QUANTUM

05 February 2026

QUANTUM SPARK 2560 / 2570 SECURITY GATEWAY APPLIANCE

T91

Getting Started Guide

CHECK POINT™

Check Point Copyright Notice

© 2025 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 Quantum Spark 2560 / 2570 Security Gateway Appliance Getting Started Guide

For more about this release, see the home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

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

Revision History

Date	Description
8 January 2026	Updated *"Health, Safety, and Compliance Information" on page 53*
04 January 2026	Updated: ▪ *"3G/4G/LTE/5G" on page 13* ▪ *"Appliance Diagrams and Specifications" on page 14*
25 November 2025	Updated *"Health, Safety, and Compliance Information" on page 53*
16 October 2025	Updated *"Health, Safety, and Compliance Information" on page 53*
14 August 2025	Reformatted Network LED tables in *"Front Panel" on page 17*
17 July 2025	First release of this document

Table of Contents

Introduction to the 2560 / 2570 Getting Started Guide ... *7*

Shipping Carton Contents ... *8*

Mounting the Appliance ... *9*

Wall Mounting ... *9*

Connecting the Cables ... *11*

First Time Deployment Options ... *12*

3G/4G/LTE/5G ... *13*

Appliance Diagrams and Specifications ... *14*

Front Panel ... *17*

Management LED ... *21*

Network LEDs ... *22*

Back Panel ... *23*

Side Panels ... *27*

Using the First Time Configuration Wizard ... *31*

Starting the First Time Configuration Wizard ... *32*

Welcome ... *33*

Zero Touch ... *33*

Authentication Details ... *35*

Appliance Date and Time Settings ... *36*

Appliance Name ... *37*

Security Policy Management ... *38*

Security Management Server Connection ... *39*

Security Management Server Authentication ... *40*

Internet Connection ... *41*

Local Network ... *43*

Wireless Network ... *44*

Administrator Access ... *45*

Appliance Registration 46
Software Blade Activation 48
Summary 49
Zero Touch Cloud Service 50
USB Drive or SD Card 52
Health, Safety, and Compliance Information 53
Informations relatives à la santé, à la sécurité, et à la conformité 69
Support 88

Introduction to the 2560 / 2570 Getting Started Guide

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 configuration instructions, see the relevant Administration Guides.

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

Shipping Carton Contents

Item	Quantity	Description
Appliance	1	2560 / 2570 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, black color. ▪ 40W for wired. ▪ 60W for WiFi, WiFi-LTE, WiFi-DSL.
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 2 2	Includes drilling hole location sticker. Screws: M4x6, truss screw. Screw anchors.
Antenna	4xWiFi / 4xWiFi + 4xCellular	**For WiFi Flavor**: ▪ 4 x WiFiAntenna, RP-SMA connector, black color. **For Cellular Flavor:** ▪ 4 x WiFiAntenna, RP-SMA connector, black color. ▪ 4 x Cellular Antenna, RP-SMA connector, black color.
Welcome Page	1	Welcome to Check Point QR Page

