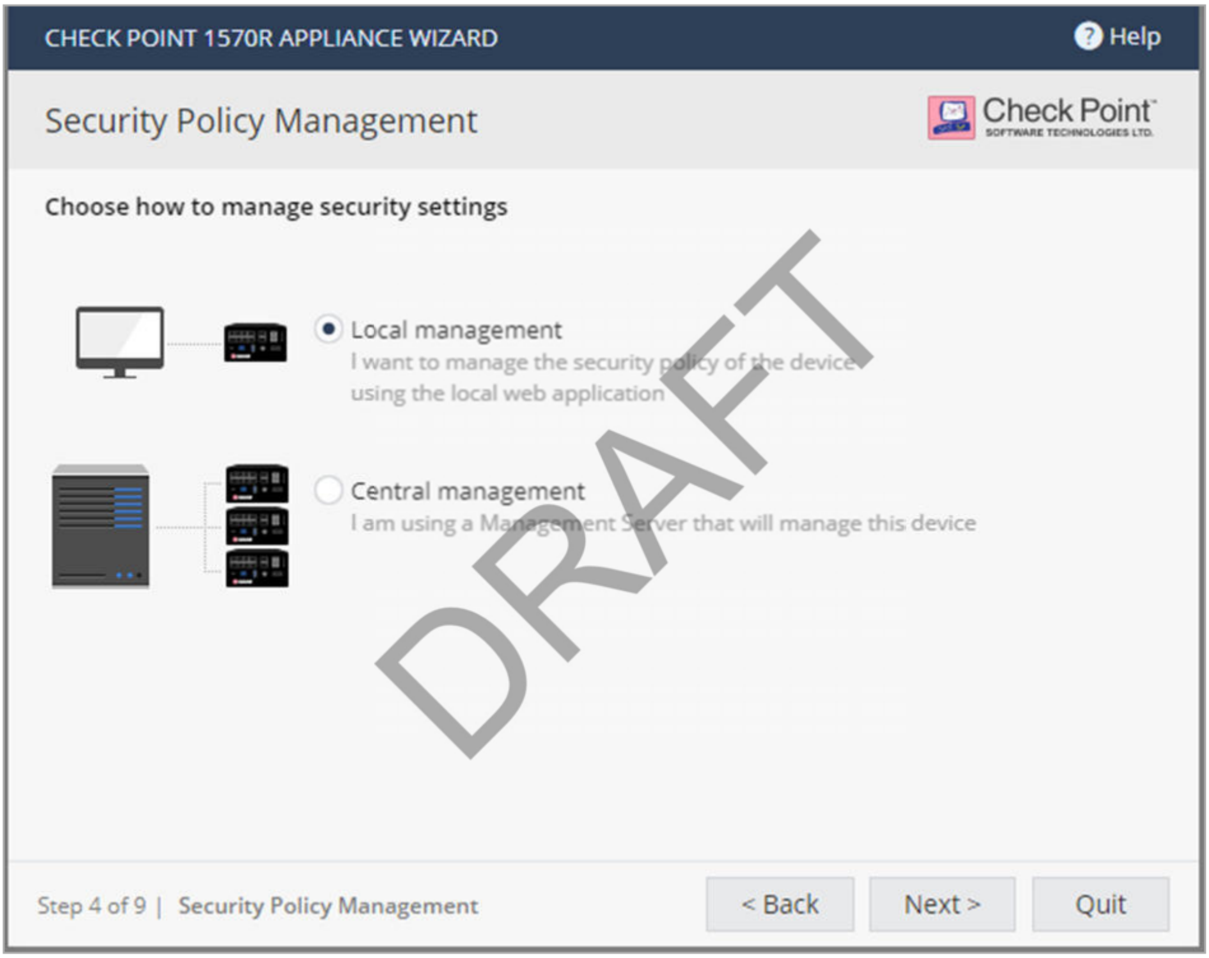
# Security Policy Management

In the **Security Policy Management** page, select how to manage security settings:

- **Central management** - A remote Security Management Server manages the Security Gateway in SmartDashboard with a network object and security policy.
- **Local management** - The appliance uses a web application to manage the security policy. After you configure the appliance with the First Time Configuration Wizard, the default security policy is enforced automatically. With the WebUI, you can configure the Software Blades you activated and fine tune the security policy.

This Getting Started Guide describes how to configure both locally and centrally managed deployments.



CHECK POINT 1570R APPLIANCE WIZARD

Security Policy Management

Choose how to manage security settings

● Local management
I want to manage the security policy of the device using the local web application

○ Central management
I am using a Management Server that will manage this device

Step 4 of 9 | Security Policy Management

# Internet Connection

In **the Internet Connection** page, configure your Internet connectivity details or select **Configure Internet connection later.**

