy based routing in the **Device > Routing** page.
To create a new service:
1. Click New.
2. In the Service tab, enter information in the fields that apply to the type of service you select. Note that not all fields may show:
   - **Name** - Enter the service’s name.
   - **Type** - Select the service type from the list:
     - **TCP**
     - **UDP**
     - **ICMP** - Select this option if it is necessary to represent a specified option in the ICMP protocol. Note that this is an advanced option.
     - **Other** - Select this option to represent any IP protocol other than TCP or UDP.
   - **Ports** - Enter the port(s) if you selected Type - TCP or UDP. Port numbers and/or ranges can be entered by separating with commas.
   - **IP Protocol** - Enter the IP protocol if you selected Type - Other.
   - **ICMP type** and **ICMP code** - Enter the ICMP type and code that you want the service object to represent as listed in RFC 792. This option is only relevant if you selected Type - ICMP.
   - **Comments** - Enter an optional comment.
   - **Disable inspection for this service** – Select this checkbox to disable deep inspection of traffic matching this service. This option is only available for built-in services.
3. Click Apply.

To edit a service:
1. Select a service from the list.
2. Click Edit.
3. Make the necessary changes. Note that not all fields can be edited.
4. Click Apply.

To delete a service:
1. Select the service from the list. Note that you can only delete a user defined service.
2. Click Delete.
3. Click Yes in the confirmation message.

To filter for a specified service:
1. In the Type to filter box, enter the service name or part of it.
2. As you enter text, the list is filtered and shows matching results.

Managing Service Groups

The Users & Objects > Service Groups page lists the service groups defined in the system. In this page you can add new service groups, and edit or delete existing service groups.

There are built in service groups for common services.
To create a new service group:

1. Click **New**.
   The New Service Group window opens.
2. Enter a **Name** for the group and **Comments** (optional).
3. Click **Select** to show the full list of available services and select the relevant checkboxes.
4. Click **New** if the existing list does not contain the services you need. For information on creating a new service object, see the **Users & Objects > Services** page.
5. Click **Apply**.
   The New Service Group window opens and shows the services you selected.
6. You can also click **New** from the New Service Group window.
7. To remove a service object from the group list, select it and click **Remove**.
8. Click **Apply**.
   The service group is added to the list of groups.

To edit a service group:

1. Select a group from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**.

To delete a service group:

1. Select the group from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

To filter for a specified service group:

1. In the **Type to filter** box, enter the service group name or part of it.
2. As you enter text, the list is filtered and shows matching results.

**Managing Network Objects**

The **Users & Objects > Network Objects** page lists the network objects defined in the system. In this page you can add new network objects, edit network objects, and delete network objects. In most cases, the most common use for these objects is to define a security policy and exceptions to it. These objects can be used as hosts for the internal DNS service and their IP addresses can be configured as fixed for the internal DHCP service.

These are the available network object types:

- **Single IP** - A network object that represents a device with a single IP address.
- **IP Range** - A network object that represents a range of IP addresses.
- **Network** - A network object that represents a network.
To create a Single IP network object:
1. Click **New**.
   The New Network Object window opens.
2. In **Type**, select **Single IP**.
3. Enter an **IP address** and **Object name**.
4. Select or clear these options as necessary:
   - **Allow DNS server to resolve this object name** - When the gateway is the DNS server for your internal networks, the name of the server/network object is translated to its IP address.
   - **Exclude from DHCP service** - The internal DHCP service does not distribute the configured IP address of this server/network object to anyone.
     - **Reserve IP address in DHCP service for MAC** - The internal DHCP service distributes the configured IP address only to this server/network object based on its MAC address.
     - **Enter the MAC address** - This is required for IP reservation. When you create the object from the **Active Devices** page, the MAC address is detected automatically.
5. Click **Apply**.

To create an IP Range network object:
1. Click **New**.
   The New Network Object window opens.
2. In **Type**, select **IP Range**.
3. In the **Start IP** and **End IP** fields, enter the IP addresses that represent the start of the IP range and end of the IP range.
4. Enter the **Object name**.
5. Select or clear this option as necessary:
   - **Exclude from DHCP service** - The internal DHCP service does not distribute the configured IP range to anyone.
6. Click **Apply**.

To create a Network type network object:
1. Click **New**.
   The New Network Object window opens.
2. In **Type**, select **Network**.
3. Enter a **Network address** and **Subnet mask**.
4. Enter the **Object name**.
5. Click **Apply**.

