Check Point
SOFTWARE TECHNOLOGIES LTD.

24 February 2020

1570/1590 APPLIANCE

R80.20.05

Getting Started Guide

Models: V-81, V-81W, V1WL [Classification: Restricted]

Check Point
INFINITY

Check Point Copyright Notice

© 2020 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

Important Information

Latest Software

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

Certifications

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

Check Point R80.20.05

For more about this release, see the R80.20.05 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.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments.

Revision History

Date	Description
24 February 2020	Added LTE-WiFi models
26 September 2019	First release of this document

Table of Contents

Introduction 6
Shipping Carton Contents 7
Setting up the Appliance 8
Wall Mounting 8
Connecting the Cables 9
First Time Deployment Options 10
Appliance Diagramals and Specifications 11
Front Panel 14
Back Panel 18
Side Panels 20
Using the First Time Configuration Wizard 24
Starting the First Time Configuration Wizard 24
Welcome 25
Zero Touch 25
Authentication Details 27
Appliance Date and Time Settings 29
Appliance Name 30
Security Policy Management 31
Internet Connection 32
Local Network 34
Wireless Network 36
Administrator Access 38
Appliance Registration 40
Security Management Server Authentication 43
Security Management Server Connection 44
Software Blade Activation 46
Summary 47
Zero Touch Cloud Service 48
USB Drive or SD Card 49
Health and Safety Information 50

Information sur la Santé et la Sécurité *58*

Support *66*

Introduction

Thank you for choosing Check Point's Internet Security Product Suite. Check Point products provide your business with the most up to date and secure solutions available today.

Check Point also delivers worldwide technical services including educational, professional, and support services through a network of Authorized Training Centers, Certified Support Partners, and Check Point technical support personnel to ensure that you get the most out of your security investment.

For more information about the appliance, see the *Check Point 1500 Appliance series Administration Guide*.

For more technical information, go to Check Point Support Center.

Shipping Carton Contents

Item	Quantity	Description
Appliance	1	1570/1590 Appliance
LAN cable	1	1.8m - RJ45 to RJ45, CAT5e, shielded, STP, black color
Console cable	1	1m, USB type-C to USB-2.0 type-A, black color
Power adapter	1	AC to 12VDC desktop, 40W wired, 60W WiFi, black color
Power cord for adapter	1	Plug types: US, UK, EU and AUS/NZ, India, China, Japan
Rubber feet	4	Assembled on the appliance
Wall mount kit	1	Includes drilling hole location sticker. Screws: M4*6, truss screw
Antenna	4 +2	WiFi Antenna RP-SMA type, black color (WiFi models only) LTE Antenna RP-SMA type, black color (for LTE models only)
DSL Cable	1	RJ11-TAE cable for Annex B or RJ11-RJ11 cable for Annex A (DSL model only)
Guides	1	*Check Point 1570/1590 Appliance Quick Start Guide*
License Agreement	1	End user license agreement

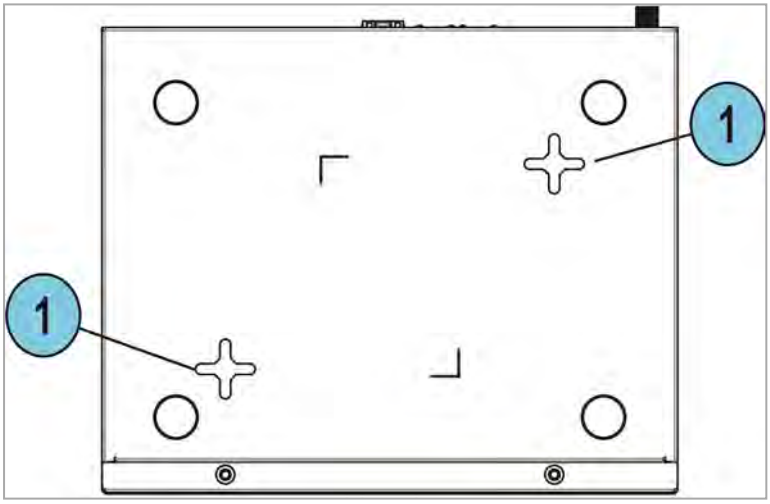
Setting up the Appliance

1. Remove the Check Point 1570/1590 Appliance appliance from the shipping carton and place it on a tabletop.
2. **Optional** - Remove the transparent protective sticker from the front panel of the appliance.
3. Attach antennas to the model (WiFi and LTE models only).
4. Identify the network interface marked as LAN1. This interface is preconfigured with the IP address 192.168.1.1.

Wall Mounting

To mount the appliance to the wall:

1. Place the wall-mount sticker on the wall and drill two holes for the screws.
2. Attach the 2 screws in the accessory kit (M4*6) to the wall.
3. Mount the appliance and verify the 2 screws are fastened well to the appliance.



Key	Item	Description
1	Holes on the bottom of the appliance	Attach screws here.

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 is connected.

2. When the appliance is turned on, the Power LED on the front panel lights up in red for a short period.

   The LED then turns blue and starts to blink. This shows a boot is in progress and firmware is being installed.

   When the LED turns a solid blue, the appliance is ready for login.

   Note - The LED is red if there is an alert or error.

3. Connect the standard network cable to the LAN1 port on the back panel of the appliance and to the network adapter on your PC.

4. **Connect the console cable to the console port on the back of the appliance, and to a USB port on a supported terminal.**

   a. Set the Flow control to **None**.

   b. To get the console driver, click: https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

   c. Verify the MD5 and SHA256 are the following:

      - MD5 - c0b27c9b0f3a3ed53927a4857853a2cb
      - SHA 256 - 5d8fa117cd499a50cab895f35d50d108a61e80b6a3f6d2ecbffa8949085b8f2e

5. **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

First Time Deployment Options

There are different options for first time deployment of your gateways:

- *"Using the First Time Configuration Wizard" on page 24*
- *"Zero Touch Cloud Service" on page 48*
- *"USB Drive or SD Card" on page 49"USB Drive or SD Card" on page 49*

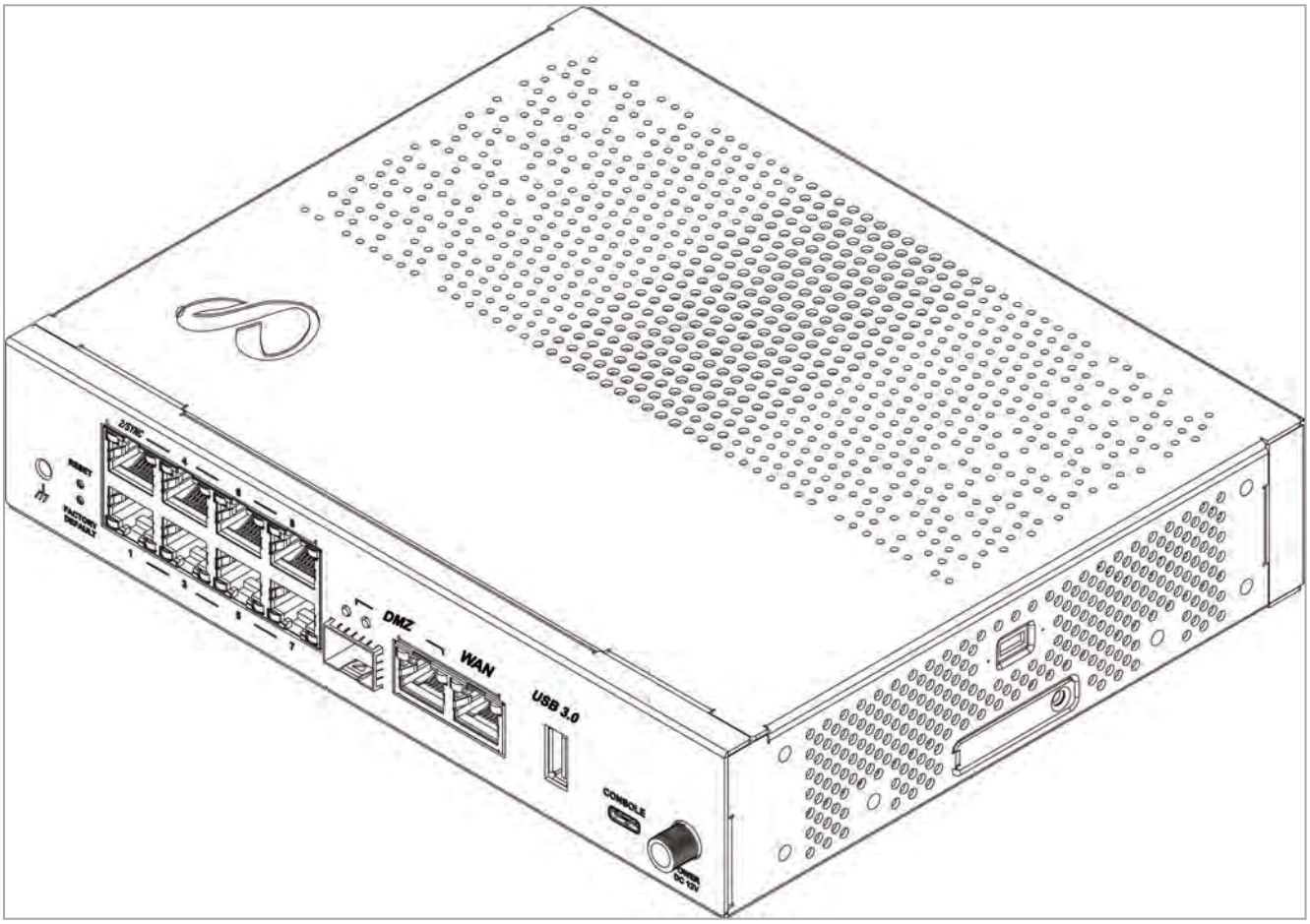
Appliance Diagramals and Specifications

This section describes the different features in the front, back, and side panels of these 1570/1590 Appliance models:

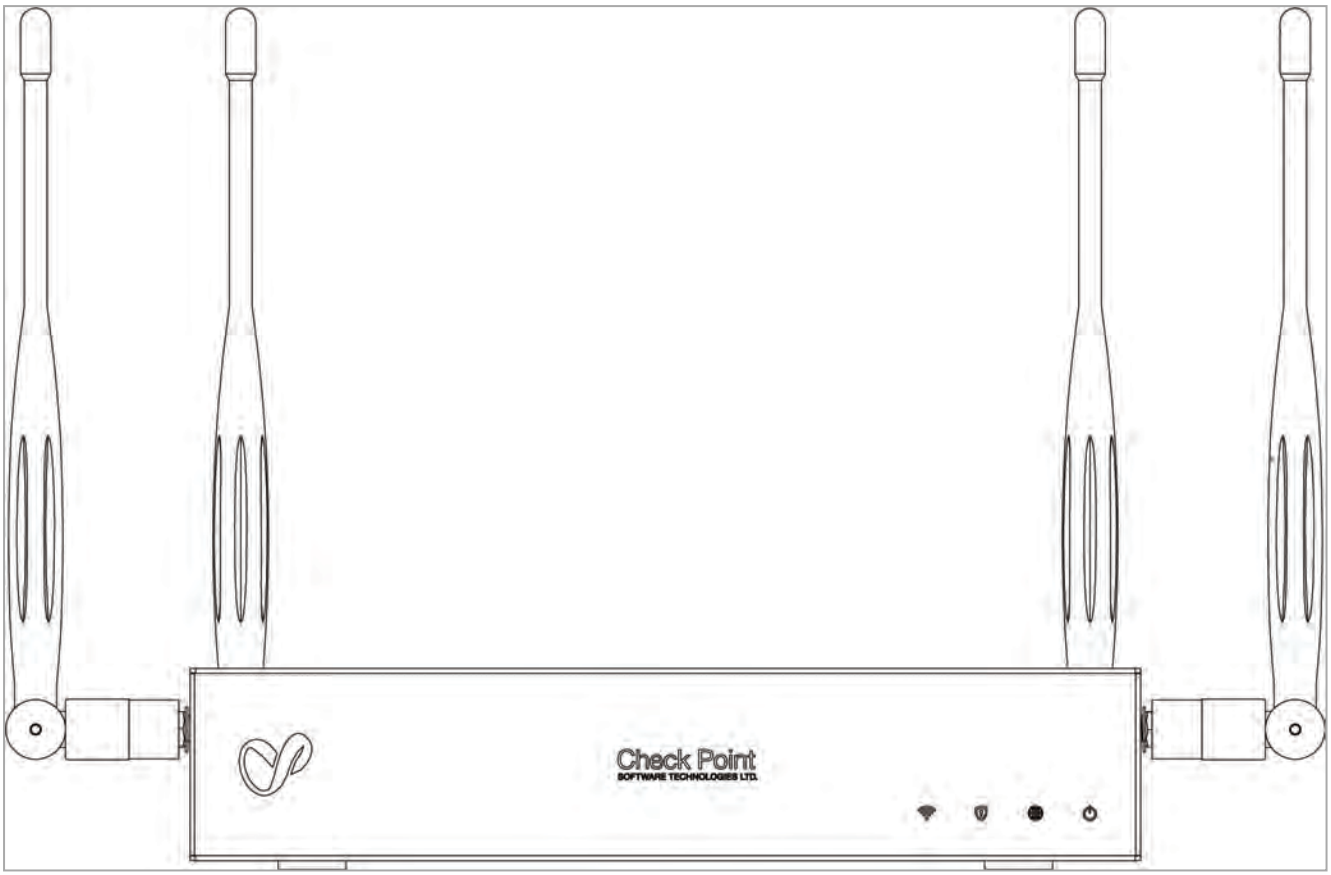
- Wired
- WiFi
- LTE-WiFi

Note - Depending on which model appliance you have, some of the specifications below may vary.