**To configure Internet connection now:**

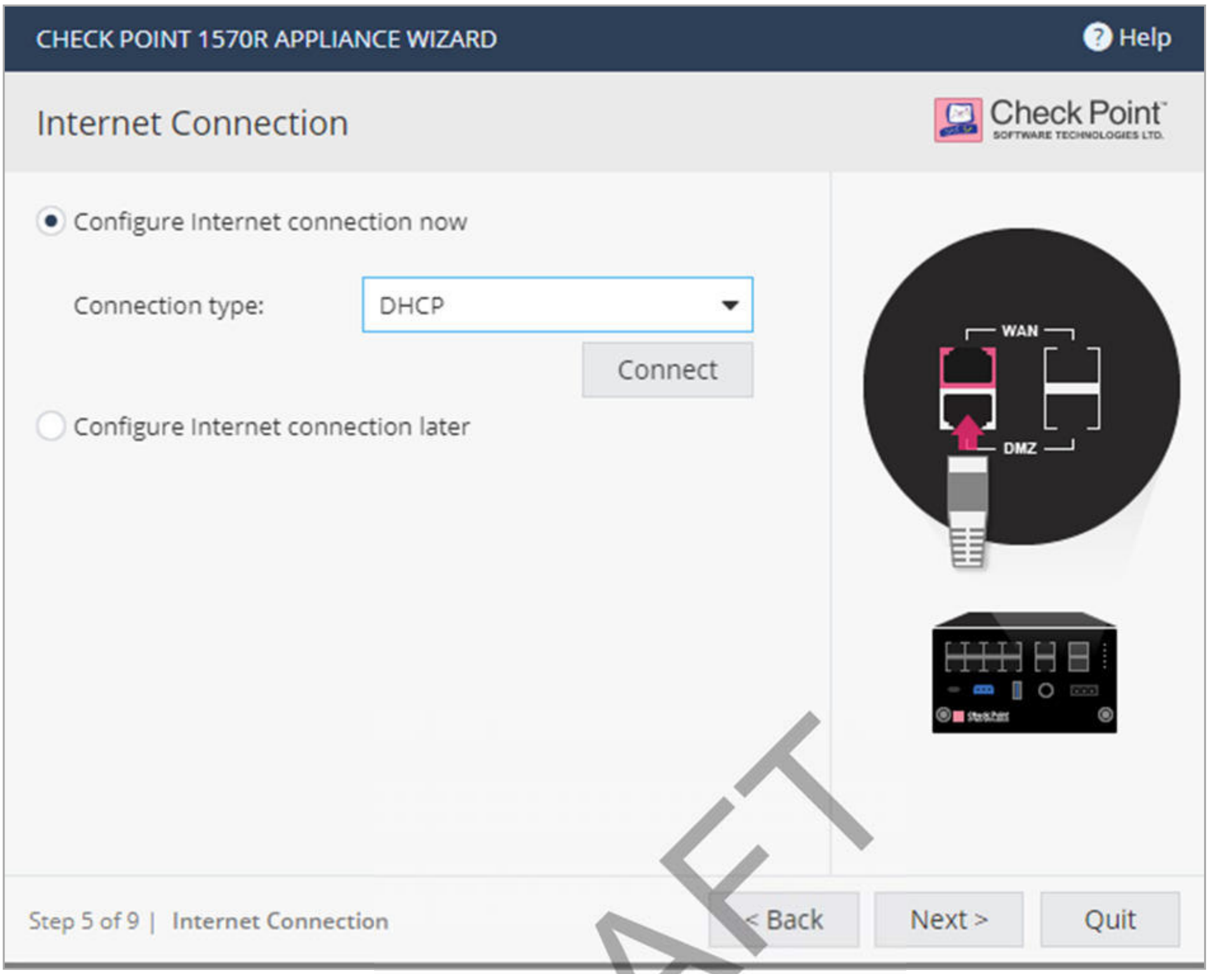
1. Select **Configure Internet connection now**.
2. From the **Connection type** drop down list, select the protocol used to connect to the Internet.
3. Enter the fields for the selected connection protocol. The information you must enter is different for each protocol. You can get it from your Internet Service Provider (ISP).
   - **Static IP** - A fixed (non-dynamic) IP address.
   - **DHCP** - Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses within a specified range to devices on a network. This is a common option when you connect through a cable modem.
   - **PPPoE (PPP over Ethernet)** - A network protocol for encapsulating 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. Enter the **ISP login user name** and **ISP login password**. **Note** - In the First Time Configuration Wizard, only dynamic IP is supported.
   - **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) implements virtual private networks. 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 used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality. It relies on an encryption protocol that it passes within the tunnel to provide privacy.
   - **Analog Modem** - Connect to the Internet using an analog modem through a USB port. In the WebUI application, you can configure to use an analog modem through the serial port.
   - **Bridge** - Connects multiple network segments at the data link layer (Layer 2).
   - **DNS Server** (Static IP and Bridge connections) - Enter the DNS server address information in the relevant fields. For DHCP, PPPoE, PPTP, L2TP, Analog Modem, the DNS settings are supplied by your service provider. You can override these settings later in the WebUI application, under **Device** > **DNS**.

We recommend that you configure the DNS as the appliance needs to perform DNS resolving for different functions. For example, to connect to Check Point User Center during license activation or when Application Control, Web Filtering, Anti-Virus, or Anti-Spam services are enabled.

**To test your ISP connection status:**

Click **Connect**.

The appliance connects to your ISP. Success or failure shows at the bottom of the page.