To edit a network object:
1. Select a network object from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**.
To delete a network object:
1. Select the network object from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

To filter for a specified network object:
1. In the **Type to filter** box, enter the name of the network object or part of it.
2. As you enter text, the list is filtered and shows matching results.

**Managing URL Lists**

The **Users & Objects > URLs Lists** page lets you override central management’s URL filtering policy in your local Check Point Appliance. Use this feature to define URL blacklists and whitelists exceptions to the global policy, whose content can be edited per gateway. Before you use this feature, the system administrator of the Security Management Server that centrally manages this gateway must complete prerequisite steps.

You can use this page to manage URLs lists:

- Add new URLs/IP addresses or regular expressions to URLs lists.
- Edit existing URLs/IP addresses or regular expressions from URLs lists.
- Delete existing entries in URLs lists.
- Enable and disable this feature.

**Prerequisite steps for the system administrator of the Security Management Server:**

1. Turn on the Application Control blade for the gateway object that represents this Check Point Appliance.
2. Configure custom applications in SmartDashboard with these guidelines:
   a) Use the prefix: LOCAL_ (case-sensitive) when naming a custom application. For example, LOCAL_whitelist or LOCAL_blacklist.
   b) Enter at least one URL for this custom application, it can be a dummy URL. The actual list of URLs to allow or block is defined locally in the Check Point Appliance.
3. Create rules in the Application Control Rule Base using the custom defined applications with the LOCAL_ prefix. Make sure to add the rules in positions that make sense in the Rule Base.
4. Install policy (on the specified gateway).

**Steps for the system administrator of this Check Point Appliance:**

1. On this page, set **Local URLs Lists Management** to **ON**.
2. Add URLs/IP addresses or regular expressions to the predefined URLs lists (the custom applications defined in Security Management Server).
   
   **Note** - The names of the predefined URLs lists does NOT show the LOCAL_ prefix that was used to define the application in Security Management Server. For example, LOCAL_whitelist is shown as just whitelist.
Important -

- If Application Control is turned off or no custom applications have been defined in the Security Management Server, this page is empty and shows a message that informs that local URLs can only be defined after URLs lists are predefined in the appliance's security policy.
- If a list was removed or renamed in the Security Management Server, a warning shows above the table and next to the URLs List in the table.

To create a new URLs list entry:

1. Click **New**.
2. Select **URL/IP Address** or **Regular Expressions**.
   - The New URL/IP Address or New Regular Expressions window opens.
3. Select the applicable **URLs list** from the list.
4. Enter a **URL/IP Address** or a **regular expression** for the URLs list.
5. Click **Apply**.
   - The URL is added to the list of entries for the specified URLs list in the table.

To edit a URLs list entry:

1. Select an entry from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**.

To delete a URLs list entry:

1. Select an entry from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

To filter for a specified URLs list:

Do one of these:

- In the **All Lists** box, select the URLs list.
- In the **Type to filter** field, enter the URLs list name to shows matching results.
Logs and Monitoring

This section describes the security and system logs. It also describes various monitoring tools.

Viewing Security Logs

The Logs & Monitoring > Security Logs page lets you browse the last 100 log records.

These logs are sent to SmartView Tracker, but are also available on this page. Note that the number of logs shown is not configurable, and is not related to the SmartDashboard setting “GW properties > Logs and alert > Max log size...” (This setting only applies to logs that are saved by the gateway when the Security Management Server cannot be reached).

To search for a security log:
Enter your query in the Enter search query box.

Use this syntax:
<IP_address>
or
<column_name>:<value>

For example:
203.0.113.64
or
action:drop
or
source_port:22

For more details, click Query Syntax in the table header.

To see the security log record:
1. Select a log entry from the list.
2. Click View Details or double-click the entry.
The log record opens.

To refresh the security log data:
Click the refresh icon.

To stop local logging:
You can stop local logging to remove the overhead to create and maintain logs to improve performance. No new logs are generated until you set the resume option.

1. Select Options > Stop local logging.
2. To resume, select Options > Resume local logging.

Logs can be stored centrally or locally. Logs can be stored locally on the appliance’s non-persistent memory or on an external SD card (persistent). When you insert an SD card, it mounts automatically and then local logs are saved to it. Before you eject an SD card, make sure to unmount it. Select Options > Eject SD card safely.
To export the log:
1. Go to Logs & Monitors > External Log Servers.
2. Under Syslog Servers, click Configure.
3. In the Syslog Server window that opens, enter the Name and IP address. Make sure Enable log server is selected.
4. Click Apply.
5. Select which logs to export.

You can add more syslog servers or edit existing syslog servers in the same menu.