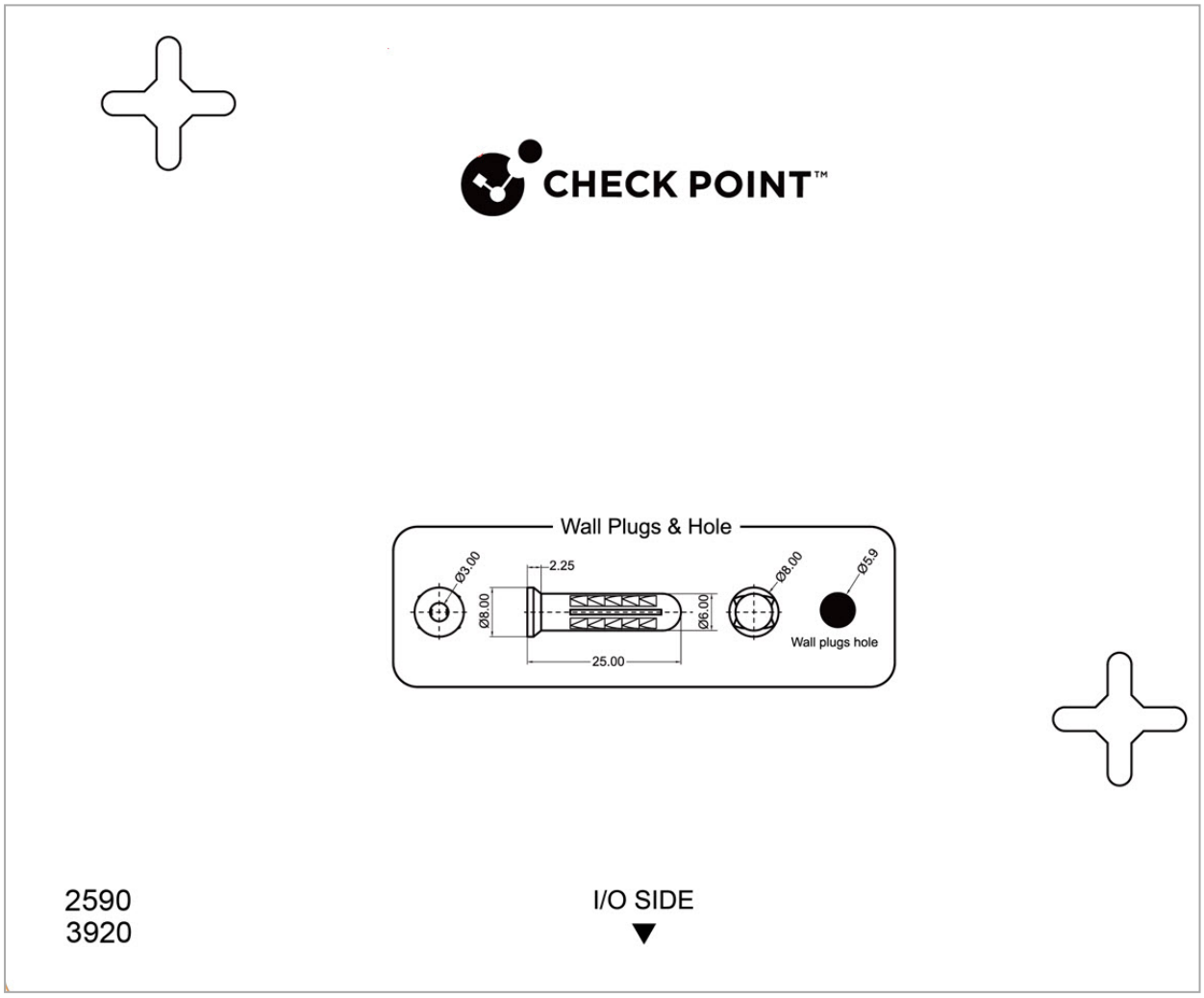
Mounting the Appliance

1. Remove the Quantum Spark 2560 / 2570 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 model only).
4. Identify the network interface marked as LAN1. This interface is preconfigured with the IP address **192.168.1.1**.