CHECK POINT 1570R APPLIANCE WIZARD

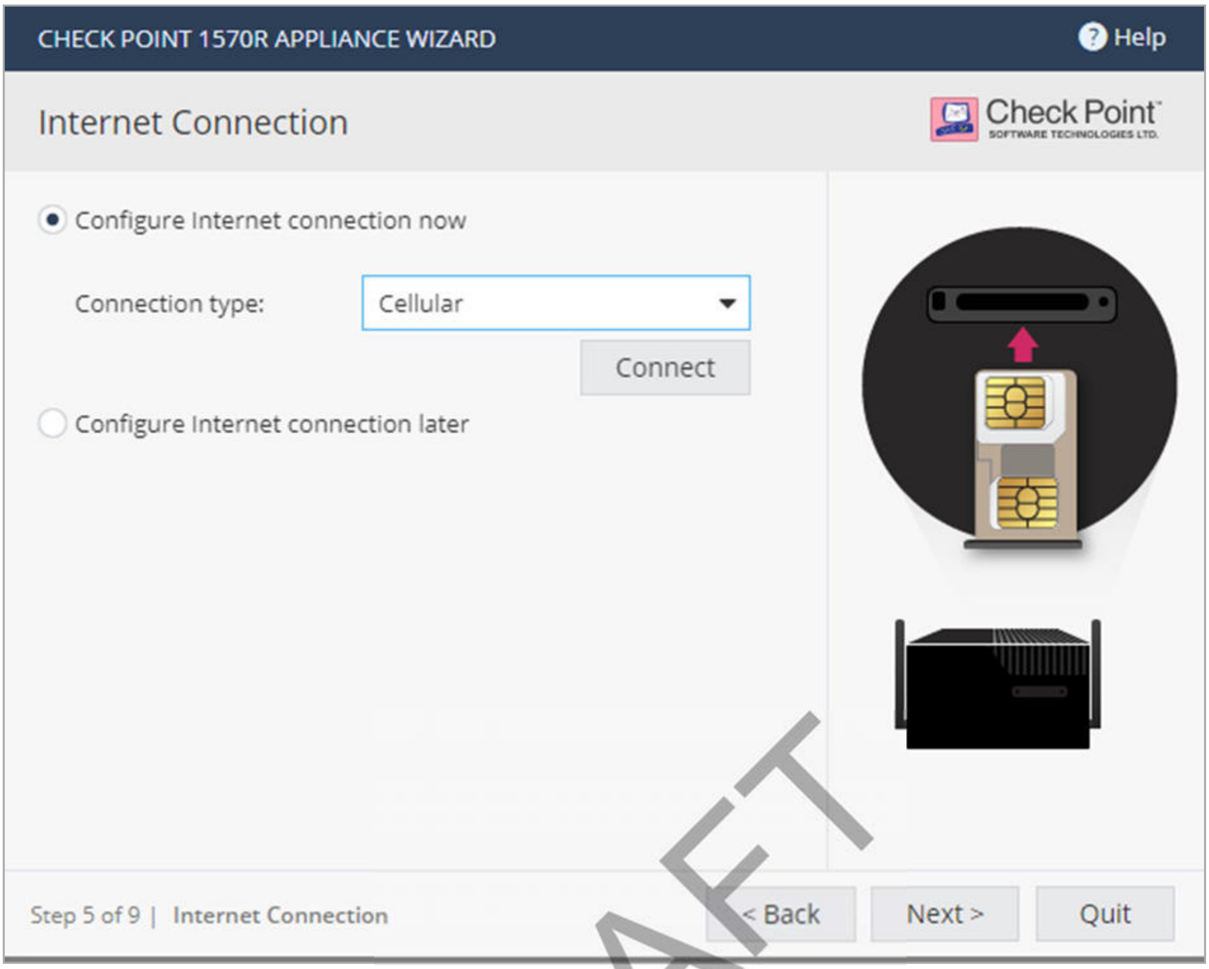
Internet Connection

● Configure Internet connection now

Connection type: DHCP

○ Configure Internet connection later

Step 5 of 9 | Internet Connection



CHECK POINT 1570R APPLIANCE WIZARD

Internet Connection

● Configure Internet connection now

Connection type: Cellular

○ Configure Internet connection later

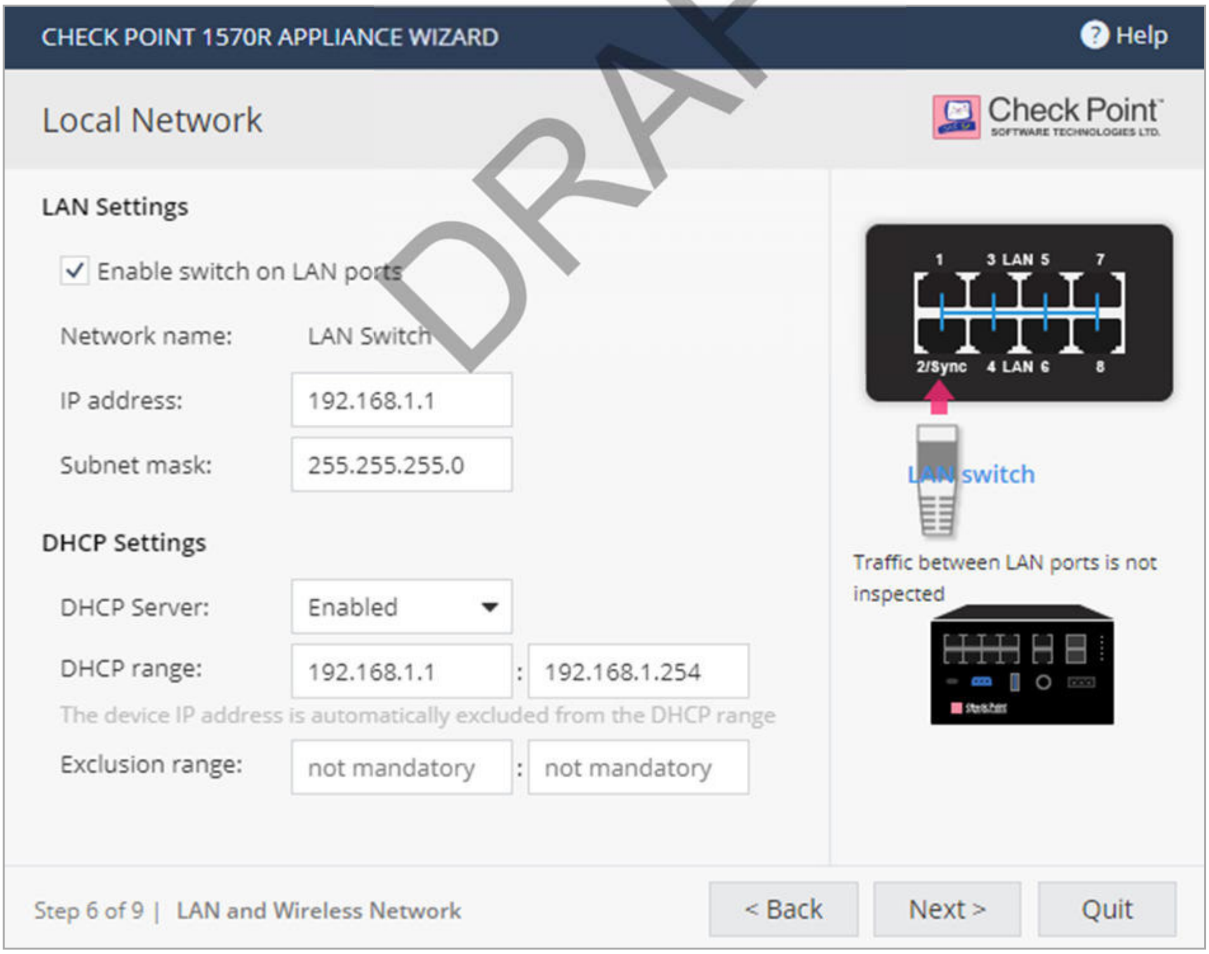
Step 5 of 9 | Internet Connection

# Local Network

In the Local Network page, select to enable or disable switch on LAN ports and configure your network settings. By default, they are enabled. You can change the IP address and stay connected as the appliance's original IP is kept as an alias IP until the first time you boot the appliance.