To delete logs from local log storage:
   A confirmation window opens.
2. Click Yes to delete logs.
   The logs are deleted, and the logs grid reloads automatically.

   Note - Logs are deleted from the external SD card (if inserted) or from the local logs storage. Logs are not deleted from the remote logs server.

Viewing System Logs
The Logs & Monitoring > System Logs page shows up to 500 systems logs (syslogs) generated from the appliance at all levels except for the debug level. These logs should be used mainly for troubleshooting purposes and can also give the administrator notifications for events which occurred on the appliance.

These are the syslog types:
- Info – Informative logs such as policy change information, administrator login details, and DHCP requests.
- Notice – Notification logs such as changes made by administrators, date, and time changes.
- Warning – Logs that show a connectivity or possible configuration failure. The problem is not critical but requires your attention.
- Error – System errors that alert you to the fact that a specific feature is not working. This can be due to misconfiguration or connectivity loss which requires the attention of your Internet Service Provider.

To download the full log file:
1. Click Download Full Log File.
2. Click Open or Save.

To save a snapshot of the syslogs to the flash disk:
1. Select Save a snapshot of system logs to flash.
2. Enter a minute value for the interval. The default is 180 minutes (3 hours). The minimum value is 30 minutes.
3. Click Apply.

This is an effort to keep syslogs persistent across boot, but not 100% guaranteed.
To refresh the system logs list:
Click **Refresh**. The list is refreshed.

To clear the log list:
1. Click **Clear Logs**.
2. Click **OK** in the confirmation message.

**Configuring External Log Servers**

The **Logs & Monitoring > Log Servers** page lets you configure external log servers for system logs when necessary for additional logging storage.

You can configure a gateway to send logs to multiple external syslog servers.

**To configure an external syslog server:**
1. Under **Syslog Servers**, click **Configure**.
   The External Syslog Server window opens.
2. Enter **Name**.
3. Enter the **IP address**.
4. Enter the **Port**.
5. Click **Enable log server**.
6. Click **Apply**.

**Managing Active Devices**

See Managing Active Devices (on page 50).

**Viewing Infected Hosts**

In the **Infected Hosts** page you can see information about infected hosts and servers in the internal networks. You can also directly create an exception rule for a specified protection related to an infected or possibly infected host or server.

The Infected Hosts table shows this information for each entry:

- **Icon** - Shows icons for the different classifications of infected hosts and servers:

<table>
<thead>
<tr>
<th>Description</th>
<th>Host Icon</th>
<th>Server Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infected host or server - When the Anti-Bot blade detects suspicious communication between the host or server and an external Command &amp; Control center due to a specified triggered protection.</td>
<td>![Infected Host Icon]</td>
<td>![Infected Server Icon]</td>
</tr>
<tr>
<td>Possibly infected host or server - When the Anti-Virus blade detects an activity that <em>may</em> result in host or server infection. For example:</td>
<td>![Possibly Infected Host Icon]</td>
<td>![Possibly Infected Server Icon]</td>
</tr>
<tr>
<td>- When you browse to an infected or a potentially unsafe Internet site, there is a possibility that malware was installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- When you download an infected file, there is a possibility that the file was opened or triggered and infected the host or server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object name - Shows the object name if the host or server was configured as a network object.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- IP/MAC address
- Device/User Name - Shows a device or user name if the information is available to the Check Point Appliance through DHCP or User Awareness.
- Incident type - Shows the detected incident type:
  - Found bot activity
  - Downloaded a malware
  - Accessed a site known to contain malware
- Severity - Shows the severity of the malware:
  - Low
  - Medium
  - High
  - Critical
- Protection name - Shows the Anti-Bot or Anti-Virus protection name.
- Last incident - The date of the last incident.
- Incidents - Shows the total number of incidents on the host or server in the last month. If there is a large amount of records, the time frame may be shorter.

To filter the infected hosts list:
1. Click Filter.
2. Select one of the filter options:
   - Servers only - Shows only machines that were identified as servers (and not any machine/device). Servers are defined as server objects in the system from the Access Policy > Servers page.
   - Possibly infected only - Shows only hosts or servers classified as possibly infected.
   - Infected only - Shows only hosts or servers classified as infected.
   - High and above severity only - Shows hosts and servers that are infected or possibly infected with malwares that have a severity classification of high or critical.