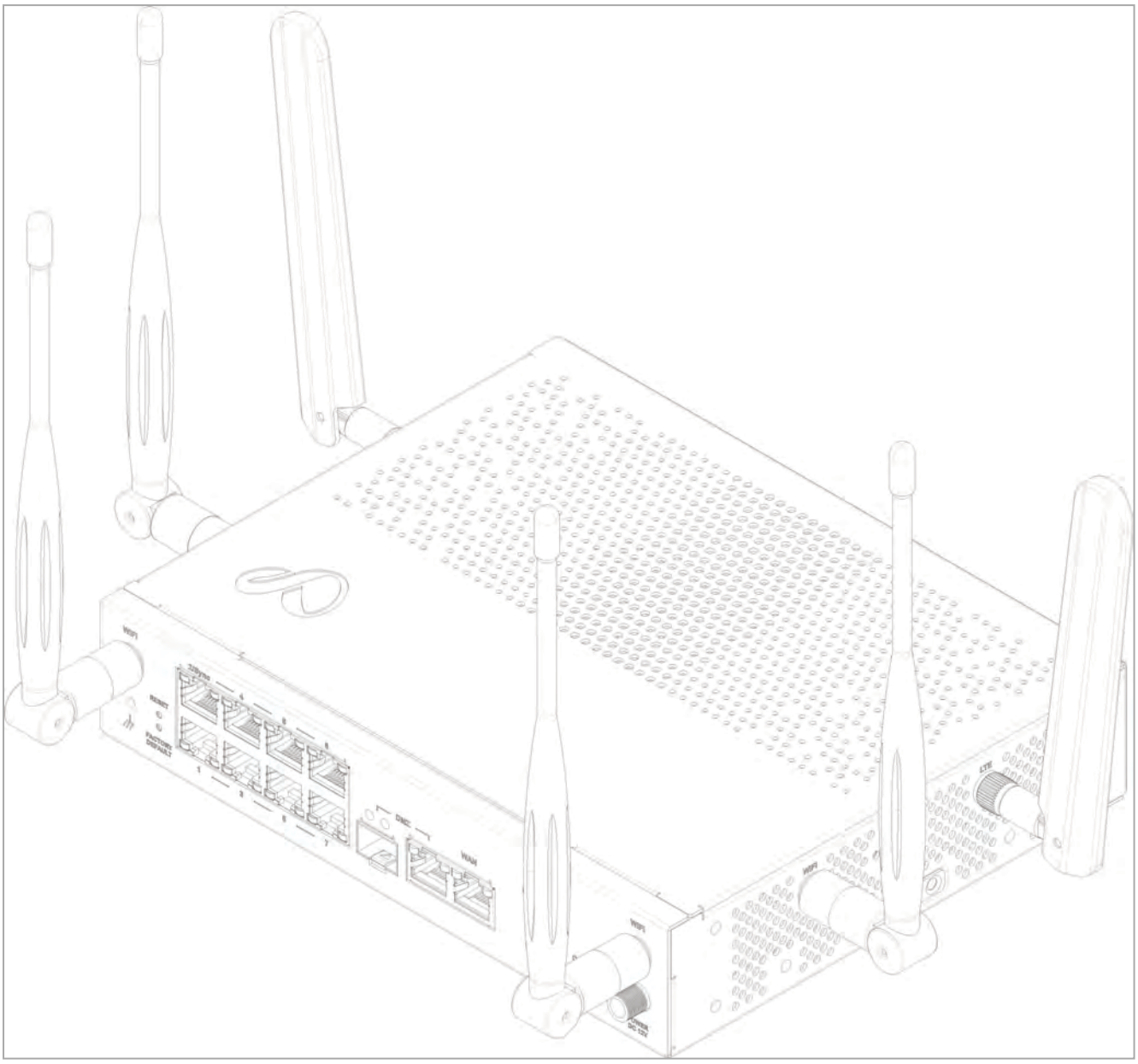
Wired



WiFi



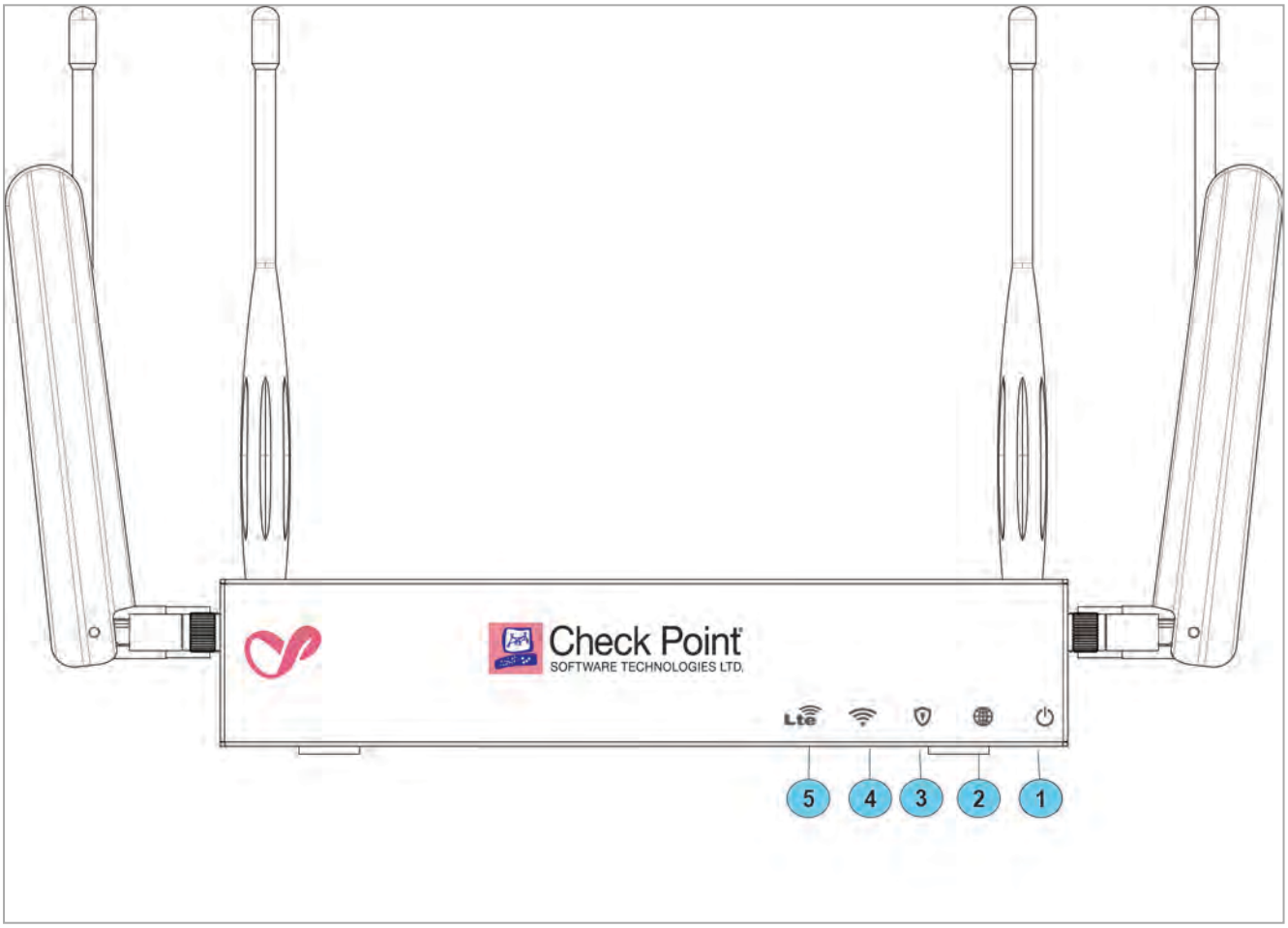
LTE-WiFi



Front Panel

Wired/WiFi (antennas not shown)

LTE-WiFi



Note - There is only one set of LEDs. These LEDs show different colors (blue or red) depending on what activity is occurring.

Table: LEDs

Key	Item	Description
1	Power LED	■ **Solid Blue** - Normal operation ■ **Blinking Blue** - Boot in progress or installing firmware. ■ **Red** - Error/Alert **Note** - This LED is red when the appliance is first turned on.
2	Internet LED	■ **Off** - No internet connection ■ **Blue** - Connected ■ **Blinking Red** - Connection failure
3	Management LED	■ **Off** - No management ■ Colors - See below
4	WiFi LED (WiFi models only)	■ **Off** - WiFi off ■ **Blue** - WiFi on and operates normally ■ **Red** - WiFi error/alert
5	LTE-WiFi LED (LTE-WiFi models only)	■ **Off** - LTE-WiFi off ■ **Solid Blue** - Cellular modem is available (operating SIM must be inserted) ■ **Blinking Blue** - Cellular data transfer ■ **Red** - Cellular modem issue (no SIM, modem off, no signal, etc.)
6	DSL WiFi LED (DSL WiFimodels only)	■ **Off** - DSL off ■ **Blinking Blue** - Syn in progress ■ **Solid Blue** - Synced ■ **Flashing Red** (LED alternates between blue and pink) - Traffic

The Management LED shows the status of the retries mechanism:

Action	Management LED Activity
Zero Touch is running.	Blinks red (slowly)
Successfully connected to Zero Touch Cloud Server and saved the deployment script.	Blinks red (rapidly)
Zero Touch process is completed. SMP activation is not needed.	LED off
Activation sleeping time.	Blinks blue (slowly)
Reactivation.	Blinks blue (rapidly)
SMP is connected.	Solid blue.
SMP mode is off.	LED off
Gateway failed to connect to the SMP and will exit from the retry script.	Constant red.

Wait times before retry:

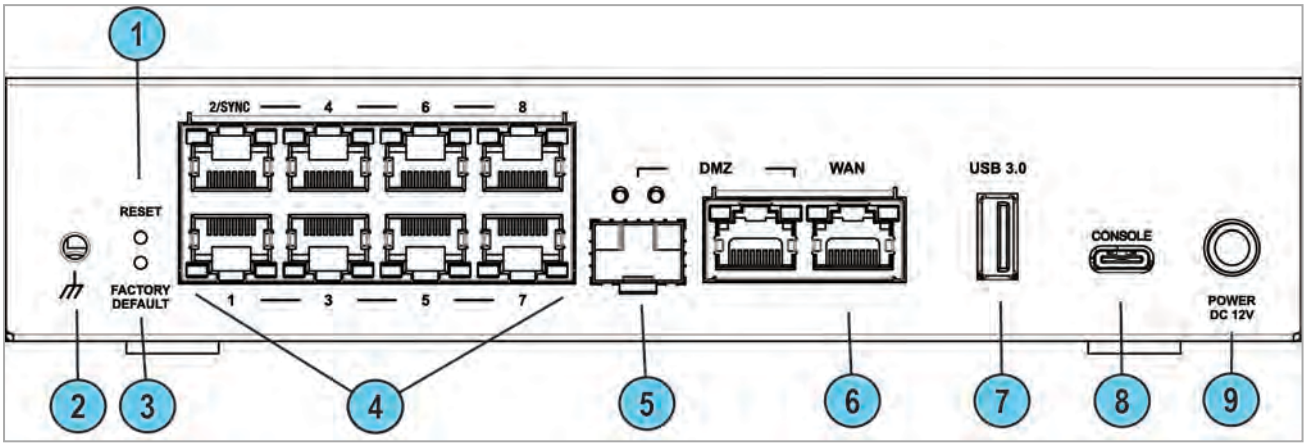
Failure	Waiting Time
1st	2 minutes
2nd	4 minutes
3rd	8 minutes
4th	16 minutes
Subsequent	Retries every 16 minutes until Cloud Services are successfully activated

The table below describes the network LEDs (RJ45 WAN and LAN ports and the SFP). Each port uses a bi-color LED to reflect the link/activity and speed, from 10M to 1GbE.

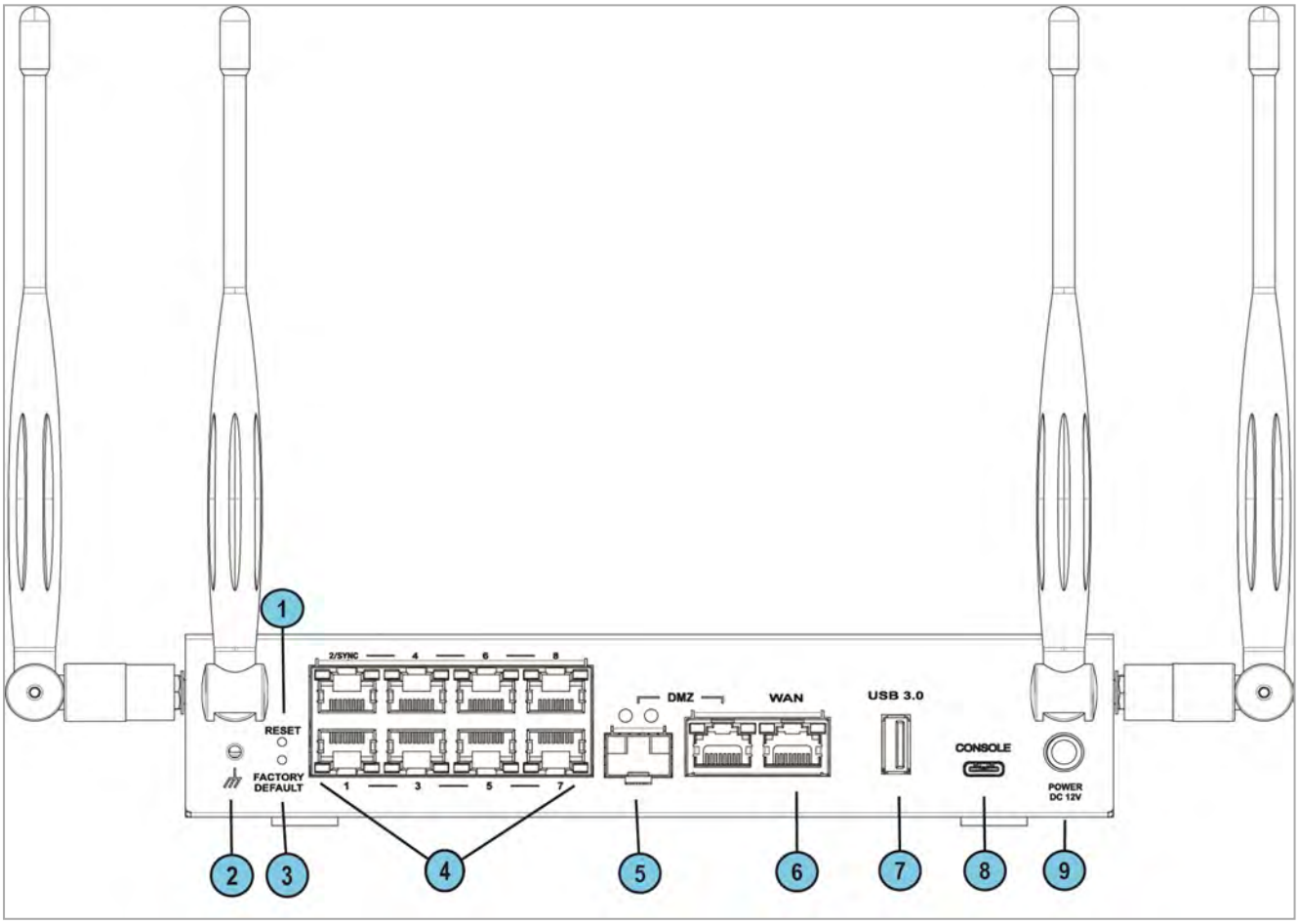
RJ45 and 1G SFP	LED1 (Green)	LED2 (Amber)
No link	Off	Off
1G link	ON	ON
1G Act	Blink	ON
100M link	ON	Off
100M Act	Blink	Off
10M link	ON	Off
10M Act	Blink	Off