Wall Mounting

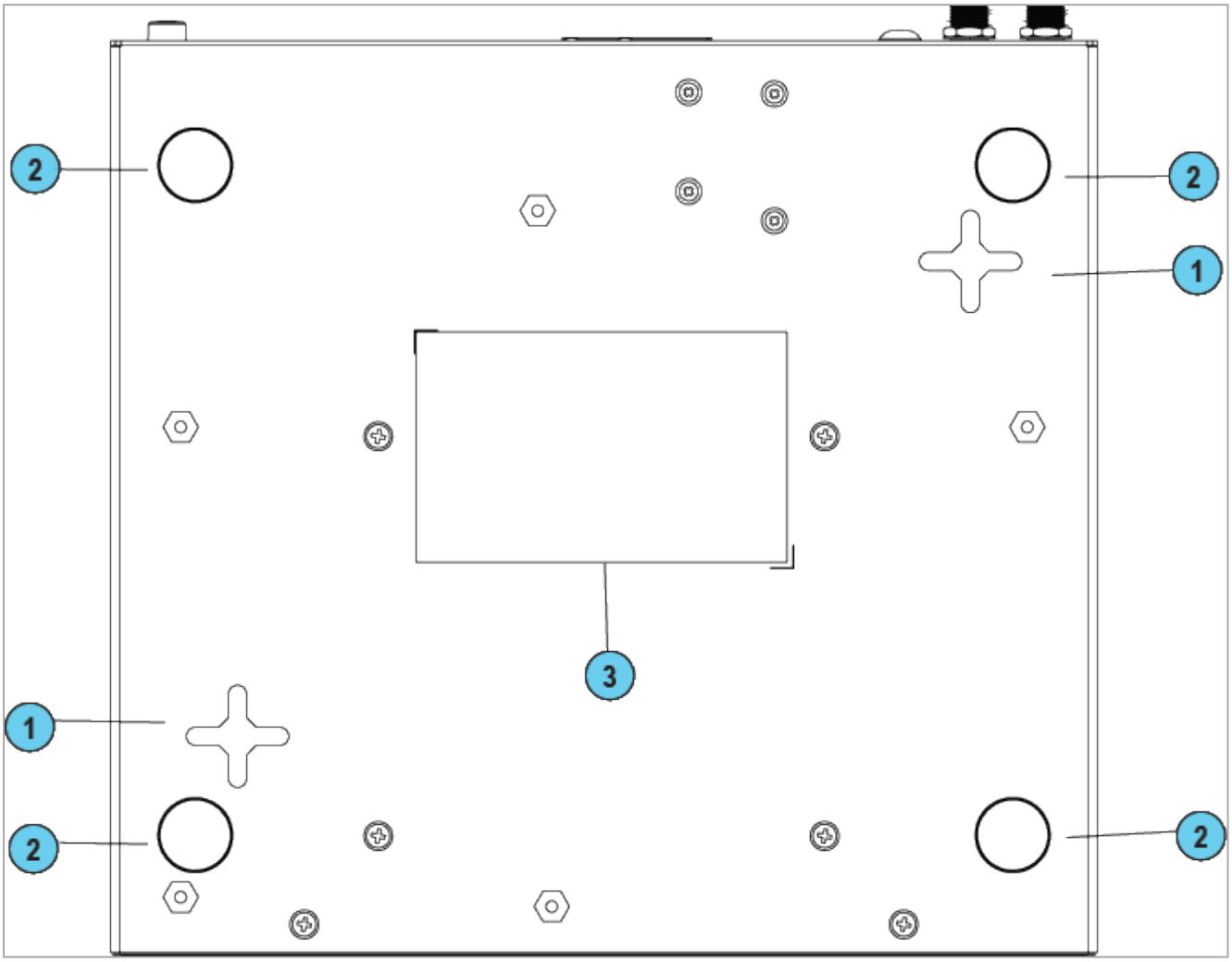
To mount the appliance to the wall:

1. Place the wall-mount sticker on the wall and drill two holes for the screws.



2. Insert the 2 screw anchors in the wall.
3. Attach the 2 screws in the accessory kit (M4*6) to the wall.
4. Mount the appliance and verify the 2 screws are fastened well to the appliance.

Bottom of the Appliance



Key	Item	Description
1	Holes on the bottom of the appliance	Attach screws here
2	Rubber Feet	Attached to the bottom of the appliance
3	Label	Location for the device label.

Connecting the Cables

1. Connect the appliance to the power supply and click the power button.
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 appliance front panel and to the network adapter on your PC.
4. **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 Internet LED on the appliance front panel lights up when the Ethernet is connected.

5. **Note** - Wait 10 seconds between power cycles (off and on).