To add a malware exception rule for a specified protection:
1. Select the list entry that contains the protection for which to create an exception.
2. Click Add Protection Exception.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the exception rule fields.
   - Scope - Select either Any or a specific scope from the list. If necessary, you can create a New network object, network object group, or local user. If it is necessary to negate a specified scope, select the scope and select the Any Scope except checkbox. For example, if the scope of the exception should include all scopes except for the DMZ network, select DMZ network and select the Any Scope except checkbox.
   - Action - Select the applicable action to enforce on the matching traffic: Ask, Prevent, Detect or Inactive. See the Threat Prevention > Threat Prevention Blade Control page for a description of the action types.
   - Log - Select the tracking option: None, Log, or Alert. Logs are shown on the Logs & Monitoring > Security Logs page. An alert is a flag on a log. You can use it to filter logs.
4. Optional - Add a comment in the Write a comment field.
5. Click Apply.
   The rule is added to Malware Exceptions on the Threat Prevention > Exceptions page.

To view the logs of a specified entry:
1. Select the list entry for which to view logs.
2. Click Logs.
   The Logs & Monitoring > Security Logs page opens and shows the logs applicable to the IP/MAC address.
   Note - This page is available from the Home and Logs & Monitoring tabs.

Viewing VPN Tunnels
In the VPN Tunnels page you can see current VPN tunnels opened between this gateway and remote sites. Some sites are configured so tunnels are established only when necessary and some are configured with permanent tunnels. When the appliance is managed by Cloud Services, this table also shows the tunnels for the gateways in the community.
This page is commonly used to see the permanent tunnels. The table shows each tunnel’s details when there is an active VPN tunnel.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Host name or IP address of the tunnel’s source gateway.</td>
</tr>
<tr>
<td>Site Name</td>
<td>Name of the VPN site name.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>Host name or IP address of the tunnel’s destination gateway.</td>
</tr>
<tr>
<td>Community Name</td>
<td>If the gateways are part of a community configured by Cloud Services, this column shows the community name with which the tunnel is associated.</td>
</tr>
<tr>
<td>Status</td>
<td>VPN tunnel status indication.</td>
</tr>
</tbody>
</table>

To filter the list:
In the Type to filter box, enter the filter criteria.
The list is filtered.

To refresh the list:
Click Refresh to manually refresh this page with updated tunnel information.
Note - This page is available from the VPN and Logs & Monitoring tabs.
Viewing Active Connections

The Logs & Monitoring > Connections page shows a list of all active connections. The list shows these fields:

- Protocol
- Source Address
- Source Port
- Destination Address
- Destination Port

To filter the list:
In the Type to filter box, enter the filter criteria. The list is filtered.

To refresh the list:
Click the Refresh link.

Viewing Monitoring Data

See Viewing Monitoring Data (on page 51).

Viewing Reports

See Viewing Reports (on page 53).

Using System Tools

See Using System Tools (on page 54).

SNMP

In the Logs & Monitoring > SNMP page you can configure SNMP settings for this gateway. You can do these actions:

- Turn the SNMP agent on or off
- Configure SNMP settings (system location, system contact, and community string for SNMP v1 and v2 authentication)
- Add SNMP v3 users
- Configure the settings for SNMP Trap receivers
- Enable or disable SNMP traps that are sent to the trap receivers

To turn SNMP on or off:

1. Change the SNMP On/Off slider position to ON or OFF.
2. Click Apply.

SNMP must be set to on to configure all SNMP settings (users, traps, and trap receivers).
To configure SNMP settings:

Click **Configure**.

The Configure SNMP General Settings window opens. You can enable SNMP traps, configure system location and contact details, and enable SNMP versions in addition to v3.

**SNMP v3 Users**

- To add a new SNMP v3 user, click **New**.
- To edit an existing SNMP v3 user, select the user from the list and click **Edit**.
- To delete an SNMP v3 user, select the user from the list and click **Delete**.

**SNMP Traps Receivers**

You can add, delete, or edit the properties of SNMP trap receivers.

- To add an SNMP trap receiver, click **New**.
  
  **Note** - To add a new SNMP v3 trap receiver, there must be an SNMP v3 user defined for it.
- To edit an existing SNMP trap receiver, select the trap receiver from the list and click **Edit**.
- To delete an SNMP trap receiver, select the trap receiver from the list and click **Delete**.

**SNMP Traps**

You can enable or disable specified traps from the list and for some traps set a threshold value. The enabled traps are sent to the receivers.

**To edit an SNMP trap:**

1. Select the trap from the list and click **Edit**.
2. Select the **Enable trap** option to enable the trap or clear it to disable the trap.
3. If the trap contains a **value**, you can edit the threshold value when necessary.
4. Click **Apply**.
Advanced Configuration

In This Section:

- Dynamic Routing ............................................................................................... 117
- Upgrade Using a USB Drive ............................................................................... 118
- Upgrade Using an SD Card ................................................................................ 120
- Boot Loader ..................................................................................................... 121
- Upgrade Using Boot Loader ............................................................................... 121
- Restoring Factory Defaults .............................................................................. 122

Dynamic Routing

Dynamic Routing is supported with Gaia networking stacks. RIP, OSPF, BGP, and PIM are supported.