Back Panel

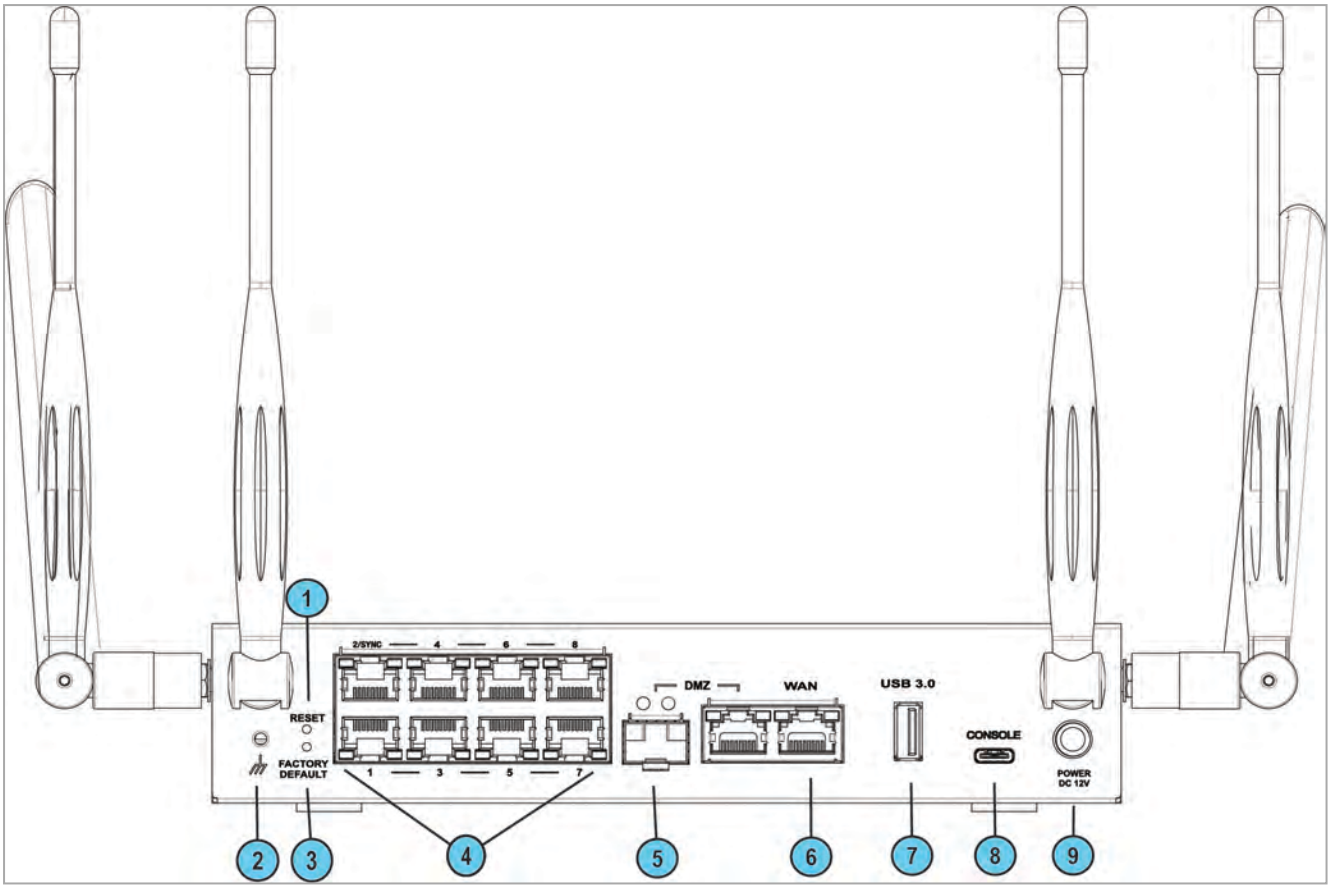
Wired



WiFi



LTE-WiFi



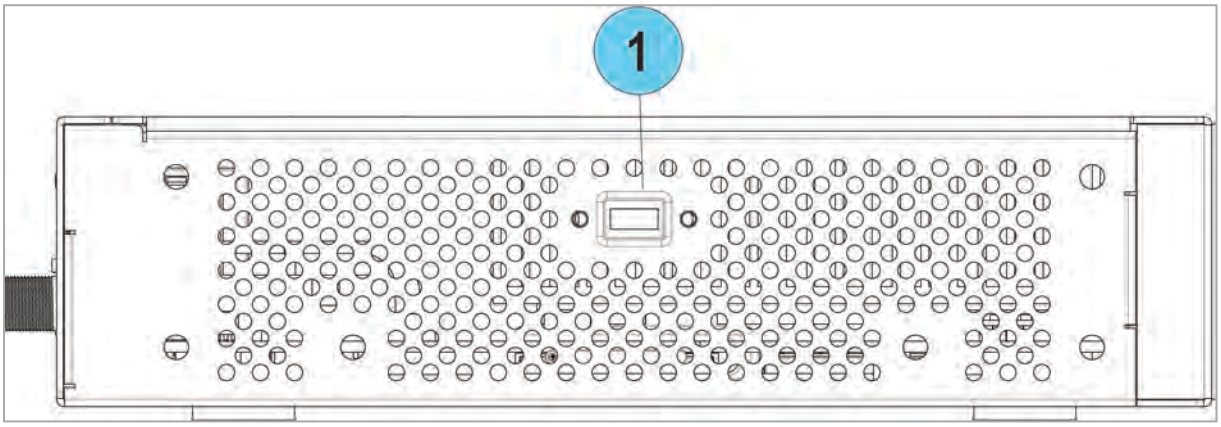
Key	Item	Description
1	Reset	Short press resets the system but does not remove any user parameters.
2	Ground screw	Functional grounding.
3	Factory default	Press the button continuously for 12 seconds to restore the appliance to its factory default. All user parameters previously configured are removed.
4	LAN ports	LAN ports 1-8. 10/100/1000MbE
5	DMZ fiber SFP port	DMZ combination port. The LEDs above indicate connection and speed (see below). 1GbE speed, short and long range.
6	RJ45 DMZ and WAN1 combo port	The DMZ is a combo port of SFP and RJ45 (on the right). Only one can operate a time once plugged in and connected. 10/100/1000MbE
7	USB port 3.0	USB port 3.0 for software download and external dongle as WiFi.
8	Console	Plug in the serial console cable here. Baud rate: 115200.

Key	Item	Description
9	Power cord socket	Plug the power adapter cord in here.

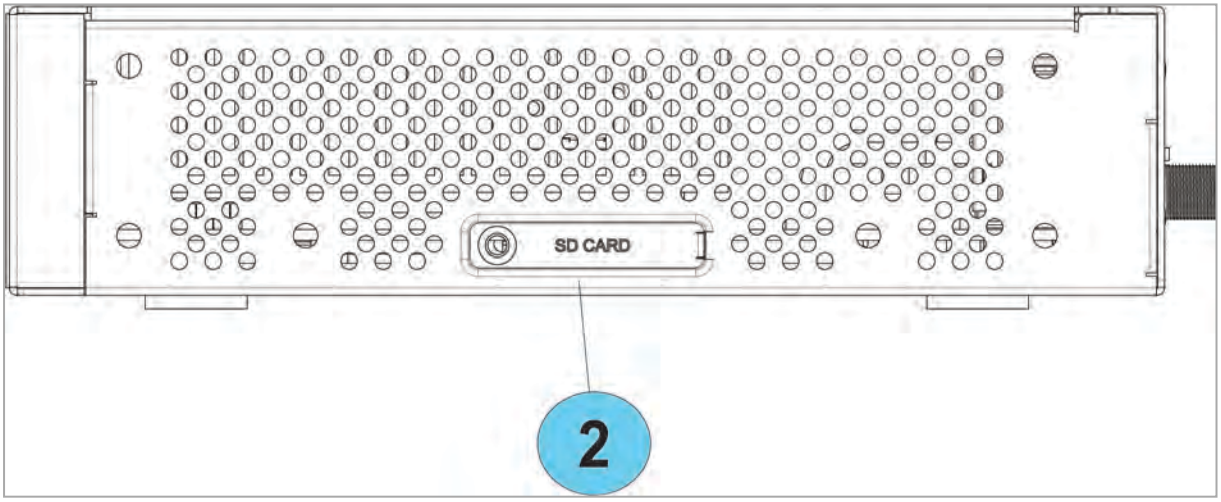
Side Panels

Wired/WiFi/

Side 1

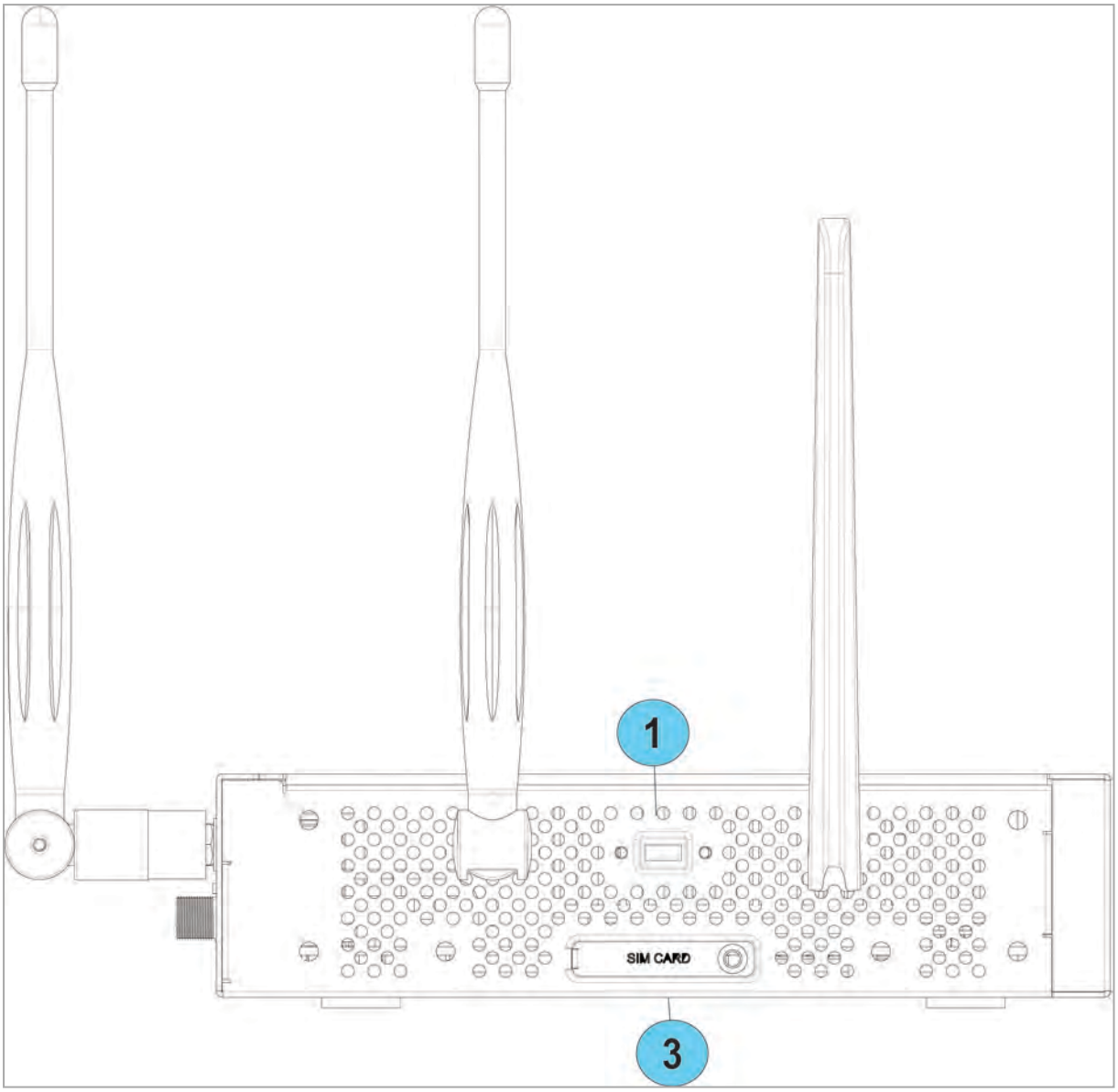


Side 2

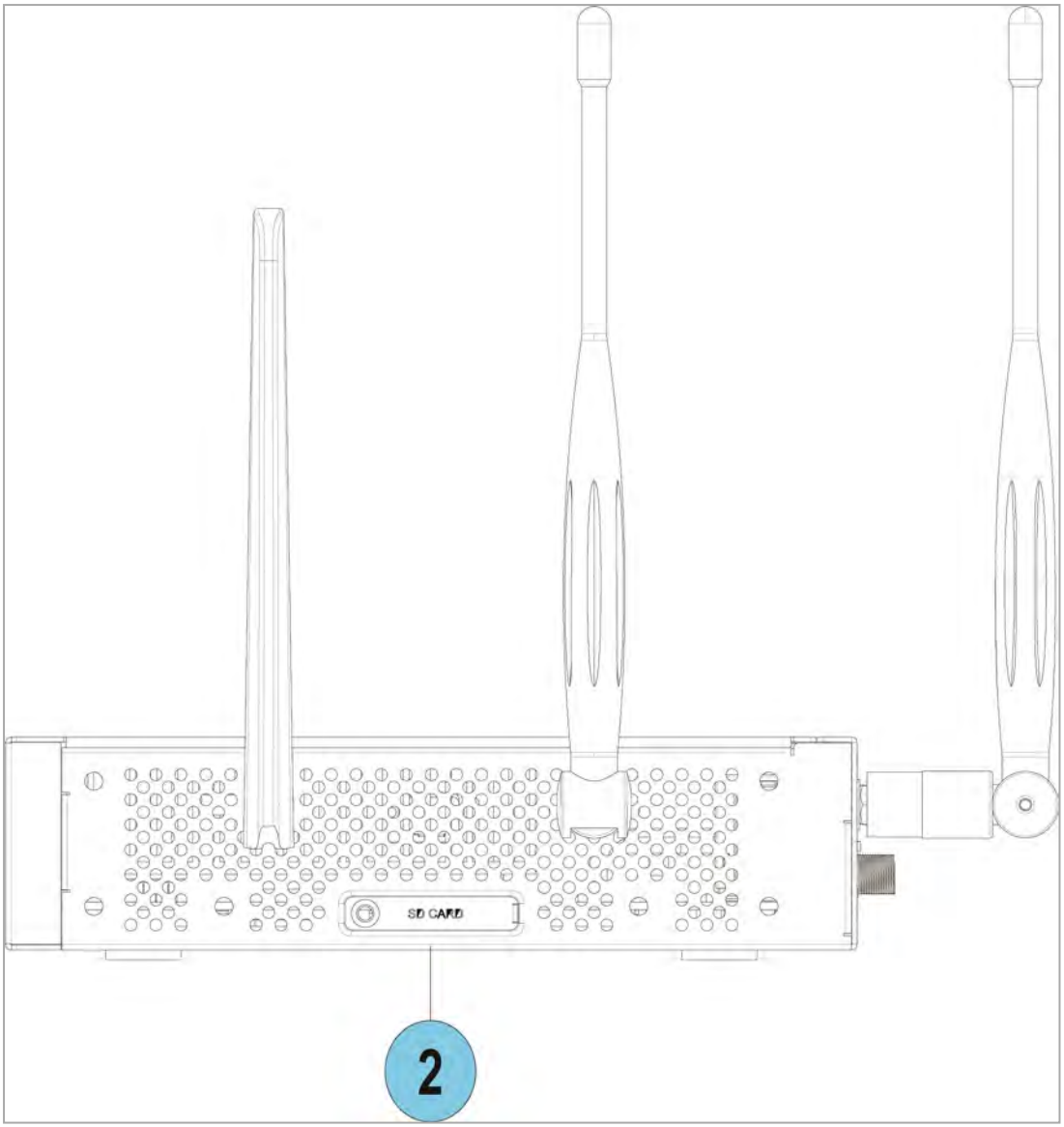


LTE-WiFi

Side 1



Side 2



Key	Item	Description
1	Anti-theft slot	Insert anti-theft cable here. Use Kensington and Sunbox TL-623M cable as a reference.
2	SD slot	Insert micro-SD card here.
3	Dual SIM slot	Insert one of two SIM cards here (LTE models only) ■ SIM1 - Micro SIM ■ SIM2 - Nano SIM

SD Card Notes:

- Micro-SD card supports formats NTFS and FAT, up to 256GB size.
- While inserting the micro-SD card, make sure the golden pins are facing upward:

Dual SIM Card Notes:

- Activation is done manually via clish/WebUI. The user selects the preferred SIM.
- The modem supports automatic failover between SIMs.

Using the First Time Configuration Wizard

Configure the Check Point 1570/1590 Appliance appliance with the First Time Configuration Wizard.

To close the wizard and save configured settings, click **Quit**.

Note - In the First Time Configuration Wizard, you may not see all the pages described in this guide. The pages that show in the wizard depend on your appliance model and the options you select.

Starting the First Time Configuration Wizard

To configure the Check Point 1570/1590 Appliance appliance for the first time after you complete the hardware setup, use the First Time Configuration Wizard.

If you do not complete the wizard because of one of these conditions, the wizard will run again the next time you connect to the appliance:

- The browser window is closed.
- The appliance is restarted while you run the wizard.

After you complete the wizard, you can use the WebUI (Web User Interface) to change settings configured with the First Time Configuration Wizard and to configure advanced settings.

To open the WebUI, enter one of these addresses in the browser:

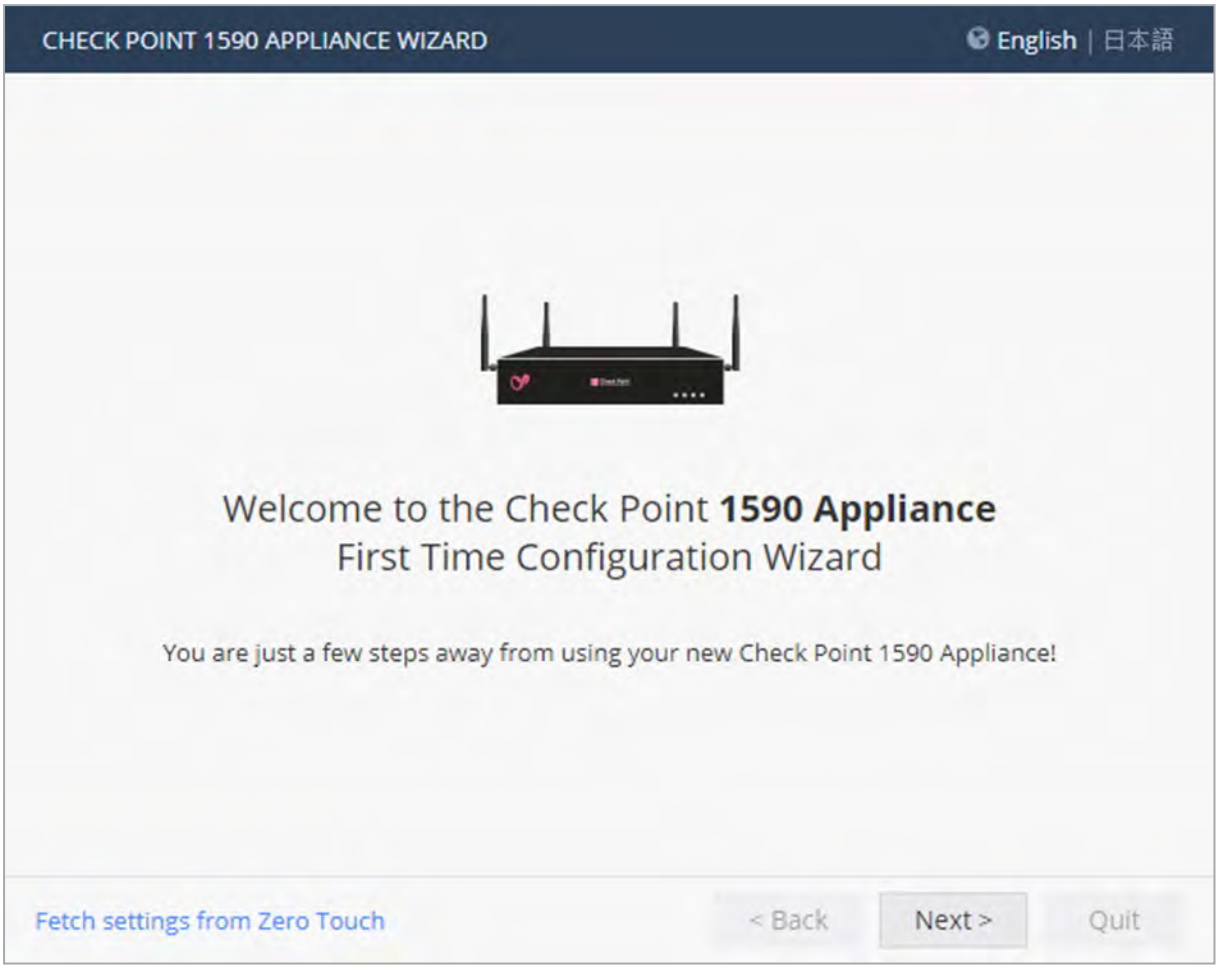
- https://my.firewall
- https://192.168.1.1:4434

If a security warning message shows, confirm it and continue.