**Tell me about the fields...**

- **Enable switch on LAN ports** - Aggregates all LAN ports to act as a switch with one IP address for the switch. If this option is disabled (checkbox is cleared), the local network is defined as LAN1 only.
- **Network name** - Enter the network name.
- **IP address** - You can modify the IP address and maintain connectivity. The appliance's original IP is kept as an alias IP to maintain connectivity until the wizard is completed.
- **Subnet mask** - Enter the subnet mask.
- **DHCP server and range fields** - DHCP is enabled by default with a default network range. Make sure to set the appropriate range and do not include predefined static IPs in your network.
- **Exclusion range** - Set the exclusion range for IP addresses that are not defined by the DHCP server. Define the range of IP addresses that the DHCP excludes when IP addresses are assigned in the network. The appliance's IP address is automatically excluded from the range. For example, if the appliance IP is 1.1.1.1 the range also starts from 1.1.1.1, but excludes its own IP address.



CHECK POINT 1570R APPLIANCE WIZARD

Local Network

LAN Settings

☑ Enable switch on LAN ports

Network name: LAN Switch

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

DHCP Settings

DHCP Server: Enabled

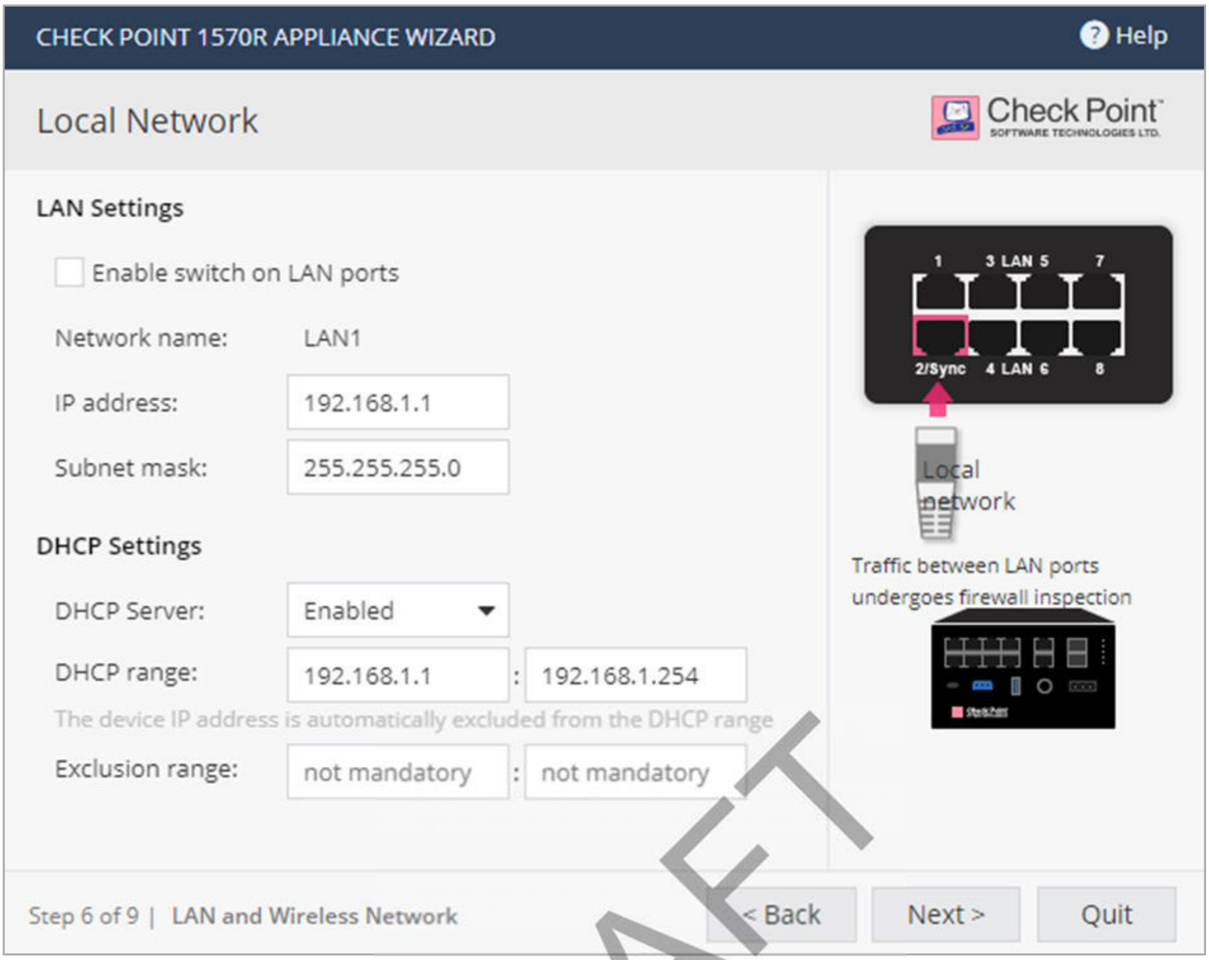
DHCP range: 192.168.1.1 : 192.168.1.254

The device IP address is automatically excluded from the DHCP range

Exclusion range: not mandatory : not mandatory

Traffic between LAN ports is not inspected

Step 6 of 9 | LAN and Wireless Network



CHECK POINT 1570R APPLIANCE WIZARD

Local Network

LAN Settings

□ Enable switch on LAN ports

Network name: LAN1

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

DHCP Settings

DHCP Server: Enabled

DHCP range: 192.168.1.1 : 192.168.1.254

The device IP address is automatically excluded from the DHCP range

Exclusion range: not mandatory : not mandatory

Step 6 of 9 | LAN and Wireless Network

Help
Check Point
SOFTWARE TECHNOLOGIES LTD.
1
3 LAN 5
7
2/Sync
4 LAN 6
8
Local network
Traffic between LAN ports undergoes firewall inspection
< Back
Next >
Quit

**Important** - If you choose to disable the switch on LAN ports (clear the checkbox), make sure your network cable is placed in the LAN1 port. Otherwise, connectivity will be lost when you click **Next**.