First Time Deployment Options

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

- *"Using the First Time Configuration Wizard" on page 31*
- *"Zero Touch Cloud Service" on page 50*
- *"USB Drive or SD Card" on page 52*

3G/4G/LTE/5G

The 2570 Cellular model supports these features:

- Embedded modem that supports the latest advanced 5G NR Sub-6 GHz connectivity, with fallback to LTE/4G and 3G networks.
- Worldwide 5G coverage with a single product.
- Dual SIM functionality is supported to enable automatic failover between SIMs.
- 5G supports Sub-6 GHz, while 4G supports Cat-20 and 3G supports DC-HSPA+ and WCDMA (no 2G support).
- Peak download rate is 4.9Gbps and uplink of 660Mbps
- Four external antennas (RP-SMA type, Main, MIMO1, MIMO2, and AUX) to allow the best RF signal and coverage.

For more information on LTE, see sk180545.

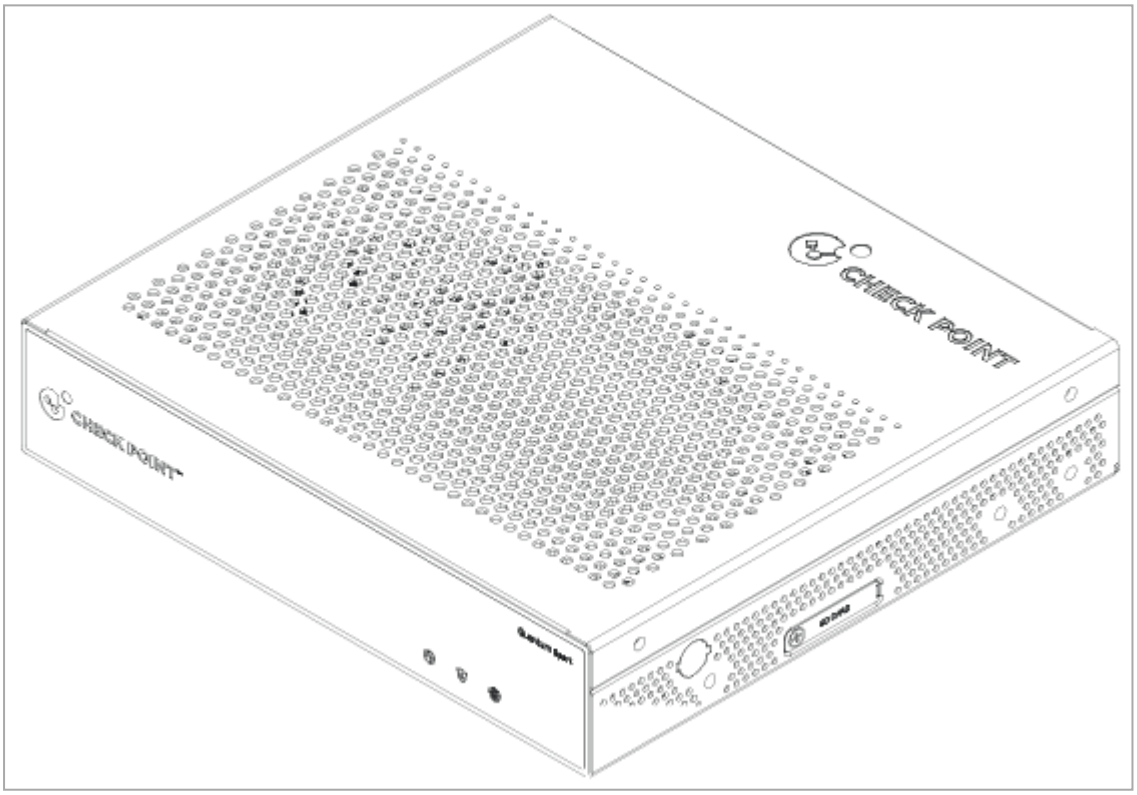
Appliance Diagrams and Specifications

This section describes the different features in the front, back, and side panels of these 2560 / 2570 Appliance models:

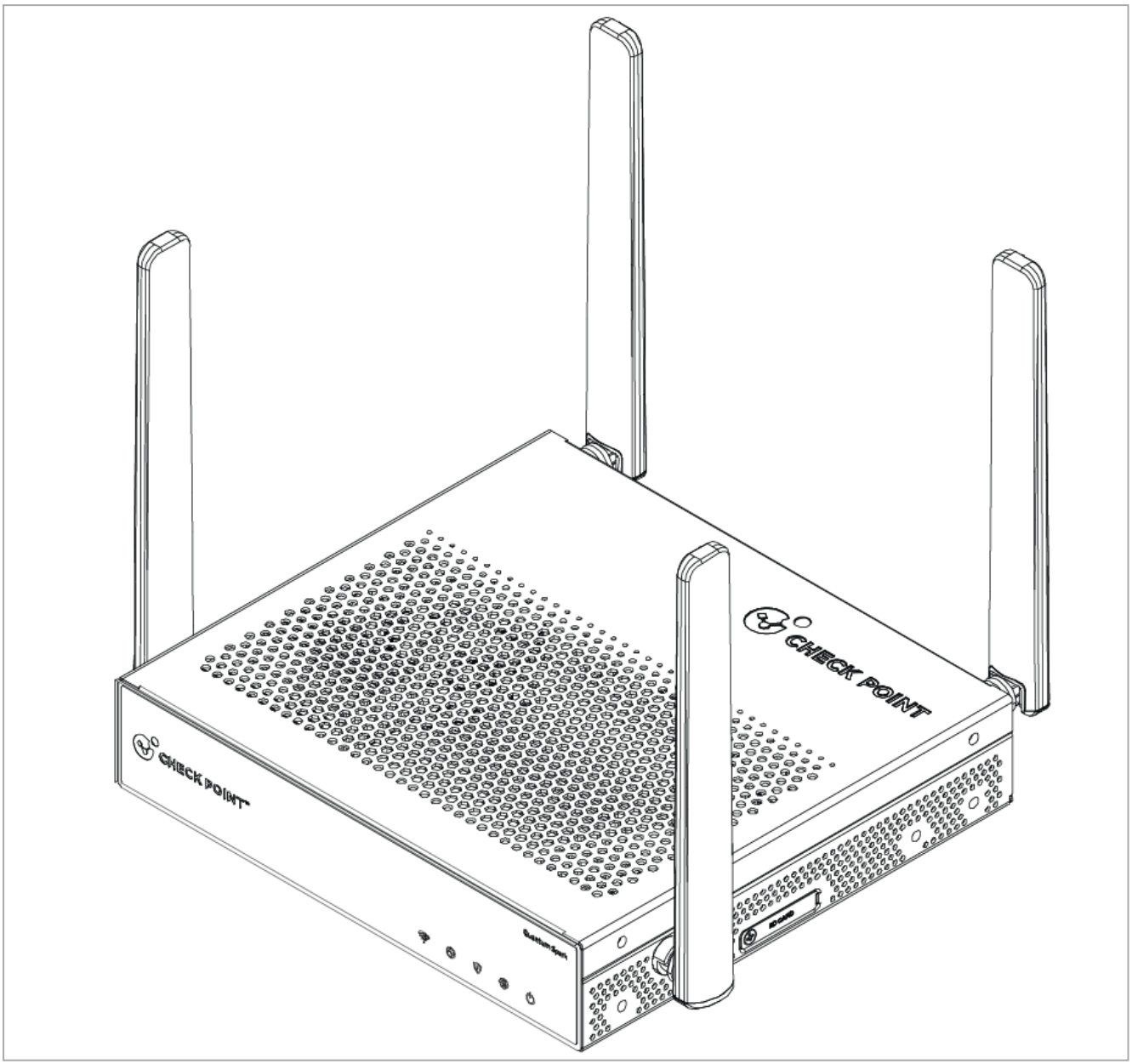
- Wired
- WiFi
- WiFi + Cellular (2570 model only)