The **First Time Configuration Wizard** runs.

Welcome

The **Welcome** page introduces the product and shows the name of your appliance.



You can connect to the Zero Touch server to fetch settings automatically from the cloud.

To change the language of the WebUI application:

Select the language link at the top of the page.

Note - Only English is allowed as the input language.

Zero Touch

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

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

If the gateway connects to the internet through DHCP, the gateway will fetch 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:

1. In the **Welcome** page, click **Fetch Settings from the cloud**.
2. In the window that opens, click **OK** to confirm that you want to proceed.
3. The **Internet connection** page opens. Configure your Internet connection and click **Connect**.
4. The **Fetching settings from the cloud** window opens and shows the **Connecting to the service provider** status. This process may take several minutes.
5. If you fail to connect, an error message appears. Possible errors include:
   - Internet connection is not configured correctly.
   - Internet connection is through a proxy server.
   - Zero Touch is already running.
   - Zero Touch service already completed.
   - The First Time Configuration Wizard already completed.
   - Zero Touch service is disabled.

   Where applicable, click **Retry** now to connect again.
6. After you connect to the server, the settings are automatically downloaded and installed. The status is shown in the **Fetching settings from the cloud** window. It may take several minutes until the installation is complete.
7. Click **Finish**.

Note - If a collision is detected between an internal network (LAN) and an IP returned using 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.

Authentication Details

In the **Authentication Details** page, enter the required details to log in to the Check Point 1590appliance WebUI application or if the wizard terminates abnormally:

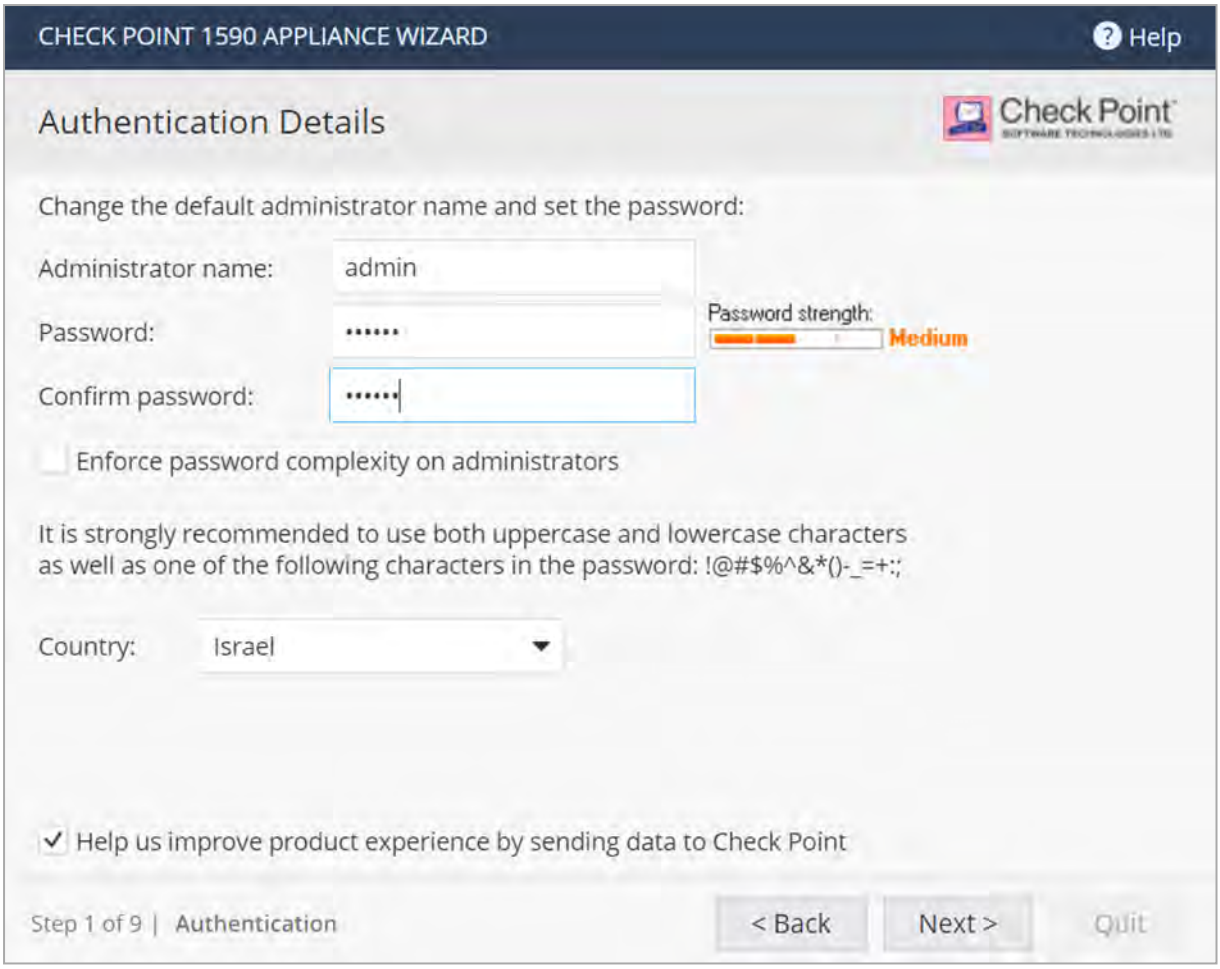
- **Administrator Name** - We recommend that you change the default "admin" login name of the administrator. The name is case sensitive.
- **Password** - A strong password has a minimum of 6 characters with at least one capital letter, one lower case letter, and a special character. Use the **Password strength** meter to measure the strength of your password.

  Note - The meter is only an indicator and does not enforce creation of a password with a specified number of character or character combination. To enforce password complexity, click the check box.
- **Confirm Password** - Enter the password again.
- **Country** - Select a country from the list (for wireless network models).

  The country where the license is set determines the wireless frequency and parameters, as the regulations vary according to region.

  If you are using a trial license, only **basic radio settings**, are allowed in all zones. A warning that selected wireless radio settings are not applied shows on the **Summary** page and also on the **Device** > **License** page. For more information on basic wireless radio settings, see sk159693.

  If you select a country and install a valid license, but the wireless region of the device does not match the selected country, a warning message shows and you must edit the country information. When the country and wireless region match, you see the full settings.

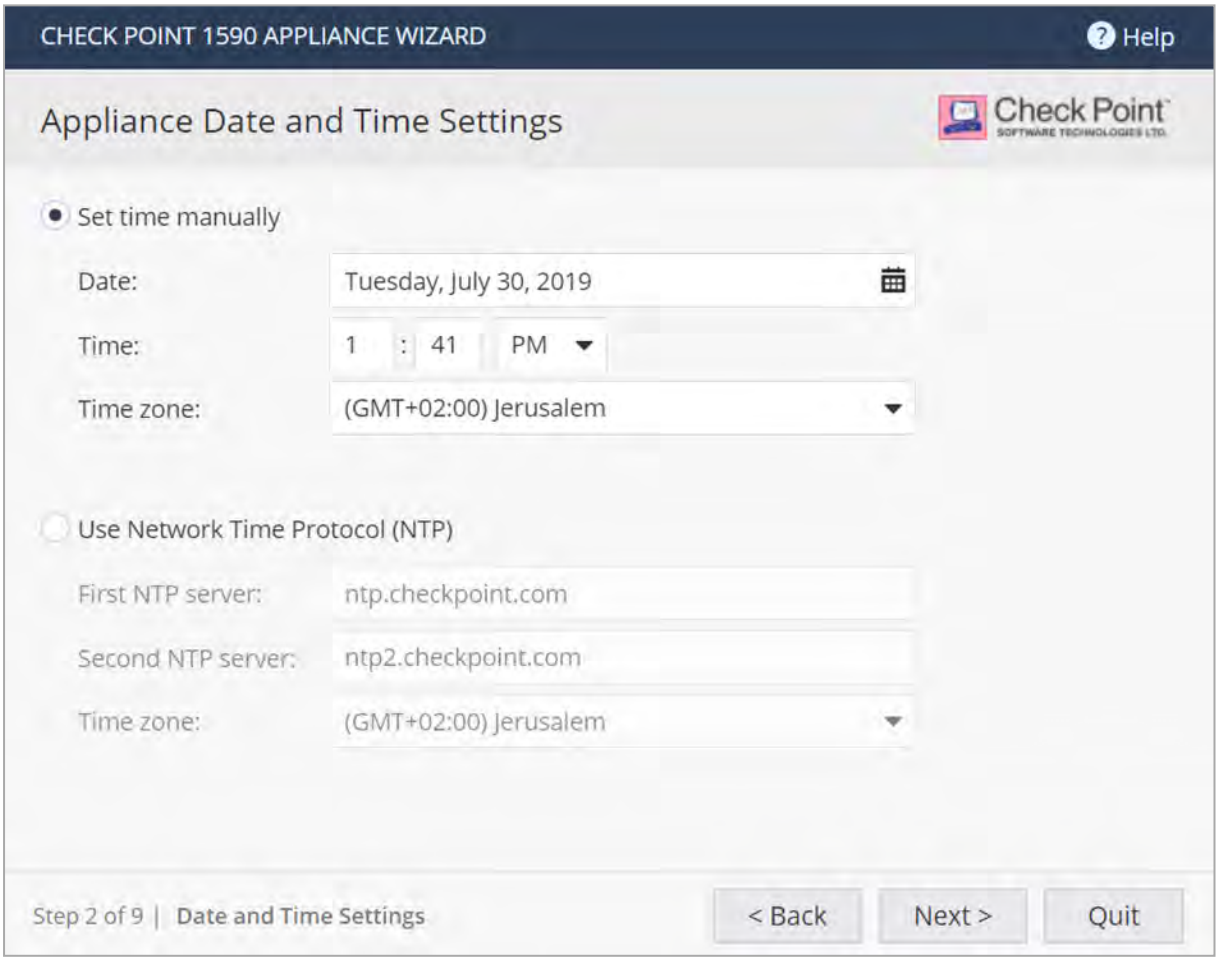

CHECK POINT 1590 APPLIANCE WIZARD
Help
Authentication Details
Check Point
Change the default administrator name and set the password:
Administrator name:
admin
Password:
Password strength:
Medium
Confirm password:
Enforce password complexity on administrators
It is strongly recommended to use both uppercase and lowercase characters as well as one of the following characters in the password: !@#$%^&*()-_=+:;
Country:
Israel
Help us improve product experience by sending data to Check Point
Step 1 of 9 | Authentication
< Back
Next >
Quit

Appliance Date and Time Settings

In the **Appliance Date and Time Settings** page, configure the appliance's date, time, and time zone settings manually or use the Network Time Protocol option.

When you set the time manually, the host computer's settings are used for the default date and time values. If necessary, change the time zone setting to show your correct location. Daylight Savings Time is automatically enabled by default. You can change this in the WebUI application on the **Device** > **Date and Time** page.

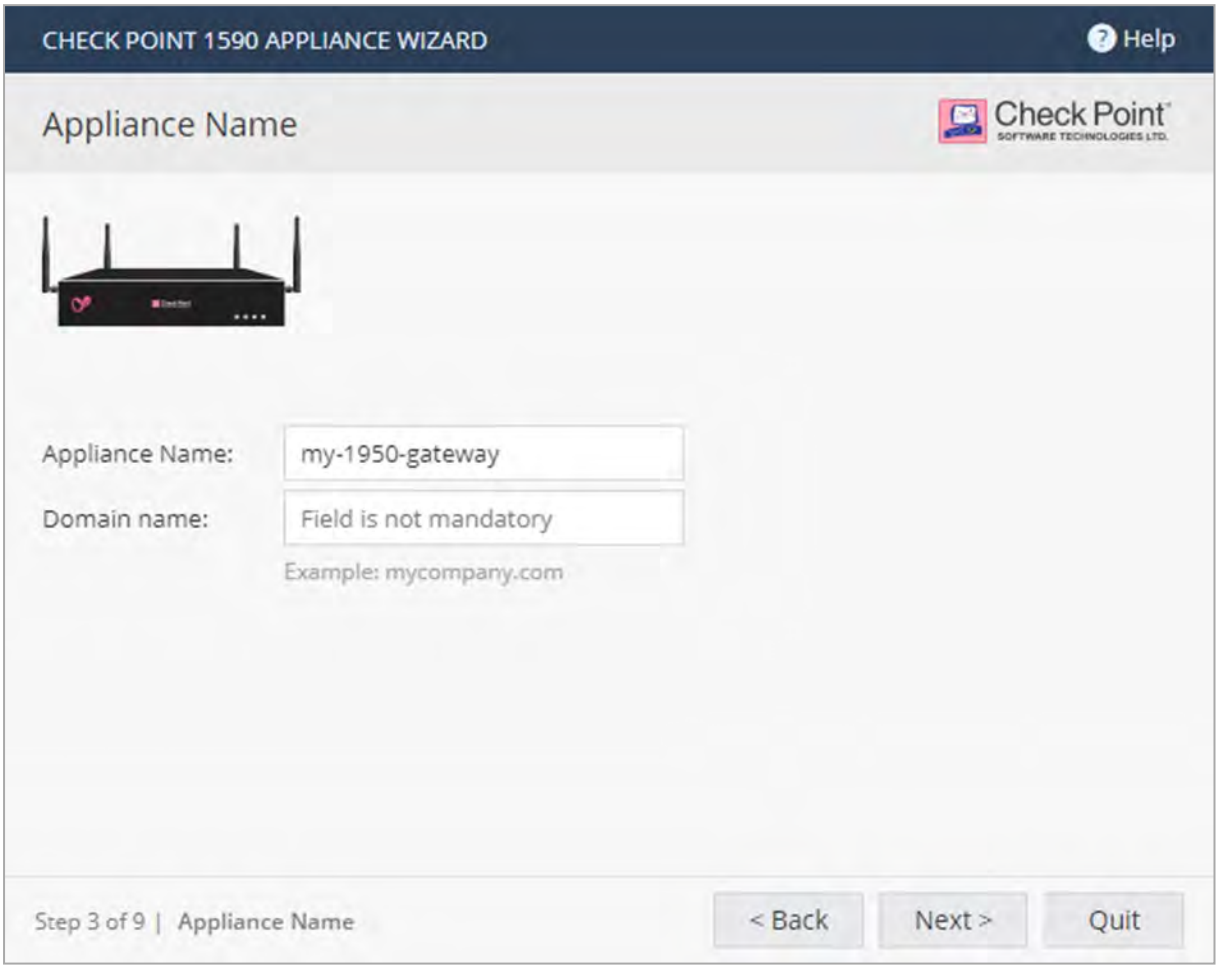
- **Date** - The host computer's date appears by default. If required, set a different date.
- **Time** - The host computer's time appears by default. If required, set a different time.
- **Time Zone** - The host computer's time zone appears by default. If required, select a time zone setting to reflect your exact location.
- **Primary NTP server** - The IP or host name of the primary NTP server. The default server is `ntp.checkpoint.com`
- **Secondary NTP server** - The IP or host name of the secondary NTP server. The default server is `ntp2.checkpoint.com`



Appliance Name

In the **Appliance Name** page, enter a name to identify the appliance, and enter a domain name (optional).

When the gateway performs DNS resolving for a specified object's name, the domain name is appended to the object name. This lets hosts in the network look up hosts by their internal names.