# Wireless Network

**For WiFi models only:**

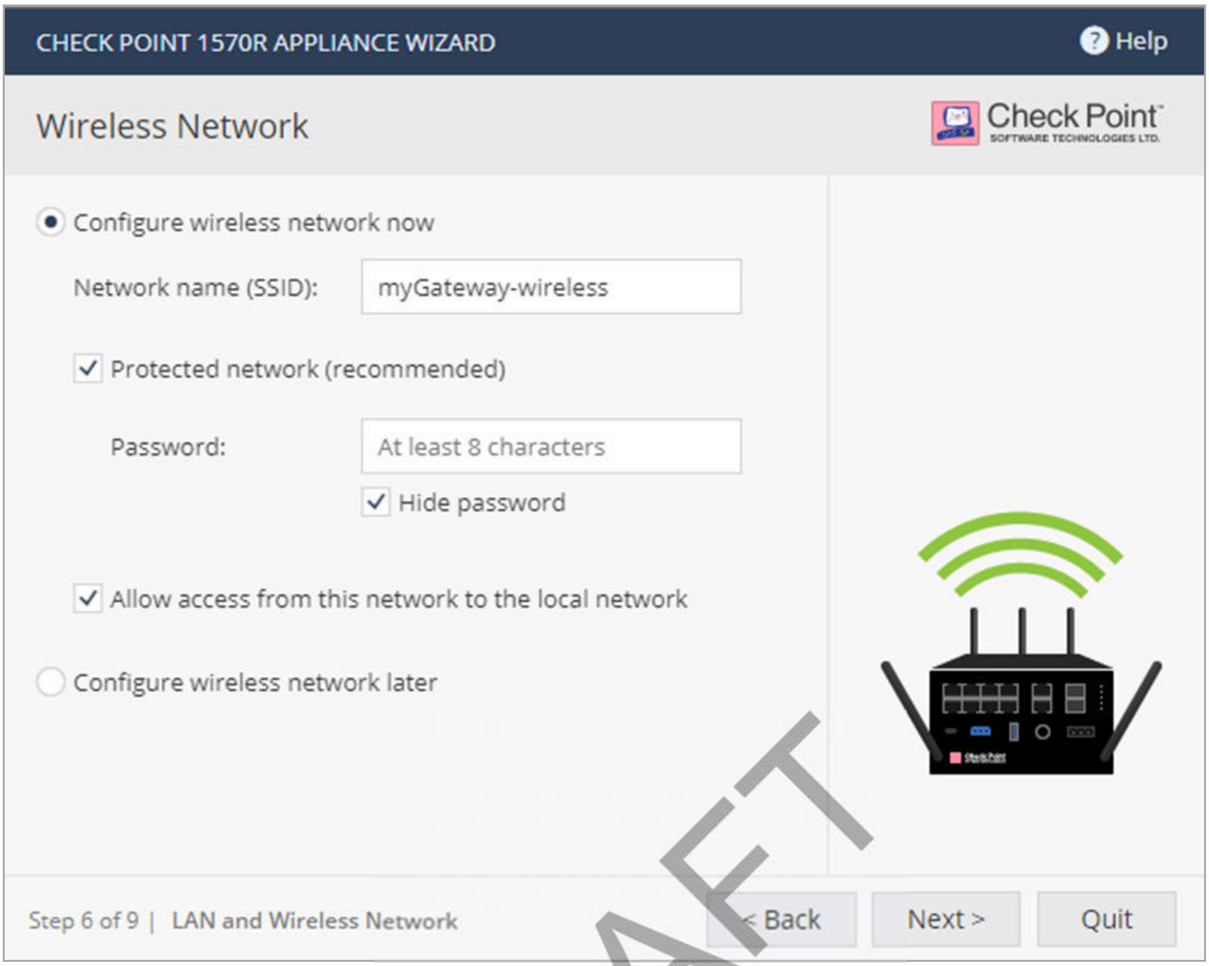
In the Wireless Network page, configure wireless connectivity details.

When you configure a wireless network, you must define a network name (SSID). The SSID (service set identifier) is a unique string that identifies a WLAN network to clients that try to open a wireless connection with it.

We recommend that you protect the wireless network with a password. Otherwise, a wireless client can connect to the network without authentication.

**To configure the wireless network now:**

1. Select **Configure wireless network now**.
2. Enter a name in the **Network name (SSID)** field. This is the name shown to clients that look for access points in the transmission area.
3. Select **Protected network (recommended)** if the wireless network is protected by password.
4. Enter a **Password**.
5. Click **Hide** to conceal the password.
6. **Allow access from this network to the local network** is selected by default. Clear if it is not necessary. If this option is selected, the wireless network is considered trusted and access by default is allowed from it to the local network.