**Note** - Configuration is only supported through the CLI.

This is a sample OSPF interface configuration:

```plaintext
set ospf
area <backbone | ospf_area> range ip_prefix <on | off>
area <backbone | ospf_area> range ip_prefix restrict <on | off>
stub-network ip_prefix <on | off>
stub-network ip_prefix stub-network-cost <1-677722>

set ospf interface if_name
area <backbone | ospf_area> <on | off>
hello-interval <1-65535>
hello-interval default
dead-interval <1-65535>
dead-interval default
retransmit-interval <1-65535>
retransmit-interval default
cost <1-65535>
priority <0-255>
passive <on | off>
virtual-address <on | off>
authype none
simple password
md5 key authorization key id secret md5 secret
md5 key authorization key id
```

See the *Gaia Advanced Routing Administration Guide* for more information.

**Note** - The `save config` and `route map` commands are not supported.
Upgrade Using a USB Drive

This section explains how you can upgrade the appliance with a USB drive without a console connection to the appliance. For more information, see Upgrade Using Boot Loader (on page 121).

**Note** - The USB drive must be formatted in FAT32.

### Installing a new firmware image from a USB drive

Check Point releases new firmware images every so often. You can reburn the appliance using the image file and a USB drive. Note that you can also upgrade through the WebUI. If the new image supports it, you do not lose your previous settings. When you reburn a new image with a USB drive, the appliance deletes your previous settings and creates a new factory default image.

**For 1200R appliances:**

**To upgrade to a new firmware image from a USB drive:**

1. Disconnect the Check Point Appliance from the power source.
2. Place the firmware image file on a USB drive in the top folder. Do not rename the file.
3. Make sure the top folder of the USB drive does not contain any previous Boot loader or Firmware images (u-boot*.ubt files or fw1*.img files).
4. Connect the USB drive to one of the USB ports on the Check Point Appliance. If the operation does not succeed, this may be because the USB port does not recognize all USB drives. Some USB drives also use a different file system and those are not supported.
5. Connect the appliance to the power source. The appropriate USB LED lights and blinks several times as it recognizes the file and uploads it to the appliance. The LED turns off when the file uploads. This takes several seconds.
   - If the file is valid, all LAN LEDs start to blink to show progress. Every other LED blinks at a different speed. Link LEDs blink orange and Activity LEDs blink green.
   - When the installation is complete, all LAN LEDs turn a constant green. The appliance is ready for your input.
6. Remove the USB drive and disconnect the appliance from the power source.
7. Reconnect the appliance to the power source. Allow the appliance to boot successfully. The first boot after an image reburn takes more time than a normal boot. Wait patiently for the Notice LED to stop blinking (this indicates that the boot is complete).
   - As this operation has removed your previous settings, refer to the *Getting Started Guide* and reconfigure your appliance with the First Time Configuration Wizard.
   - **Note** - When you upgrade with a USB drive, you also replace the saved factory default image of the appliance as this method reburn the appliance.

### Installing a new Boot-Loader from a USB drive

Check Point releases new Boot Loader rarely. This usually comes with a new image. To upgrade to a new U-Boot or Firmware image, you must boot the appliance.

Replace the Boot Loader before you upgrade to a new image.

**To replace Boot-Loader:**

1. Disconnect your Check Point Appliance from the power source.
2. Place the Boot loader file on a USB drive in the top folder. Do not rename the file.
3. Make sure the top folder of the USB drive does not contain any previous Boot loader or Firmware images (u-boot*.ubt files or fw1*.img files).

4. Connect the USB drive to one of the appliance USB ports. If the operation does not succeed, this may be because the USB port does not recognize all USB drives. Some USB drives also use a different file system and those are not supported.

5. Connect the appliance to the power source. The appropriate USB LED lights and blinks several times as it recognizes the file and uploads it to the appliance. The LED turns off when the file uploads. This takes several seconds.
   - If the file is valid, all LAN LEDs start to blink to show progress. Every other LED blinks at a different speed. Link LEDs blink orange and Activity LEDs blink green.
   - When the installation is complete, all LAN LEDs turn a constant green. The appliance is ready for your input.