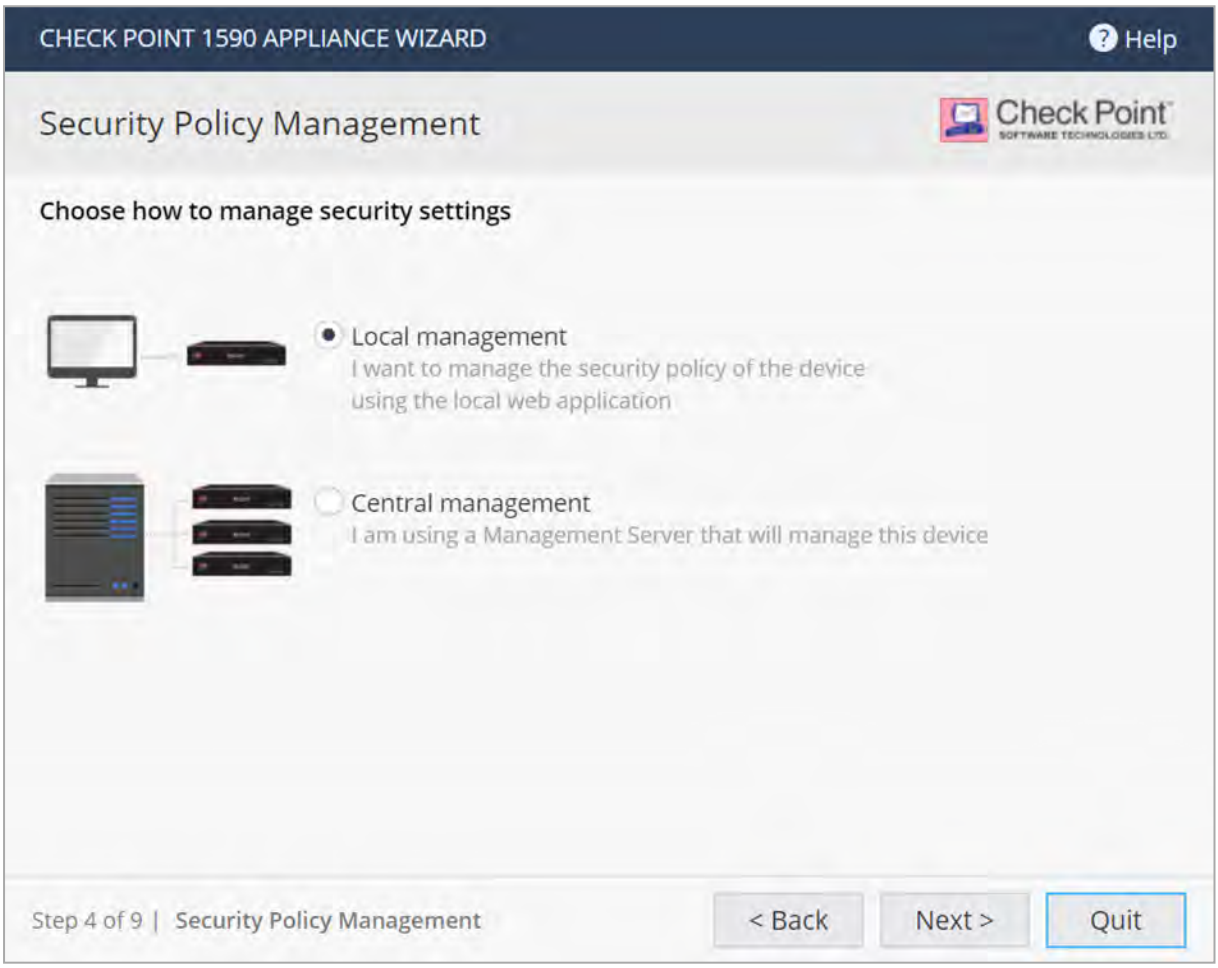


Security Policy Management

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.



Internet Connection

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

To configure Internet connection now:

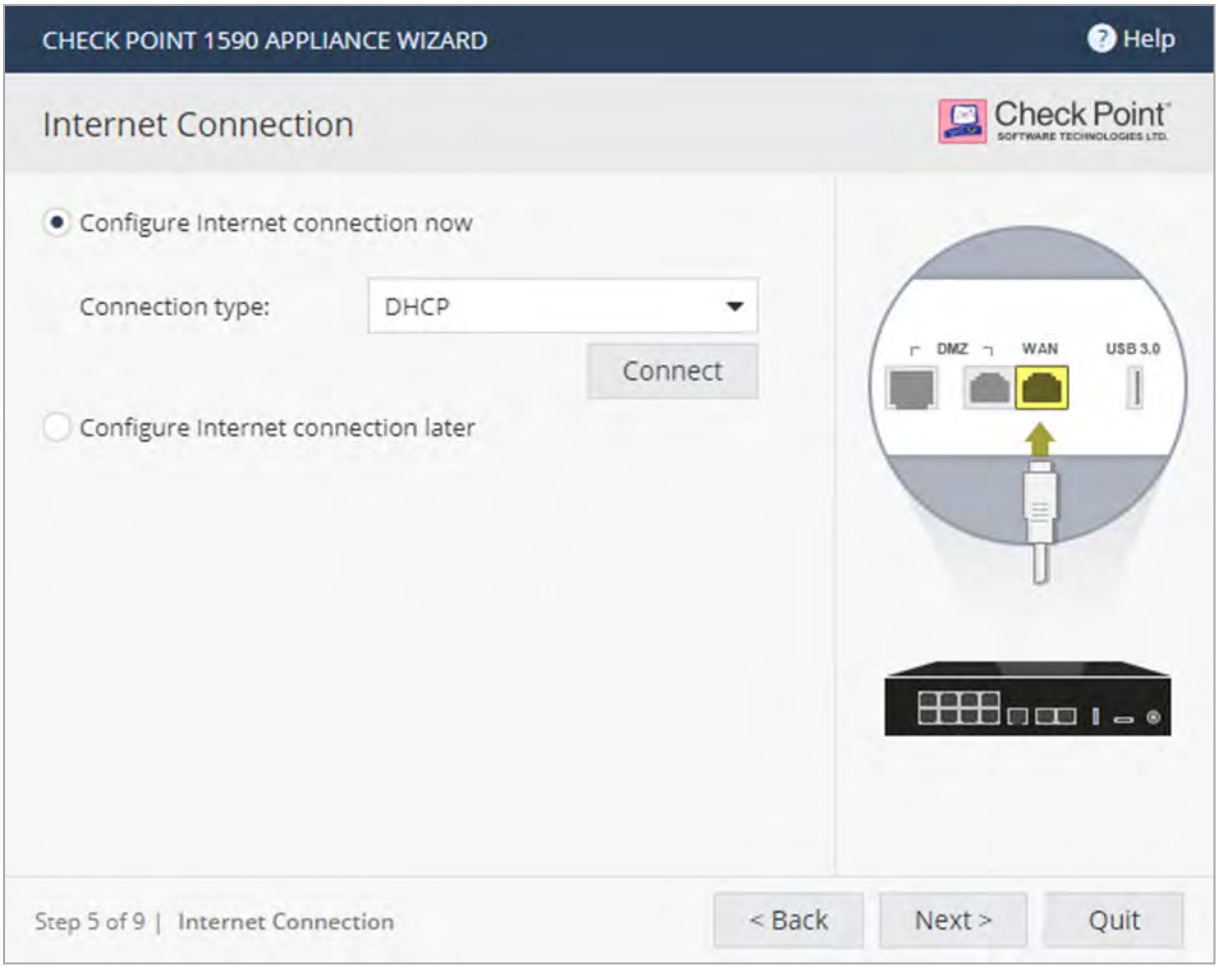
1. Select Configure Internet connection now.
2. From the Connection type drop down list, select the protocol used to connect to the Internet.
3. Enter the fields for the selected connection protocol. The information you must enter is different for each protocol. You can get it from your Internet Service 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.

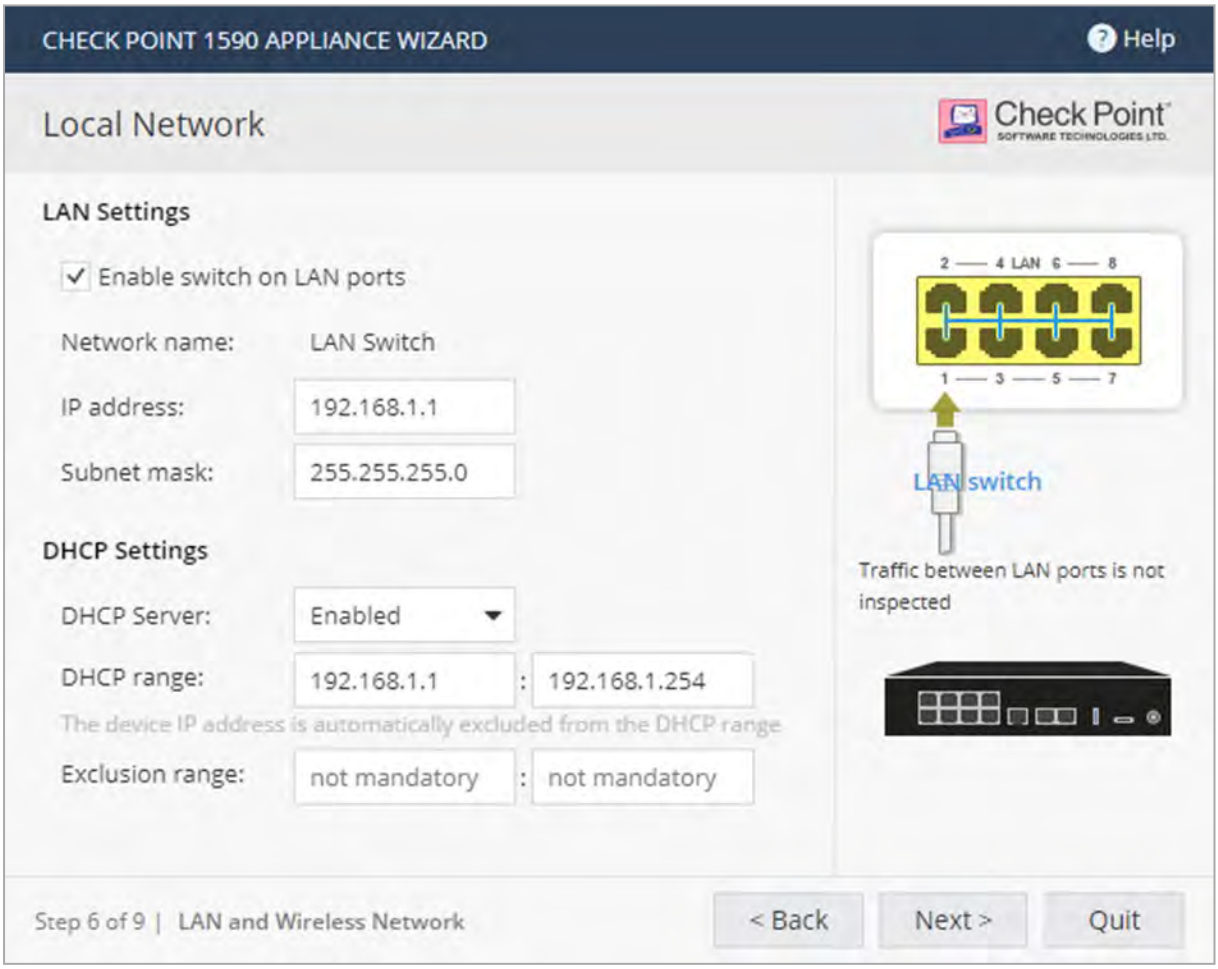

CHECK POINT 1590 APPLIANCE WIZARD
Help
Internet Connection
Check Point
SOFTWARE TECHNOLOGIES LTD.
Configure Internet connection now
Connection type:
DHCP
Connect
Configure Internet connection later
DMZ
WAN
USB 3.0
Step 5 of 9 | Internet Connection
< Back
Next >
Quit

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.



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:

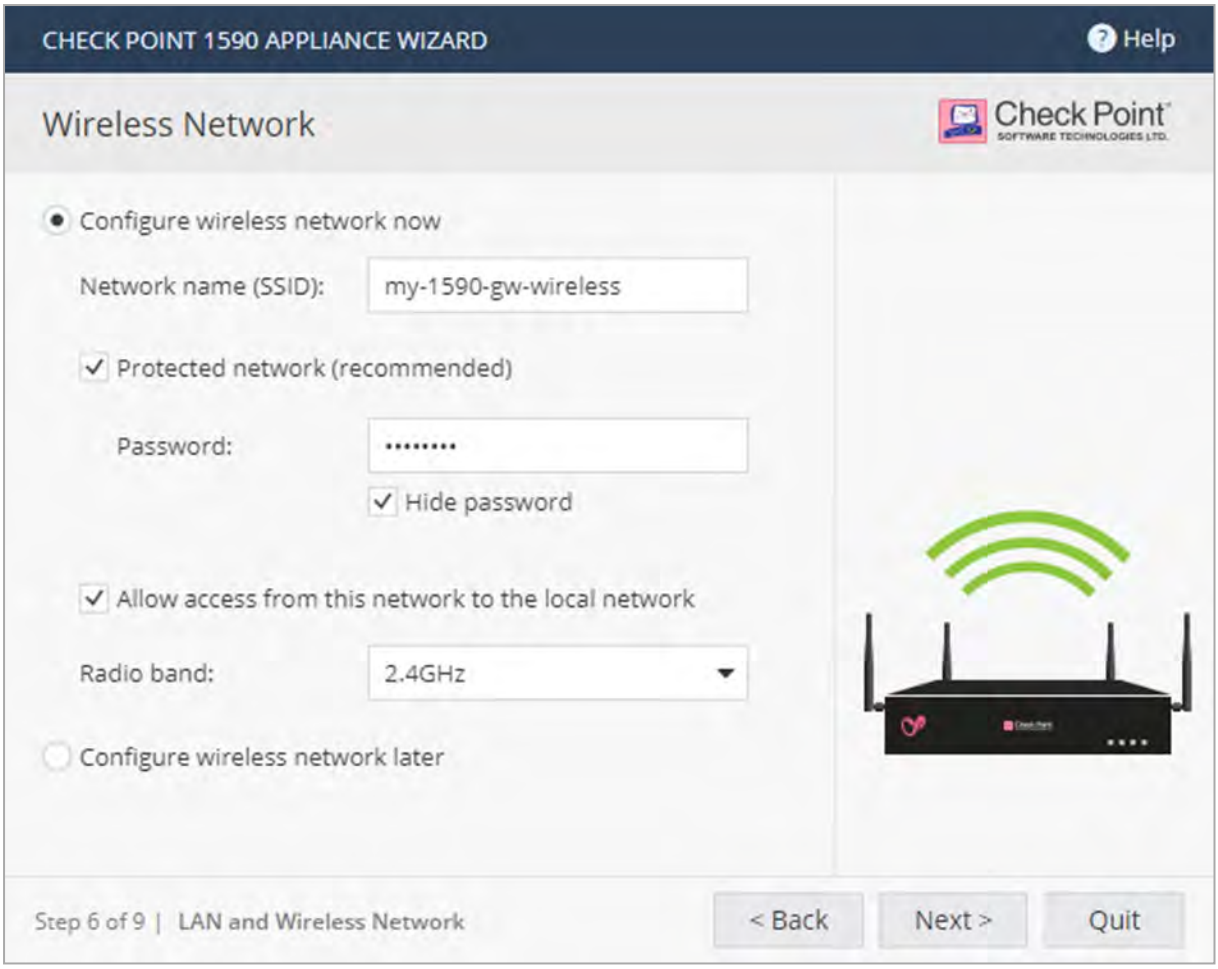
In the Wireless Network page, configure wireless connectivity details.