CHECK POINT 1570R APPLIANCE WIZARD

Wireless Network

● Configure wireless network now

Network name (SSID): myGateway-wireless

☑ Protected network (recommended)

Password: At least 8 characters

☑ Hide password

☑ Allow access from this network to the local network

○ Configure wireless network later

Step 6 of 9 | LAN and Wireless Network

# Administrator Access

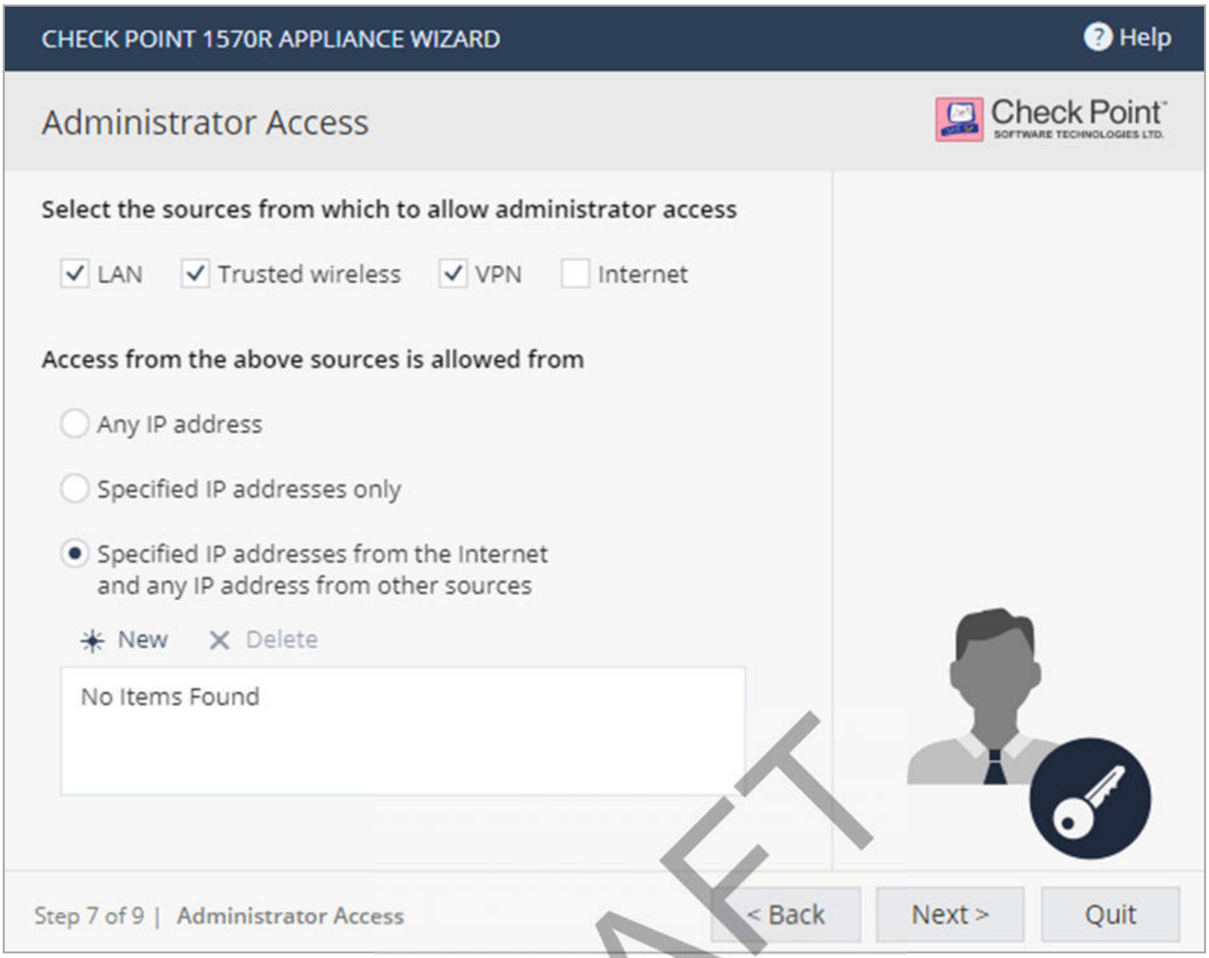
In the **Administrator Access** page, configure if administrators can use the appliance from a specified IP address or any IP address.

**To configure administrator access:**

1. Select the sources from where administrators are allowed access:
   - **LAN** - All internal physical ports.
   - **Trusted wireless** - A known wireless network.
   - **VPN** - Using encrypted traffic through VPN tunnels from a remote site or using a remote access client.
   - **Internet** - Clear traffic from the Internet (not recommended).
2. Select the IP address from which the administrator can access the appliance:
   - **Any IP address**
   - **Specified IP addresses only** - Select this option to let administrators access the appliance from a specified IP address or network. Click **New** to configure the IP address information.
   - **Specified IP addresses from the Internet and any IP address from other sources** - Select this option to allow administrator access from the Internet from specific IP addresses only and access from other selected sources from any IP address. This option is the default.

**To specify IP addresses:**

1. Click **New**.
2. In the IP Address Configuration window, select an option:
   - **Specific IP address** - Enter the **IP address** or click **Get IP from my computer**.
   - **Specific network** - Enter the **Network IP** address and **Subnet mask**.
3. Click **Apply**.



CHECK POINT 1570R APPLIANCE WIZARD

Administrator Access

Select the sources from which to allow administrator access

☑ LAN ☑ Trusted wireless ☑ VPN □ Internet

Access from the above sources is allowed from

○ Any IP address

○ Specified IP addresses only

● Specified IP addresses from the Internet and any IP address from other sources

No Items Found

Step 7 of 9 | Administrator Access

# Appliance Registration

The appliance can connect to the Check Point User Center with its credentials to pull the license information and activate the appliance.

**If you have Internet connectivity configured:**

Click **Activate License**.

You are notified that you successfully activated the appliance and you are shown the status of your license for each blade.

**If you are working offline while configuring the appliance:**

1. From a computer with authorized access to the Check Point User Center, do procedure a or b:

   a. **Use your User Center account:**

      - Log into your User Center account.
      - Select the specified container of your appliance.
      - From the **Product Information** tab, click **License** > **Activate**.