6. Remove the USB drive and disconnect the appliance from the power source.

7. If you need to install a new firmware image, refer to the firmware image installation section before you reconnect the appliance to the power source.

For 1400 appliances

To upgrade to a new firmware image from a USB drive:

1. Disconnect the Check Point Appliance from the power source.

2. Place the firmware image file on a USB drive in the top folder. Do not rename the file.

3. Make sure the top folder of the USB drive does not contain any previous Boot loader or Firmware images (u-boot*.bin files, or fw1*.img files).

4. Connect the USB drive to the USB port on the Check Point Appliance.

5. Connect the appliance to the power source.
   - After a few seconds, the Notice LED blinks until the system boots. When the system is up, the USB LED is on. After the system boot is complete, it checks the image version on the USB.
   - If the file is valid, the LAN LEDs start to blink until the file is uploaded. After a few seconds, all of the LAN LEDs are on and the system reboots. When the Notice LED is off, the installation is complete and the appliance awaits your input.

6. Remove the USB drive.

7. As this operation has removed your previous settings, refer to the Getting Started Guide and reconfigure your appliance with the First Time Configuration Wizard.

**Note** - When you upgrade with a USB drive, you also replace the saved factory defaults image of the appliance as this method reboots the appliance.

**Note** - Uboot update from a USB drive is currently not supported in 1400 appliances.
Upgrade Using an SD Card

You can use an SD card to upgrade to a new firmware image or auto-configuration file. When you install a new image with an SD card, the appliance deletes your previous settings and creates a new factory default image. Back up your settings so you can restore them after the installation is complete.

**Note** - The SD card must be formatted to FAT32.

**To upgrade to a new firmware image from an SD card:**

1. Disconnect the Check Point Appliance from the power source.
2. Place the firmware image on the SD card in the top folder. Do not rename the file.
   Make sure the top folder of the SD card does not contain any previous Boot loader or firmware images (u-boot*.bin files or fw1*.gz files).
3. Insert the SD card into the SD card slot on the Check Point Appliance. If the operation does not succeed, this may be because the SD card slot does not recognize all devices.
4. Connect the appliance to the power source.

The installation begins with the image file. This takes several minutes.

If the file is valid, all LAN LEDs start to blink to show progress. The LEDs are different colors and blink at different speeds.

<table>
<thead>
<tr>
<th>LEDs</th>
<th>Colors</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN LEDs</td>
<td>Orange and green</td>
</tr>
<tr>
<td>Link LEDs</td>
<td>Orange</td>
</tr>
<tr>
<td>Activity LEDs</td>
<td>Green</td>
</tr>
</tbody>
</table>

When the installation is complete, all LAN LEDs turn a constant green. The appliance is ready for your input.

Restore your settings. For more information, see Backup, Restore, Upgrade, and Other System Operations ("Using the Software Upgrade Wizard" on page 82).

**To upgrade using CLIsh commands:**

These are the file names that you can use:

- `autoconf.clish`
- `autoconf.<MAC address>.clish`
  
  `<MAC address>` is the specified MAC address in this format: `XX-XX-XX-XX-XX`

You can create multiple configuration files for Check Point Appliance gateways. The gateways run both files or only one of them. First the `autoconf.clish` configuration file is loaded. If there is a configuration file with the same MAC address as the gateway, that file is loaded second.

Use the `#` symbol to add comments to the configuration file.
Boot Loader

The Gaia Embedded Boot Menu shows during boot and is available if you press Ctrl+C while the appliance boots if you have a console connection. The menu contains the available options.

1. Start in normal Mode
2. Start in debug Mode
3. Start in maintenance Mode
4. Restore to Factory Defaults (local)
5. Install/Update Image/Boot-Loader from Network
6. Restart Boot-Loader
7. Run Hardware diagnostics
8. Install DSL Firmware / Upload preset configuration file

Please enter your selection:

When you are in Boot Loader, all interfaces are down and you can only activate them for options that require connectivity. At this point Check Point’s services are not active.

Options 1-3 start the appliance.

- Normal mode is the default boot mode for the appliance.
- Debug mode boot gives printouts of processes that are initialized during boot.
- Maintenance mode boots the machine and gives access only to the file system (network interfaces, Check Point processes and the appliance’s services are down).

**Note** - During normal/debug boot, if there is an error and the appliance cannot boot properly, it reverts to maintenance mode and the Power LED turns a constant red.

Options 4-5 are explained in the subsequent sections.

Option 6 restarts the appliance.

Option 8 installs new firmware for the DSL modem (supported in DSL models only) or uploads a preset configuration file.