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 1590 APPLIANCE WIZARD
Help
Wireless Network
Check Point
SOFTWARE TECHNOLOGIES LTD.
Configure wireless network now
Network name (SSID):
my-1590-gw-wireless
Protected network (recommended)
Password:
Hide password
Allow access from this network to the local network
Radio band:
2.4GHz
Configure wireless network later
Step 6 of 9 | LAN and Wireless Network
< Back
Next >
Quit

Administrator Access

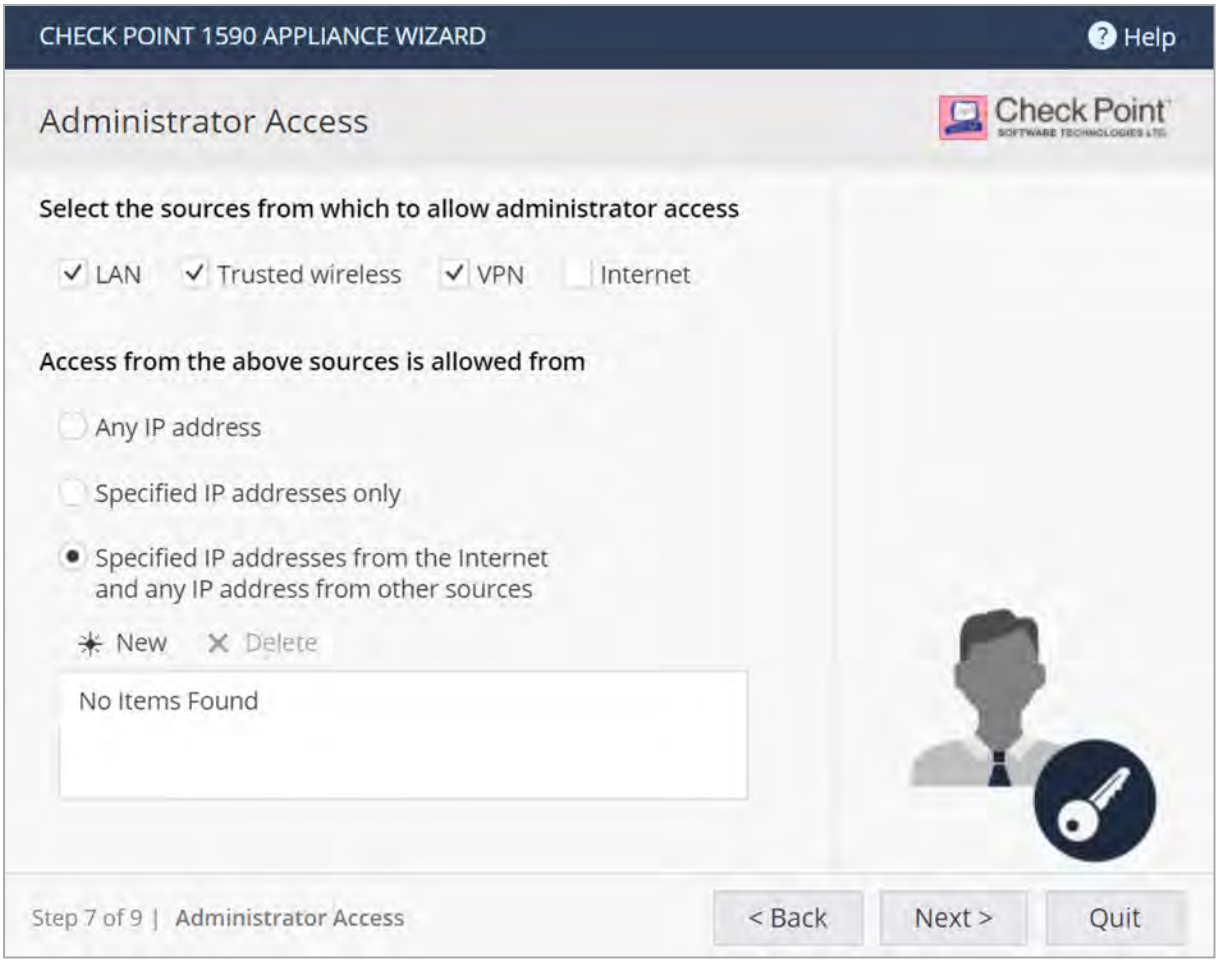
In the **Administrator Access** page, configure if administrators can use the appliance from a specified IP address or any IP address.

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 1590 APPLIANCE WIZARD
Help
Administrator Access
Check Point
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
New
Delete
No Items Found
Step 7 of 9 | Administrator Access
< Back
Next >
Quit

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.

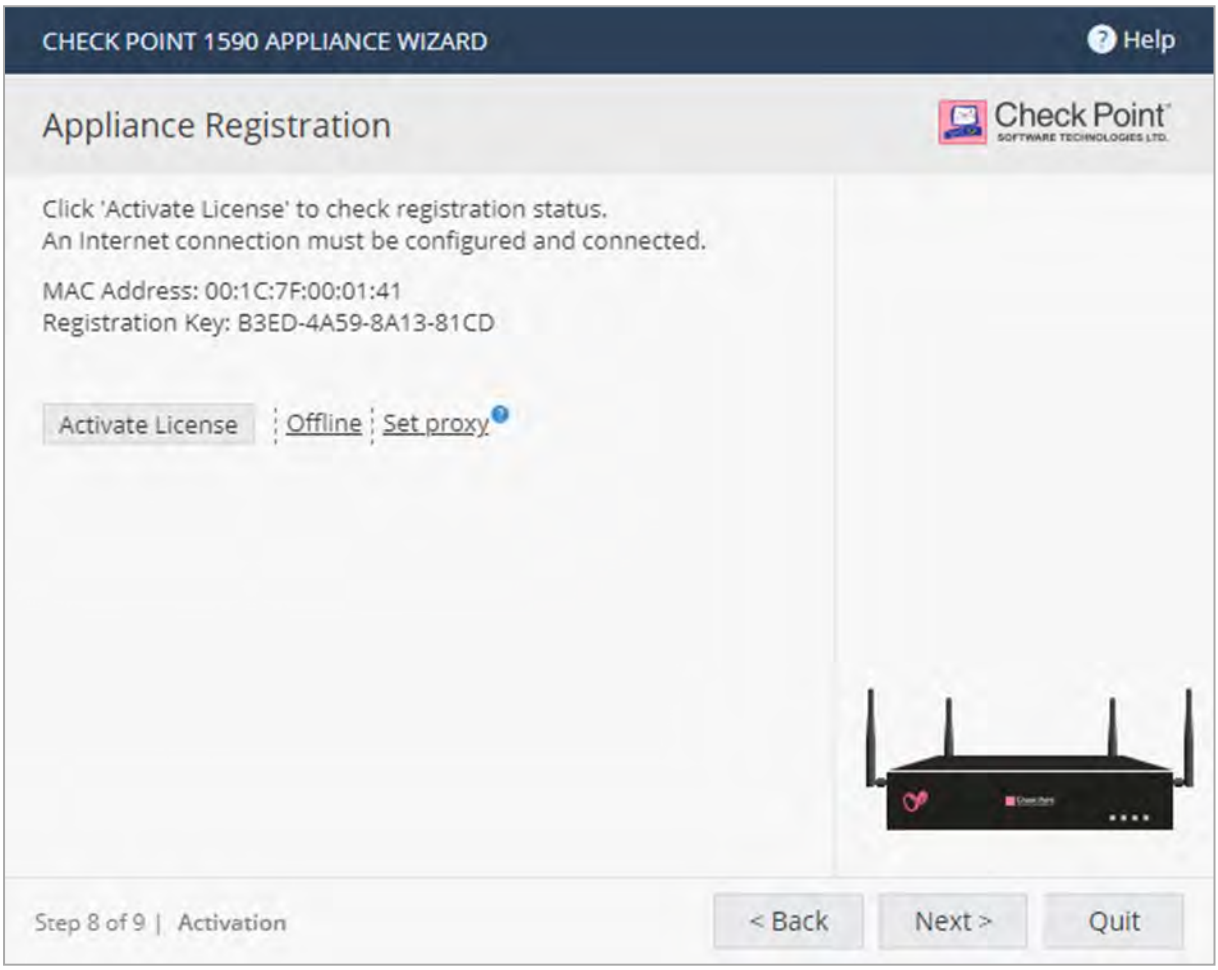
To postpone appliance registration and get a 30-day trial license:

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.



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.

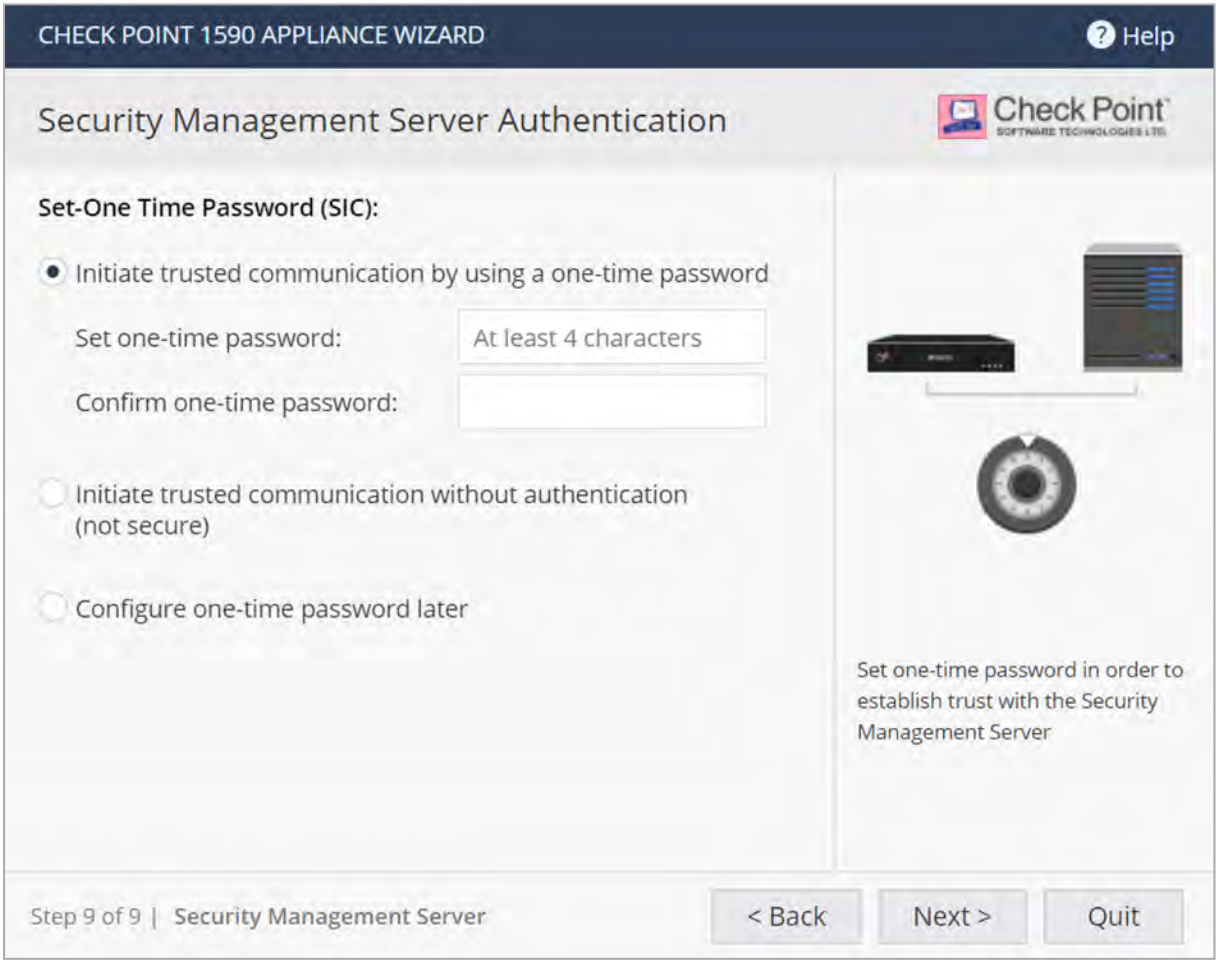
Select an option to authenticate trusted communication with the Security Management Server:

- **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.



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.

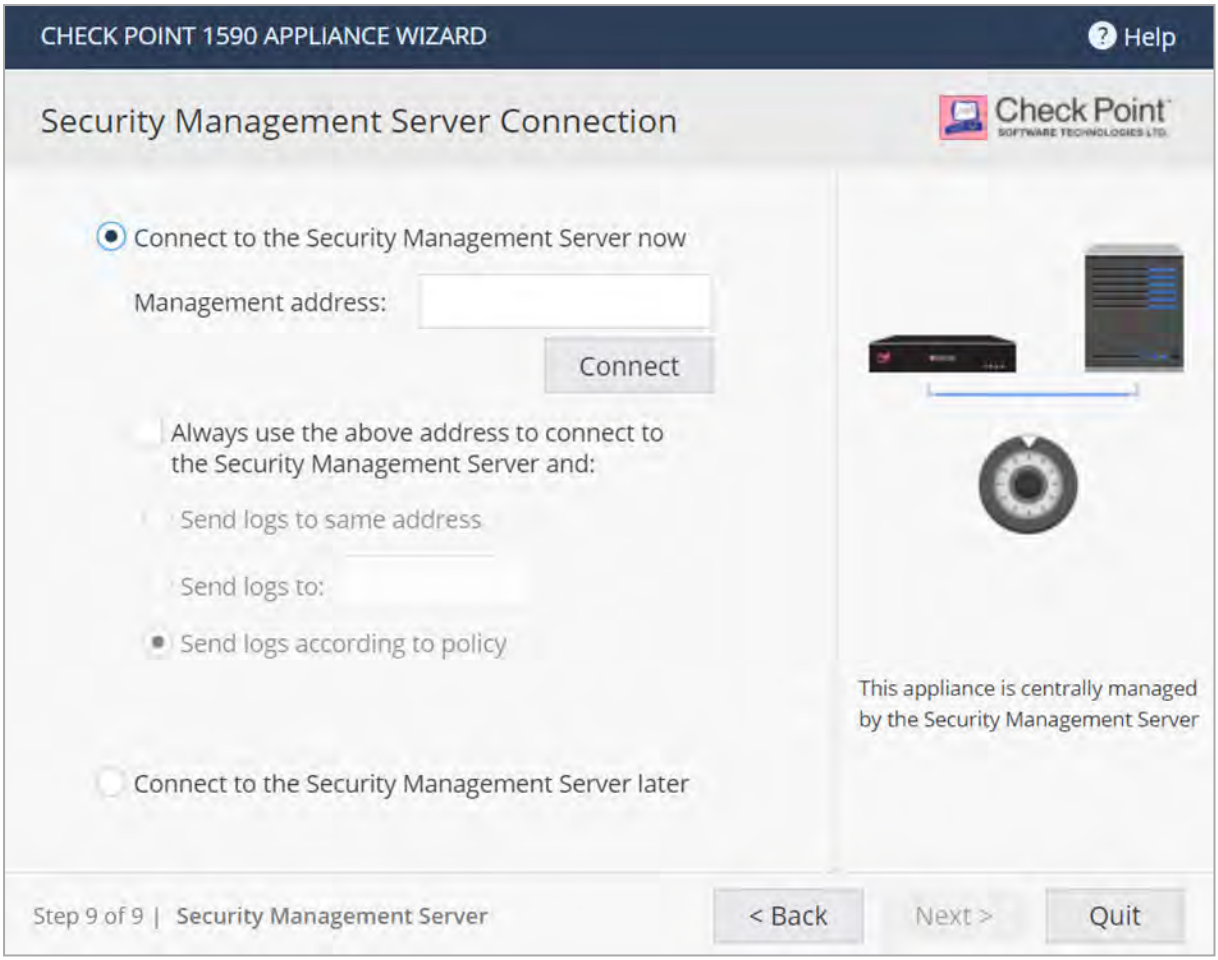
  If you enter an IP address, it will override the automatic mechanism that determines the routable IP address of the Security Management Server for each appliance.