        This message is shown: "Licenses were generated successfully."
      - Click **Get Activation File** and save the file locally.

   b. **Register your appliance:**

      - Go to: https://smbregistration.checkpoint.com
      - Enter your appliance details and click **Activate**.

        This message is shown: "Licenses were generated successfully."
      - Click **Get Activation File** and save the file locally.

2. In the Appliance Activation page of the First Time Configuration Wizard, click **Offline**.

   The Import from File window opens

3. Browse to the activation file you downloaded and click Import. The activation process starts.

   You are notified that you successfully activated the appliance and you are shown the status of your license for each blade.

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.**

You are notified that you successfully activated the appliance and you are shown the status of your license for each blade.

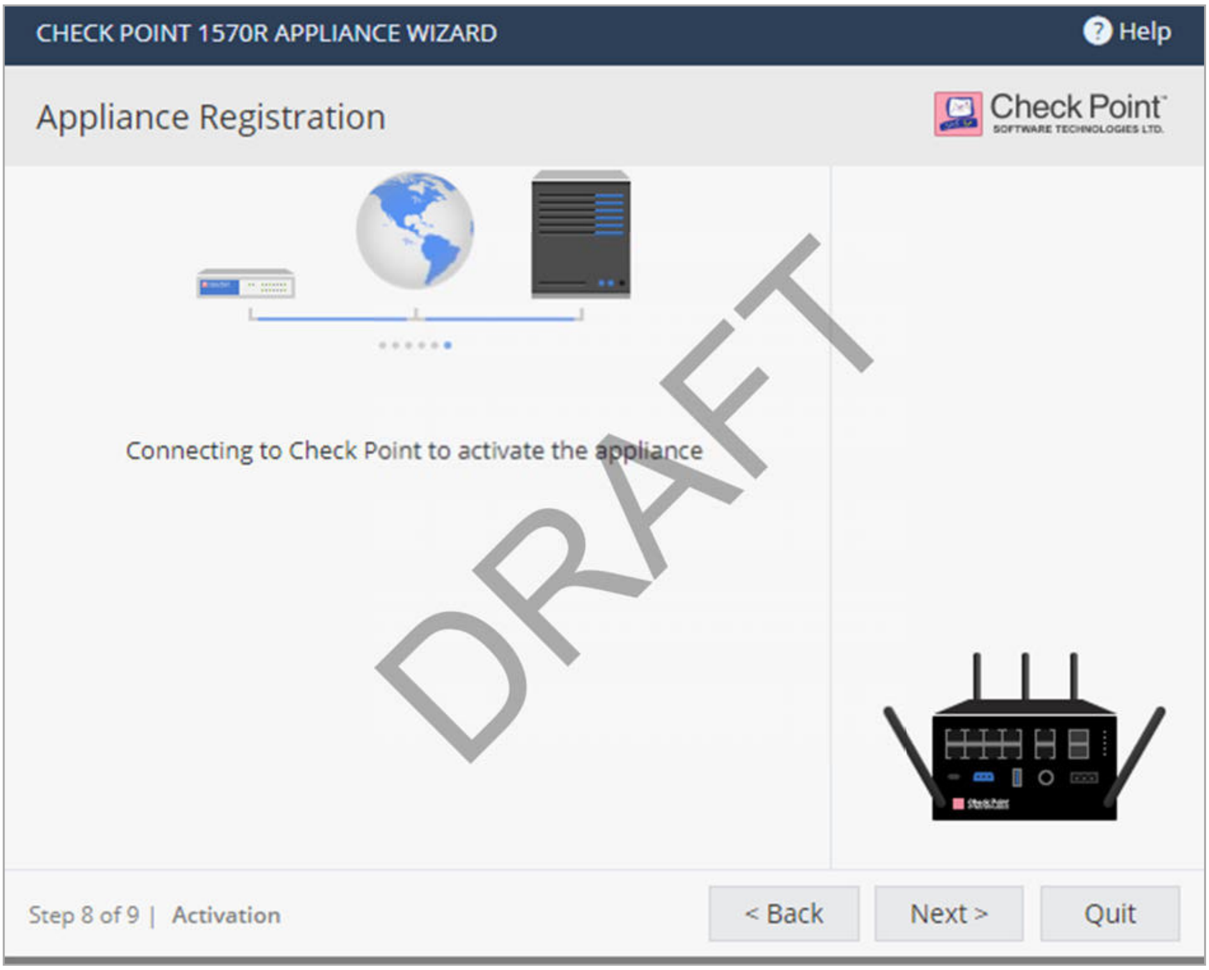
**To postpone appliance registration and get a 30-day trial license:**

1. Click **Next**.

   The License activation was not complete notification message is shown.

2. Click **OK**.

   The appliance uses a 30-day trial license for all blades. You can register the appliance later from the WebUI Device > **License** page.



CHECK POINT 1570R APPLIANCE WIZARD

Appliance Registration

Connecting to Check Point to activate the appliance

If your device is not paired with a User Center account, you must create an account or ask your company admin to create one for you.

**To create a new User Center account (Locally Managed only):**

1. Click **Activate License**.

   The Appliance Registration window opens.

2. Select **Create a new User Center account** and click **Next**.

3. In the new window, enter:
   - **First name**
   - **Last Name**
   - **Email**. You must enter this a second time to confirm.
   - **Company** - This is the Account Name to which the appliance is paired.
4. Click **Next**.

The Software Blades Activation page opens.

# Security Management Server Authentication

**For Centrally managed appliances only:**

When you select central management as your security policy management method, the **Security Management Server Authentication** page opens.