Upgrade Using Boot Loader

To upgrade the Check Point Appliance using U-boot (boot loader):

**Note** - In 1470/1490 and 1200R appliances, Bootloader is supported only through the DMZ port and is not available through the LAN ports.

1. Connect to the appliance with a console connection (use the serial console connection on the back panel of the appliance), boot the appliance and press Ctrl+C. The Gaia Embedded Boot Menu is shown.
2. Press 5 to select Install/Update Image/Boot-Loader from Network.
3. You are asked if you want to manually load the image from a TFTP server, or if you want to use automatic mode with a bootp server.
4. If you select manual mode, you are asked to fill in the IP of the Check Point Appliance, the IP of the TFTP server, and the image name.
5. If you select automatic mode, the procedure starts automatically to search for the bootp server.
6. While in menu mode, press Ctrl+C again to return to the Boot Loader menu.
During the upgrade, all LAN Link and Activity LEDs blink orange and green alternately to indicate progress. This takes up to a minute.

When all LAN Link and Activity is successfully completed, the LEDs light in green, and the appliance waits for you to press a key. Error in the upgrade process is indicated by all LAN Link and Activity LEDs blinking red.

Restoring Factory Defaults

The Check Point Appliance contains a default factory image. When the appliance is turned on for the first time, it loads with the default image.

As part of a troubleshooting process, you can restore the Check Point Appliance to its factory default settings if necessary.

You can restore a Check Point Appliance to the factory default image with the WebUI, Boot Loader, or a button on the back panel.

⚠️ **Important** - When you restore factory defaults, you delete all information on the appliance and it is necessary to run the First Time Configuration Wizard.

To restore factory defaults with the WebUI:

1. In the Check Point Appliance WebUI, click **Device > System Operations**. The System Operations pane opens.
2. In the Appliance section, click **Factory Defaults**.
3. In the pop-up window that opens, click **OK**.
4. While factory defaults are restored, all LAN Link and Activity LEDs blink orange and green alternately to show progress.
   This takes some minutes. When this completes, the appliance reboots automatically.

To restore factory defaults with the button on the back panel:

1. Press the Factory Default button with a pin. Hold for at least
   1400 appliances - 12 seconds.
   1200R - 3 seconds.
2. When the Power and Notice LEDs are lit red, release the button. The appliance reboots itself and starts to restore factory defaults immediately.
3. While factory defaults are restored, all LAN Link and Activity LEDs blink orange and green alternately to show progress.
   This takes some few minutes. When this completes, the appliance reboots automatically.

**1200R appliances:**

To restore the Check Point Appliance to its default factory configuration using U-boot (boot loader):

1. Connect to the appliance with a console connection (use the serial console connection on the back panel of the appliance).
2. Boot the appliance and press Ctrl-C.
   The Gaia Embedded Boot Menu is shown.
Welcome to Gaia Embedded Boot Menu:
1. Start in normal Mode
2. Start in debug Mode
3. Start in maintenance Mode
4. Restore to Factory Defaults (local)
5. Install/Update Image/Boot-Loader from Network
6. Install/Update Image from USB
7. Install/Update Boot-Loader from USB
8. Restart Boot-Loader

Please enter your selection:

3. Enter 4 to select **Restore to Factory Defaults (local)**.

4. When you are prompted: “Are you sure? [y/n]” select y to continue and restore the appliance to its factory defaults settings.

   While factory defaults are restored, all LAN Link and Activity LEDs blink orange and green alternately to indicate progress. This takes up to a few minutes. When completed, the appliance boots automatically.

**1400 appliances:**

To restore the Check Point Appliance to its default factory configuration using U-boot (boot loader):

1. Connect to the appliance with a console connection (use the serial console connection on the back panel of the appliance).

2. Boot the appliance and press **Ctrl-C**.

   The Gaia Embedded Boot Menu is shown.

   Welcome to Gaia Embedded Boot Menu:
   1. Start in normal Mode
   2. Start in debug Mode
   3. Start in maintenance Mode
   4. Restore to Factory Defaults (local)
   5. Install/Update Image/Boot-Loader from Network
   6. Restart Boot-Loader
   7. Run Hardware diagnostics
   8. Install DSL Firmware/Upload preset configuration file

   Please enter your selection:

3. Enter 4 to select **Restore to Factory Defaults (local)**.

4. When you are prompted: “Are you sure? [y/n]” select y to continue and restore the appliance to its factory defaults settings.