  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:

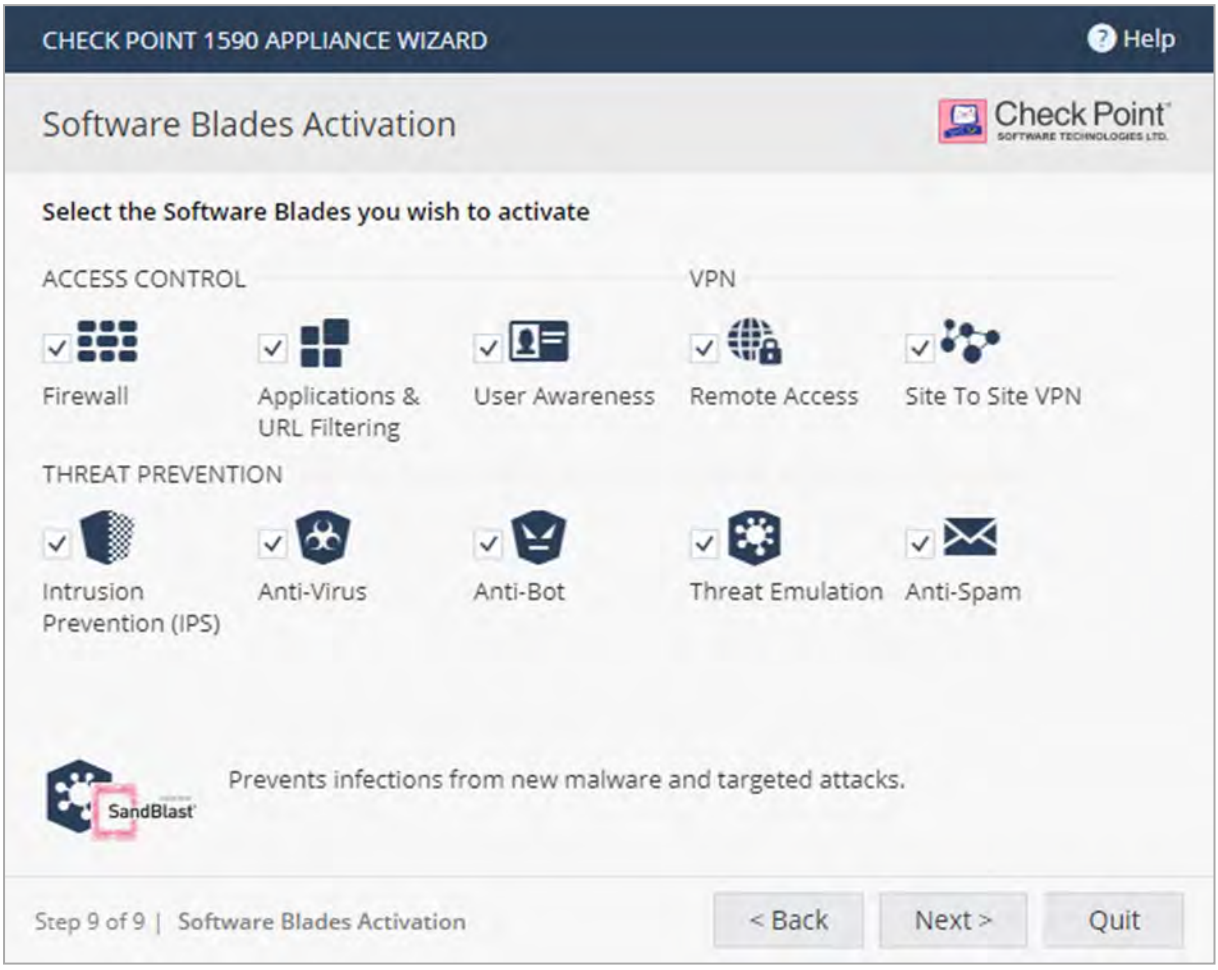
  - **Send logs to same address** - The logs are sent to the IP address entered on this page for the Security Management Server.
  - **Send logs to** - Enter the IP address of a log server.
  - **Send logs according to policy** - The logs are sent according to the log server definitions that are defined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


CHECK POINT 1590 APPLIANCE WIZARD
Help
Security Management Server Connection
Check Point
SOFTWARE TECHNOLOGIES LTD.
Connect to the Security Management Server now
Management address:
Connect
Always use the above address to connect to the Security Management Server and:
Send logs to same address
Send logs to:
Send logs according to policy
Connect to the Security Management Server later
This appliance is centrally managed by the Security Management Server
Step 9 of 9 | Security Management Server
< Back
Next >
Quit

Software Blade Activation

Select the Software Blades to activate on this appliance.

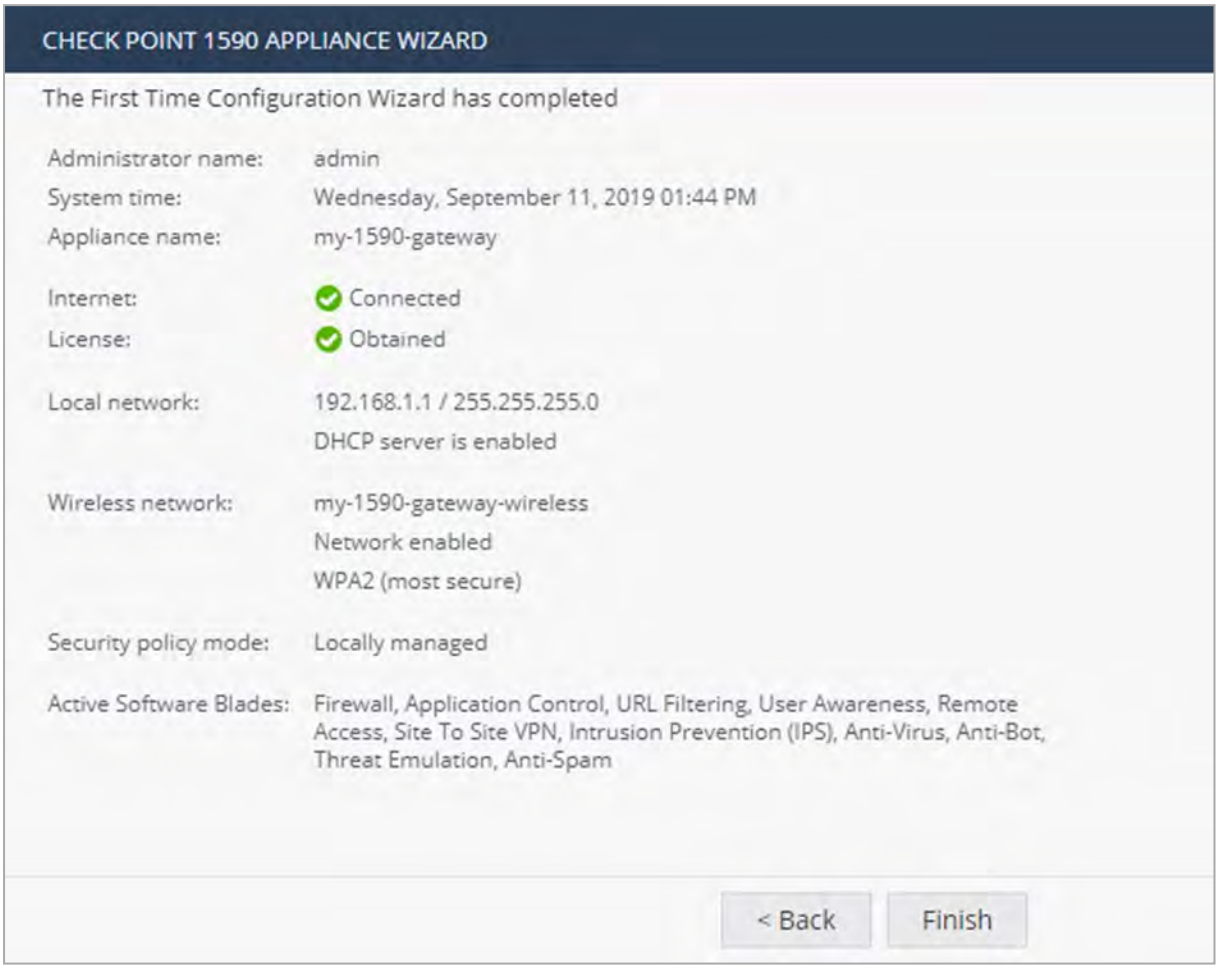
QoS (bandwidth control) can only be activated from the WebUI after completing the First Time Configuration Wizard.



Summary

The **Summary** page shows the details of the elements configured with the First Time Configuration Wizard.

Click **Finish** to complete the First Time Configuration Wizard.



The WebUI opens on the **Home** > **System** page.

To back up the system configuration in the WebUI:

Go to **Device** > **System Operations** > **Backup**.

Zero Touch Cloud Service

The Zero Touch Cloud Service lets you easily manage the initial deployment of your gateways in the Zero Touch portal.

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

Note - If you already used the First Time Configuration Wizard to configure your appliance, you cannot use the Zero Touch Cloud service. If you start the First Time Configuration Wizard while the Zero Touch settings are being installed, the installation process terminates.

If the gateway connects to the internet via DHCP, the gateway will fetch 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**.

   The settings are automatically downloaded and installed.

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

When you reconnect to the WebUI or click **Refresh**, you may see one of these:

- **Login** page - This means the process ended successfully and your settings are installed.
- **Welcome** page of the First Time Configuration Wizard - The process is still running. The settings are installing or they do not exist in the cloud.

  Note - If you click **Next** on the **Welcome** page, the Zero Touch settings installation process terminates
- **Page not found** - The appliance local IP address may have been changed by the cloud settings installation. Try `http://my.firewall` or consult your administrator for the new local IP address.

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

For more information on how to use Zero Touch, see sk116375 and the R80.20 Zero Touch Web Portal Admin Guide.

Retries mechanism:

During cloud activation, there are sometimes temporary issues which prevent the gateway from activating Cloud Services. See the Management LED description in the *"Front Panel" on page 14* section.

USB Drive or SD Card

The USB drive or SD card can be used for rapid deployment of configuration files, or to install an image, 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.

Health and Safety Information

Read these warnings before setting up or using the appliance.

Warning - Do not block air vents. A minimum 1/2 inch clearance is required.

Warning - This appliance does not contain any user-serviceable parts. Do not remove any covers or attempt to gain access to the inside of the product. Opening the device or modifying it in any way has the risk of personal injury and will void your warranty. The following instructions are for trained service personnel only.

Power Supply Information

To reduce potential safety issues with the DC power source, only use one of these:

- The AC adapter supplied with the appliance.
- A replacement AC adapter supplied by Check Point.
- An AC adapter purchased as an accessory from Check Point.

To prevent damage to any system, it is important to handle all parts with care. These measures are generally sufficient to protect your equipment from static electricity discharge:

- Restore the communications appliance system board and peripherals back into the antistatic bag when they are not in use or not installed in the chassis. Some circuitry on the system board can continue operating when the power is switched off.
- Do not allow the lithium battery cell used to power the real-time clock to short. The battery cell may heat up under these conditions and present a burn hazard.

  Warning - DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

- Do not dispose of batteries in a fire or with household waste.
- Contact your local waste disposal agency for the address of the nearest battery deposit site.
- Disconnect the system board power supply from its power source before you connect or disconnect cables or install or remove any system board components. Failure to do this can result in personnel injury or equipment damage.
- Avoid short-circuiting the lithium battery; this can cause it to superheat and cause burns if touched.
- Do not operate the processor without a thermal solution. Damage to the processor can occur in seconds.

IMPORTANT SAFETY INSTRUCTIONS: When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.
- This equipment is not suitable for use in locations where children are likely to be present.
- Make sure to connect the power cord to a socket-outlet with a grounded connection.
- Never open the equipment. For safety reasons, the equipment should be opened only by a qualified skilled person.

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.

For California:

Perchlorate Material - special handling may apply. See http://www.dtsc.ca.gov/hazardouswaste/perchlorate

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

Proposition 65 Chemical

Chemicals identified by the State of California, pursuant to the requirements of the California Safe Drinking Water and Toxic Enforcement Act of 1986, California Health & Safety Code s. 25249.5, et seq. ("Proposition 65"), that is "known to the State to cause cancer or reproductive toxicity." See http://www.calepa.ca.gov.

WARNING:

Handling the cord on this product will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Declaration of Conformity

Manufacturer's Name:	Check Point Software Technologies Ltd.
Manufacturer's Address:	5 Shlomo Kaplan Street, Tel Aviv 67897, Israel
Model Number:	V-81, *V-81W, *V-81WL
Product Options:	1570/1590 Appliance Wired, 1570/1590 Appliance WiFi, 1570/1590 Appliance LTE-WiFi
Date First Applied:	August 2019

Declares under our sole responsibility, that the products: Conform to the following Product Specifications:

RF/Wi-Fi (* marked model)

Certification New	Type
CE EN 55032:2015 + AC:2016, Class B CE EN 55032:2012 + AC:2013, Class B CE EN 55024:2010 / A1:2015 CE EN 55024:2010 FCC Part15B ICES-003 AS/NZS CISPR32 VCCI, V-3/2015.4 , V4/2012.04,Class B VCCI CISPR 32:2016 * EN300 328 * EN301 893 * ETSI EN301 489-1 * ETSI EN301 489-1-17 * EN62311:2008 * EN50386:2002, EN50383:2010 * AS/NZS 4268:2017 * FCC Part15C+E * RSS-247 * RSS-102 * JP ARIB STD-T66 * JP ARIB STD-T71	EMC, *RF/Wi-Fi
IEC 62368-1 UL 62368-1	Safety

Date and Place of Issue: August 2019, Tel Aviv, Israel

Federal Communications Commission (FCC) Statement:

FCC SDOC

According to FCC Part 15

We, Check Point Software Technologies Ltd.

Address: Shlomo Kaplan St 5, / HaSolelim St 5 Tel Aviv-Yafo # 67897, Phone: +972-3-753-4555.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 29 centimeters between the radiator and your body.

For Country Code Selection Usage (WLAN Devices)

Note: The country code selection is for non-US models only and is not available to all US models. Per FCC regulation, all WiFi products marketed in the US must be fixed to US operation channels only.

Customer Information - Part 68 Statement

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of the device that contains, among other information, a product identifier in the format US: FK1DL01AL71WD. If requested, this number must be provided to the telephone company.

Applicable connector jack Universal Service Order Codes ("USOC”) for the Equipment is RJ11-C.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:

FK1DL01AL71WD. The digits represented by 0.1 are the REN without a decimal point (e.g., 03 is a REN of 0.3).

If this Gateway causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this Gateway, for repair or warranty information, please contact:

Check Point

6330 Commerce Drive Suite 120, Irving, Texas 75063

Office Phone Numbers 972-444-6612

If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this equipment does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

WHEN PROGRAMMING EMERGENCY NUMBERS AND(OR) MAKING TEST CALLS TO EMERGENCY NUMBERS:

1. Remain on the line and briefly explain to the dispatcher the reason for the call.
2. Perform such activities in the off-peak hours, such as early morning or late evenings.

Canadian Department Compliance Statement

This radio transmitter [IC: 7849A-WLE1216V220, IC: 7849A-WLE1216V520] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [IC: 7849A-WLE1216V220, IC: 7849A-WLE1216V520] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Frequency Band	Antenna Type	Max. Gain	Impedance Ω
2414-2462 MHz	Dipole Antenna (RP-SMA)	2.22 dBi	50Ω
5180-5240MHz, 5745-5825MHz	Dipole Antenna (RP-SMA)	4.29 dBi	50Ω

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 29 cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 29 cm de distance entre la source de rayonnement et votre corps.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage, et
2. L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter, except tested built-in radios.

Cet appareil et son antenne ne doivent pas être situés ou fonctionner en conjonction avec une autre antenne ou un autre émetteur, exception faites des radios intégrées qui ont été testées.

The County Code Selection feature is disabled for products marketed in the US/ Canada.

La fonction de sélection de l'indicatif du pays est désactivée pour les produits commercialisés aux États-Unis et au Canada.

FOR WLAN 5 GHz DEVICE:

Caution :

1. The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
2. The maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and
3. The maximum antenna gain permitted for devices in the band 5725-5850 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.
4. The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) shall be clearly indicated. (For 5G B2 with DFS devices only)
5. Where applicable, antenna type(s), antenna models, and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.
6. Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

1. Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
2. Le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5470-5725 MHz doit se conformer à la limite de p.i.r.e.;
3. Le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.
4. Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3), doivent être clairement indiqués. (Pour 5G B2 avec les périphériques DFS uniquement)
5. De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

NOTICE: This equipment meets the applicable ISED Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that ISED technical specifications were met. It does not imply that ISED approved the equipment.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 01. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Industry Canada Statement

This device complies with ISED's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with greater than 29 cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 29 cm entre le radiateur et votre corps.

Detachable Antenna Usage

This radio transmitter (IC: 2417C-EM7455 / Model: EM7455) has been approved by ISED to operate with the antenna type listed below with maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (IC: 2417C-EM7455 / Model: EM7455) a été approuvé par ISED pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Approved Antenna(s) List

Type	Gain	Brand	Manufacturer
Dipole	3.2dBi	-	-

Japan Class A Compliance Statement:

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

European Union (EU) Electromagnetic Compatibility Directive

This product is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive (2014/30/EU).

This product is in conformity with Low Voltage Directive 2014/35/EU, and complies with the requirements in the Council Directive 2014/35/EU relating to electrical equipment designed for use within certain voltage limits and the Amendment Directive 93/68/EEC.

Product Disposal

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office or your household waste disposal service.

Information sur la Santé et la Sécurité

Avant de mettre en place ou d'utiliser l'appareil, veuillez lire les avertissements suivants.

Avertissement - .ne pas obturer les aérations. Il faut laisser au moins 1,27 cm d'espace libre.