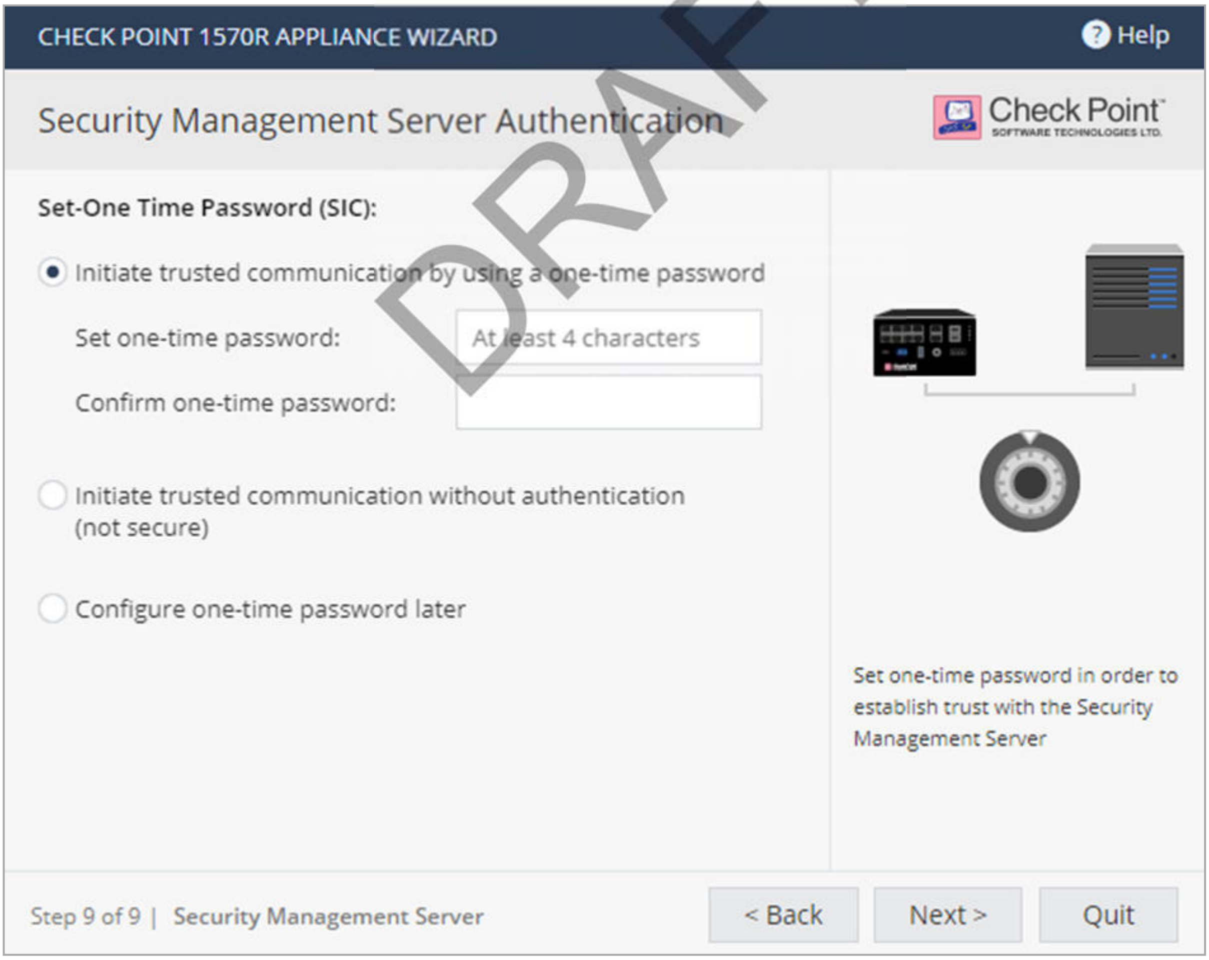
Select an option to authenticate trusted communication with the Security Management Server:

- **Initiate trusted communication securely by using a one-time password** - The one-time password is used to authenticate communication between the appliance and the Security Management Server securely.

  Enter a **one-time password** and confirm it. This password is only used for establishing the initial trust. When established, trust is based on security certificates.

  **Important** - This password must be identical for the Secure Communication authentication one-time password configured for the appliance object in the SmartConsole of the Security Management Server.

- **Initiate trusted communication without authentication (not secure)** - Use this option only if there is no risk of malicious behavior (for example, when in a lab setting).
- **Configure one-time password later** - Set the one-time password at a different time using the WebUI application.



CHECK POINT 1570R APPLIANCE WIZARD

Security Management Server Authentication

Set-One Time Password (SIC):

● Initiate trusted communication by using a one-time password

Set one-time password: At least 4 characters

Confirm one-time password:

○ Initiate trusted communication without authentication (not secure)

○ Configure one-time password later

Set one-time password in order to establish trust with the Security Management Server

Step 9 of 9 | Security Management Server

# Security Management Server Connection

**For Centrally managed appliances only:**

After you set a one-time password for the Security Management Server and the appliance, you can connect to the Security Management Server to establish trust between the Security Management Server and the appliance.

**To connect to the Security Management Server, select:**

- **Connect to the Security Management Server now**.

  Or

- **Connect to the Security Management Server later**

**If you select to connect now, enter the data for these fields:**

- **Management address** - Enter the IP address or host name of the Security Management Server.
- **Connect** - When you successfully connect to the Security Management Server, the security policy will automatically be fetched and installed.
- If the Security Management Server is deployed behind a 3rd party NAT device, select **Always use the above address to connect to the Security Management Server**. Manually enter the IP address or the host name of the appliance should connect to reach the Security Management Server.

  If you enter an IP address, it will override the automatic mechanism that determines the routable IP address of the Security Management Server for each appliance.

  If you enter a host name, it is saved and the Security Gateway will re-resolve the name of the IP address changes. This configuration can be edited later in the **Home** > **Security Management** page of the WebUI.

  If you do not select this checkbox and you use a host name to fetch the policy, when the policy is fetched, the Security Management Server IP is set to the IP address in the policy.

  Select where to send logs:

  - **Send logs to same address** - The logs are sent to the IP address entered on this page for the Security Management Server.
  - **Send logs to** - Enter the IP address of a log server.
  - **Send logs according to policy** - The logs are sent according to the log server definitions that are defined in the policy.