   While factory defaults are restored, all LAN Link and Activity LEDs blink orange and green alternately to indicate progress. This takes up to a few minutes. When completed, the appliance boots automatically.
To disable the reset to default:
Use this CLI command:
> set additional-hw-settings reset-timeout 0

To enable the reset to default:
Use this CLI command:
> set additional-hw-settings reset-timeout 12
Creating the Security Policy • 17
D
Defining a Gateway Cluster Object • 13
Defining a Gateway Object • 10
Defining a SmartLSM Appliance Cluster Profile • 23
Defining a SmartLSM Gateway Profile for a Large-scale Deployment • 23
Defining SmartLSM Gateways Using LSM CLI • 32
Deploying from a USB Drive or SD Card • 40
Deploying the Configuration File - Existing Configuration • 41
Deploying the Configuration File - Initial Configuration • 41
Deploying with SmartProvisioning • 24
Deployment Types • 9
Dynamic Routing • 117
F
Finish • 30, 31
First Time Deployment Options • 38
G
General Properties • 28, 30
I
Important Information • 3
Installation • 8
Installing a Security Policy • 19, 25
Introduction to the WebUI Application • 45
L
Large-scale Deployment Installation • 22
Large-scale Deployment Workflow • 22
Logs and Monitoring • 110
M
Managing Active Devices • 50, 112
Managing Authentication Servers • 102
Managing Date and Time • 91
Managing Device Details • 90
Managing Device Settings • 32
Managing Installed Certificates • 93
Managing Licenses • 49
Managing Network Objects • 106
Managing Service Groups • 105
Managing System Services • 104
Managing the Device • 56
Managing URL Lists • 108
Managing Users and Objects • 96
More Information • 28, 31
P
Predefining a Centrally Managed Deployment • 9
Preparing the Configuration Files • 41

About the PoE • 9
Advanced Configuration • 117
Appliance Configuration • 45
Backing up the System • 83
Backup, Restore, Upgrade, and Other System Operations • 80
Boot Loader • 121
Check Point 1200R and 1400 Appliance Overview • 7
Cluster Interface Configuration • 15
Cluster Names • 31
Cluster Properties • 30
Communication Properties • 31
Communication Properties • 29
Configuration File Error • 42
Configuring a Configuration Script • 36
Configuring a Hotspot • 72
Configuring a Provisioning Profile • 36
Configuring Administrator Access • 89
Configuring Advanced Settings • 94
Configuring DDNS and Access Services • 91
Configuring External Log Servers • 112
Configuring Firmware • 32
Configuring High Availability • 94
Configuring Hotspot • 35
Configuring Internet Connectivity • 56
Configuring Local and Remote System Administrators • 84, 97
Configuring Local Users and User Groups • 96
Configuring MAC Filtering • 77
Configuring RADIUS • 34
Configuring the Check Point Appliance Gateways • 14
Configuring the Cluster Object in SmartDashboard • 14
Configuring the DNS Server • 79
Configuring the Local Network • 64
Configuring the Proxy Server • 80
Configuring the Routing Table • 74
Configuring the Wireless Network • 61
Connecting the Cables • 8
Controlling and Monitoring Software Blades • 46
Converting an Existing Check Point Appliance to a Cluster • 16
Creating a Cluster for New Gateways • 13
Creating a Gateway • 28
Creating a SmartLSM Appliance Cluster • 30
Creating the Security Policy • 17
Defining a Gateway Cluster Object • 13
Defining a Gateway Object • 10
Defining a SmartLSM Appliance Cluster Profile • 23
Defining a SmartLSM Gateway Profile for a Large-scale Deployment • 23
Defining SmartLSM Gateways Using LSM CLI • 32
Deploying from a USB Drive or SD Card • 40
Deploying the Configuration File - Existing Configuration • 41
Deploying the Configuration File - Initial Configuration • 41
Deploying with SmartProvisioning • 24
Deployment Types • 9
Dynamic Routing • 117
Finish • 30, 31
First Time Deployment Options • 38
General Properties • 28, 30
Important Information • 3
Installation • 8
Installing a Security Policy • 19, 25
Introduction to the WebUI Application • 45
Large-scale Deployment Installation • 22
Large-scale Deployment Workflow • 22
Logs and Monitoring • 110
Managing Active Devices • 50, 112
Managing Authentication Servers • 102
Managing Date and Time • 91
Managing Device Details • 90
Managing Device Settings • 32
Managing Installed Certificates • 93
Managing Licenses • 49
Managing Network Objects • 106
Managing Service Groups • 105
Managing System Services • 104
Managing the Device • 56
Managing URL Lists • 108
Managing Users and Objects • 96
More Information • 28, 31
Predefining a Centrally Managed Deployment • 9
Preparing the Configuration Files • 41

Index