Avertissement - cet appareil ne contient aucune pièce remplaçable par l'utilisateur. Ne pas retirer de capot ni tenter d'atteindre l'intérieur. L'ouverture ou la modification de l'appareil peut entraîner un risque de blessure et invalidera la garantie. Les instructions suivantes sont réservées à un personnel de maintenance formé.

Information pour l'alimentation

Pour limiter les risques avec l'alimentation CC, n'utilisez que l'une des solutions suivantes :

- L'adaptateur secteur fourni avec l'appareil
- Un adaptateur secteur de remplacement, fourni par Check Point
- Un adaptateur secteur acheté en tant qu'accessoire auprès de Check Point

Pour éviter d'endommager tout système, il est important de manipuler les éléments avec soin. Ces mesures sont généralement suffisantes pour protéger votre équipement contre les décharges d'électricité statique :

- Remettez dans leur sachet antistatique la carte système et les périphériques de l'appareil de communications lorsqu'ils ne sont pas utilisés ou installés dans le châssis. Certains circuits sur la carte système peuvent rester fonctionnels lorsque si l'appareil est éteint.
- Ne jamais court-circuiter la pile au lithium (qui alimente l'horloge temps-réel). Elle risque de s'échauffer et de causer des brûlures.

  Avertissement - DANGER D'EXPLOSION SI LA PILE EST MAL REMPLACÉE. NE REMPLACER QU'AVEC UN TYPE IDENTIQUE OU ÉQUIVALENT, RECOMMANDÉ PAR LE CONSTRUCTEUR. LES PILES DOIVENT ÊTRE MISES AU REBUT CONFORMÉMENT AUX INSTRUCTIONS DE LEUR FABRICANT.
- Ne pas jeter les piles au feu ni avec les déchets ménagers.
- Pour connaître l'adresse du lieu le plus proche de dépôt des piles, contactez votre service local de gestion des déchets.
- Débrancher l'alimentation de la carte système de sa source électrique avant de connecter ou déconnecter des câbles ou d'installer ou retirer des composants. À défaut, les risques sont d'endommager l'équipement et de causer des blessures corporelles.
- Ne pas court-circuiter la pile au lithium : elle risque de surchauffer et de causer des brûlures en cas de contact.
- Ne pas faire fonctionner le processeur sans refroidissement. Le processeur peut être endommagé en quelques secondes.

INSTRUCTIONS DE SÉCURITÉ IMPORTANTES : Lorsque vous utilisez votre équipement téléphonique, des précautions de sécurité élémentaires doivent toujours être respectées afin de réduire le risque incendie, d'électrocution ou de blessures, comme celles qui suivent :

- Ne pas utiliser ce produit à proximité de l'eau, par exemple près d'une baignoire, d'un lavabo, d'un évier de cuisine ou de buanderie, dans un sous-sol humide ou près d'une piscine.
- Evitez d'utiliser un téléphone (autre qu'un téléphone sans fil) par temps de foudre. Les éclaires impliquent un risque faible d'électrocution.
- N'utilisez pas la téléphone pour signaler une fuite de gaz si vous vous tenez près de cette fuite.
- Utilisez uniquement le cordon alimentation et les piles indiquées dans ce manuel. Ne pas jeter les piles au feu. Elles risquent d'exploser. Consultez les réglementations locales pour toute instruction spécifique concernant leur élimination.
- Cet équipement ne convient pas pour une utilisation dans des endroits où des enfants sont susceptibles d'être présents.
- Veillez à connecter le cordon d'alimentation à une prise de courant reliée à la terre.
- N'ouvrez jamais l'équipement. Pour des raisons de sécurité, les équipements ne doivent être ouverts que par un homme de métier qualifié.

SAUVEGARDEZ CES INSTRUCTIONS

ATTENTION : Pour réduire tout risque d'incendie, utilisez uniquement un cordon de ligne téléphonique 26 AWG ou plus large (ex. 24 AWG) homologué UL et certifié CSA.

Pour la Californie :

Matériau perchloraté : manipulation spéciale potentiellement requise. Voir http://www.dtsc.ca.gov/hazardouswaste/perchlorate

L'avis suivant est fourni conformément au California Code of Regulations, titre 22, division 4.5, chapitre 33. Meilleures pratiques de manipulation des matériaux perchloratés. Ce produit, cette pièce ou les deux peuvent contenir une pile au dioxyde de lithium manganèse, qui contient une substance perchloratée.

Produits chimiques « Proposition 65

Les produits chimiques identifiés par l'état de Californie, conformément aux exigences du California Safe Drinking Water and Toxic Enforcement Act of 1986 du California Health & Safety Code s. 25249.5, et seq. (« Proposition 65 »), qui sont « connus par l'état pour être cancérigène ou être toxiques pour la reproduction » (voir http://www.calepa.ca.gov)

AVERTISSEMENT :

La manipulation de ce cordon vous expose au contact du plomb, un élément reconnue par l'état de Californie pour être cancérigène, provoquer des malformations à la naissance et autres dommages relatifs à la reproduction. Se laver les mains après toute manipulation.

Déclaration de conformité

Nom du constructeur :	Check Point Software Technologies Ltd.
Adresse du constructeur :	5 Shlomo Kaplan Street, Tel Aviv 67897, Israel
Numéro de modèle :	V-81, *V-81W, *V-81WL
Options de produit :	1570/1590 Appliance Wired,1570/1590 Appliance WiFi, 1570/1590 Appliance LTE-WiFi
Date de demande initiale :	Aout 2019

Déclare sous son entière responsabilité que les produits sont conformes aux normes produit suivantes :

RF/Wi-Fi (modèle signalé par *)

Certification Nouvelle	Type
CE EN 55032:2015 + AC:2016, Class B CE EN 55032:2012 + AC:2013, Class B CE EN 55024:2010 / A1:2015 CE EN 55024:2010 FCC Part15B ICES-003 AS/NZS CISPR32 VCCI, V-3/2015.4 , V4/2012.04,Class B VCCI CISPR 32:2016 * EN300 328 * EN301 893 * ETSI EN301 489-1 * ETSI EN301 489-1-17 * EN62311:2008 * EN50386:2002, EN50383:2010 * AS/NZS 4268:2017 * FCC Part15C+E * RSS-247 * RSS-102 * JP ARIB STD-T66 * JP ARIB STD-T71	EMC, *RF/Wi-Fi
IEC 62368-1 UL 62368-1	Sécurité

Date et lieu d'émission : Aout 2016, Tel Aviv, Israël

Déclaration à la Federal Communications Commission (FCC) :

Selon section 15 des réglementations de la FCC

Nous, Check Point Software Technologies Ltd.

Adresse: Shlomo Kaplan St 5, / HaSolelim St 5 Tel Aviv-Yafo # 67897, Phone: +972-3-753-4555.

Ce dispositif est conforme à la section 15 des réglementations de la FCC. Son fonctionnement est soumis aux deux conditions suivantes : (1) Cet appareil ne doit pas causer d'interférence préjudiciable et (2) Cet appareil doit tolérer toute interférence reçue, y compris celles qui pourraient causer un fonctionnement indésirable.

Partie responsable

Nom de la compagnie: Check Point Software Technologies Inc.

Adresse de la compagnie: 959 Skyway Road Suite 300, San Carlos, CA 94070

Téléphone: 1-800-429-4391

Cet équipement a été testé et déclaré conforme aux limites pour appareils numériques de classe B, selon la section 15 des règlements de la FCC. Ces limitations sont conçues pour fournir une protection raisonnable contre les interférences nocives dans un environnement résidentiel. Cet appareil génère, et peut diffuser des fréquences radio et, dans le cas d'une installation et d'une utilisation non conforme aux instructions, il peut provoquer des interférences nuisibles aux communications radio. Cependant, il n'existe aucune garantie qu'aucune interférence ne se produira dans le cadre d'une installation particulière. Si cet appareil provoque des interférences avec un récepteur radio ou un téléviseur, ce qui peut être détecté en mettant l'appareil sous et hors tension, l'utilisateur peut essayer d'éliminer les interférences en suivant au moins l'une des procédures suivantes :

- Réorienter ou déplacer l'antenne de réception.
- Augmenter la distance entre l'appareil et le récepteur.
- Brancher l'appareil sur une prise appartenant à un circuit différent de celui sur lequel est branché le récepteur.
- Consulter le distributeur ou un technicien radio/télévision qualifié pour obtenir de l'aide.

FCC Attention

- Tout changement ou modification non expressément approuvé par la partie responsable de la conformité pourrait empêcher l'utilisateur autorisé de faire fonctionner cet appareil.
- Cet émetteur ne doit pas être installé ou utilisé en conjonction avec d'autres antennes ou émetteurs.
- Les opérations dans la bande 5.15-5.25GHz sont limitées à une utilisation en intérieur.

Déclaration à la FCC sur l'exposition aux rayonnements

Cet équipement respecte les limites de la FCC en matière d'exposition aux rayonnements radio, pour un environnement non contrôlé. Cet équipement doit être installé et utilisé en réservant au moins 29 cm entre l'élément rayonnant et l'utilisateur.

Concernant la sélection du code pays (appareils WLAN)

Remarque: la sélection du code pays est uniquement pour les modèles hors Etats-Unis, et reste indisponible pour tout modèle vendus aux États-Unis. Selon la règlementation FCC tous les produits WIFI commercialisés aux Etats-Unis sont fixés uniquement sur des canaux américains.

Information client – Déclaration de la section 68

Cet équipement répond aux règles de la section 68 du Code des règlements fédéraux (FCC) et aux exigences adoptées par l'ACTA. Au bas de l'appareil est indiqué, entre autres informations, un identifiant produit au format US : FK1DL01AL71WD. Si besoin, ce numéro devra être fourni à la compagnie de téléphone.

Le code USOC (Universal Service Order Code) du connecteur applicable pour l'équipement est RJ11-C (connecteur courant continu).

La prise et le connecteur utilisés pour brancher cet équipement au câblage et au réseau téléphonique sur place doit répondre aux règles de la section 68 du FCC et aux exigences adoptées par l'ACTA. Un cordon de ligne téléphonique conforme et un connecteur modulaire sont fournis avec ce produit. Il est conçu pour être branché à un connecteur modulaire qui devra lui aussi être aux normes. Voir les instructions d'installation pour plus de détails.

Le numéro de REN (Ringer Equivalence Number) est utilisé pour déterminer le nombre d'appareils pouvant être branchés sur une ligne téléphonique. Un trop grand nombre de REN sur une même ligne téléphonique peut avoir pour résultat que les appareils n'émettront pas de sonnerie lors d'un appel entrant. Dans la plupart des zones, la somme des REN ne devra pas dépasser cinq (5.0). Pour être certain du nombre d'appareils pouvant être branchés sur une même ligne téléphonique, tel que déterminé par le total des REN, contactez votre compagnie de téléphone. Pour les produits approuvés après le 23 juillet 2001, le REN pour ce produit est inclus dans l'identifiant de produit au format US :

FK1DL01AL71WD. Les chiffres représentés par le 0.1 sont le REN sans point décimal (ex., 03 est un REN de 0.3).

En cas d'endommagement du réseau téléphonique causé par la Passerelle, la compagnie de téléphone vous informera à l'avance du temps d'arrêt nécessaire pour que le problème soit résolu. Si une notification préalable n'est pas possible, la compagnie de téléphone en informera le client dès que possible. Aussi, vous serez informé de votre droit de porter plainte en vertu du FCC si vous pensez que cela est nécessaire.

La compagnie de téléphone peut effectuer des changements au niveau de ses installations, équipements, opérations ou procédures pouvant affecter le fonctionnement de l'équipement. Dans ce cas, la compagnie de téléphone vous en informera à l'avance pour que vous puissiez effectuer les modifications nécessaires pour maintenir un service continu.

En cas de problème avec cette passerelle, et pour toute information concernant une réparation ou la garantie, veuillez contacter :

Check Point

6330 Commerce Drive Suite 120, Irving, Texas 75063

Numéro de téléphone de nos bureaux 972-444-6612

En cas d'endommagement du réseau téléphonique causé par l'équipement, il se peut que la compagnie de téléphone vous demande de débrancher l'équipement jusqu'à ce que le problème soit résolu.

La connexion au service de ligne est assujettie aux tarifs en vigueur dans votre État. Veuillez contacter la Commission des services collectifs de proximité, la Commission des services publics et la Commission des sociétés de votre État pour plus d'information.

Si votre domicile est équipé d'une alarme spécifique branchée à la ligne téléphonique, assurez-vous que l'installation de cet équipement ne désactive pas votre équipement d'alarme. Si vous avez des questions concernant ce qui pourrait désactiver votre équipement d'alarme, veuillez contacter votre compagnie de téléphone ou un installateur agréé.

LORSQUE VOUS PROGRAMMEZ DES NUMÉROS D'URGENCE ET (OU) EFFECTUEZ DES TESTS D'APPEL À DES NUMÉROS D'URGENCE :

1. Restez en ligne et expliquez brièvement à l'opérateur la raison de votre appel.
2. Faites cela pendant les heures creuses, comme en fin de matinée et en début de soirée.

Déclaration de conformité du département Canadien :

Le présent émetteur radio [IC: 7849A-WLE1216V220, IC: 7849A-WLE1216V520] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Frequency Band	Antenna Type	Max. Gain	Impedance Ω
2414-2462 MHz	Dipole Antenna (RP-SMA)	2.22 dBi	50Ω
5180-5240MHz, 5745-5825MHz	Dipole Antenna (RP-SMA)	4.29 dBi	50Ω

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 29 cm de distance entre la source de rayonnement et votre corps.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage, et
2. L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Cet appareil et son antenne ne doivent pas être situés ou fonctionner en conjonction avec une autre antenne ou un autre émetteur, exception faites des radios intégrées qui ont été testées.

La fonction de sélection de l'indicatif du pays est désactivée pour les produits commercialisés aux États-Unis et au Canada.

POUR WLAN 5 GHz DISPOSITIF:

Avertissement:

1. Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
2. Le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5470-5725 MHz doit se conformer à la limite de p.i.r.e.;
3. Le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5850 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.
4. Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3), doivent être clairement indiqués. (Pour 5G B2 avec les périphériques DFS uniquement)
5. Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3, doivent être clairement indiqués.
6. De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Restrictions concernant le raccordement de matériel

Avis: Le présent matériel est conforme aux spécifications techniques d'ISED applicables au matériel terminal. Cette conformité est confirmée par le numéro d'enregistrement. Le sigle IC, placé devant le numéro d'enregistrement, signifie que l'enregistrement s'est effectué conformément à une déclaration de conformité et indique que les spécifications techniques d'ISED ont été respectées. Il n'implique pas qu'ISED a approuvé le matériel.

Avis: L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 01. L'IES assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Industry Canada Statement

Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 29 cm entre le radiateur et votre corps.

Detachable Antenna Usage

Le présent émetteur radio (IC: 2417C-EM7455 / Model: EM7455) a été approuvé par ISED pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Approved Antenna(s) List

Type	Gain	Brand	Manufacturer
Dipole	3.2dBi	-	-

Déclaration de conformité de classe A pour le Japon :

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Directive de l'Union européenne relative à la compatibilité électromagnétique

Ce produit est certifié conforme aux exigences de la directive du Conseil concernant le rapprochement des législations des États membres relatives à la directive sur la compatibilité électromagnétique (2014/30/EU).

Ce produit est conforme à la directive basse tension 2014/35/EU et satisfait aux exigences de la directive 2014/35/EU du Conseil relative aux équipements électriques conçus pour être utilisés dans une certaine plage de tensions, selon les modifications de la directive 93/68/CEE.

Mise au rebut du produit

Ce symbole apposé sur le produit ou son emballage signifie que le produit ne doit pas être mis au rebut avec les autres déchets ménagers. Il est de votre responsabilité de le porter à un centre de collecte désigné pour le recyclage des équipements électriques et électroniques. Le fait de séparer vos équipements lors de la mise au rebut, et de les recycler, contribue à préserver les ressources naturelles et s'assure qu'ils sont recyclés d'une façon qui protège la santé de l'homme et l'environnement. Pour obtenir plus d'informations sur les lieux où déposer vos équipements mis au rebut, veuillez contacter votre municipalité ou le service de gestion des déchets.

Support

For technical assistance, contact Check Point 24 hours a day, seven days a week at:

- +1 972-444-6600 (Americas)
- +972 3-611-5100 (International)

When you contact support, you must provide your MAC address.

For more technical information, go to: http://supportcenter.checkpoint.com

To learn more about the Check Point Internet Security Product Suite and other security solutions, go to: https://www.checkpoint.com