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

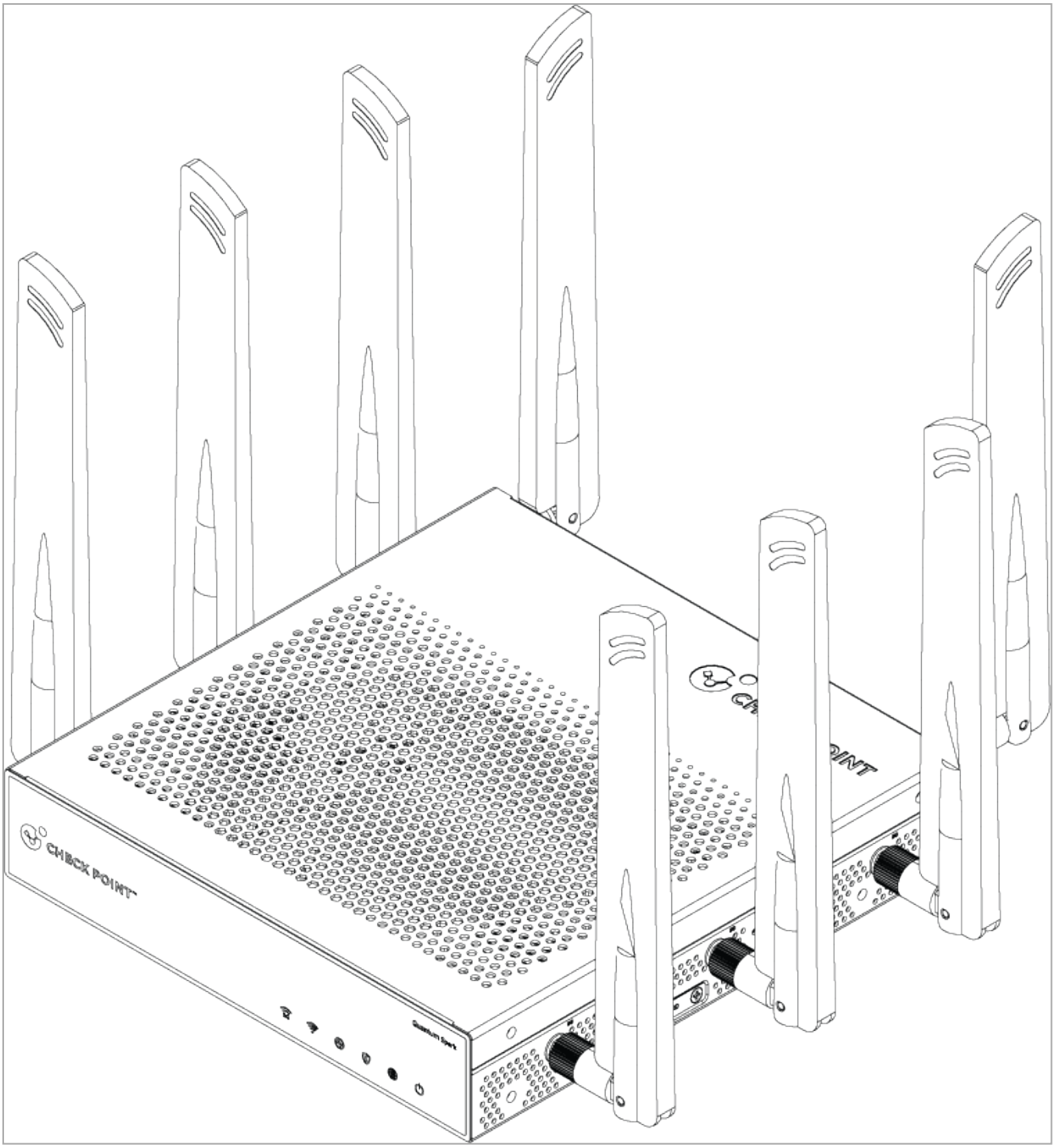
Wired



WiFi



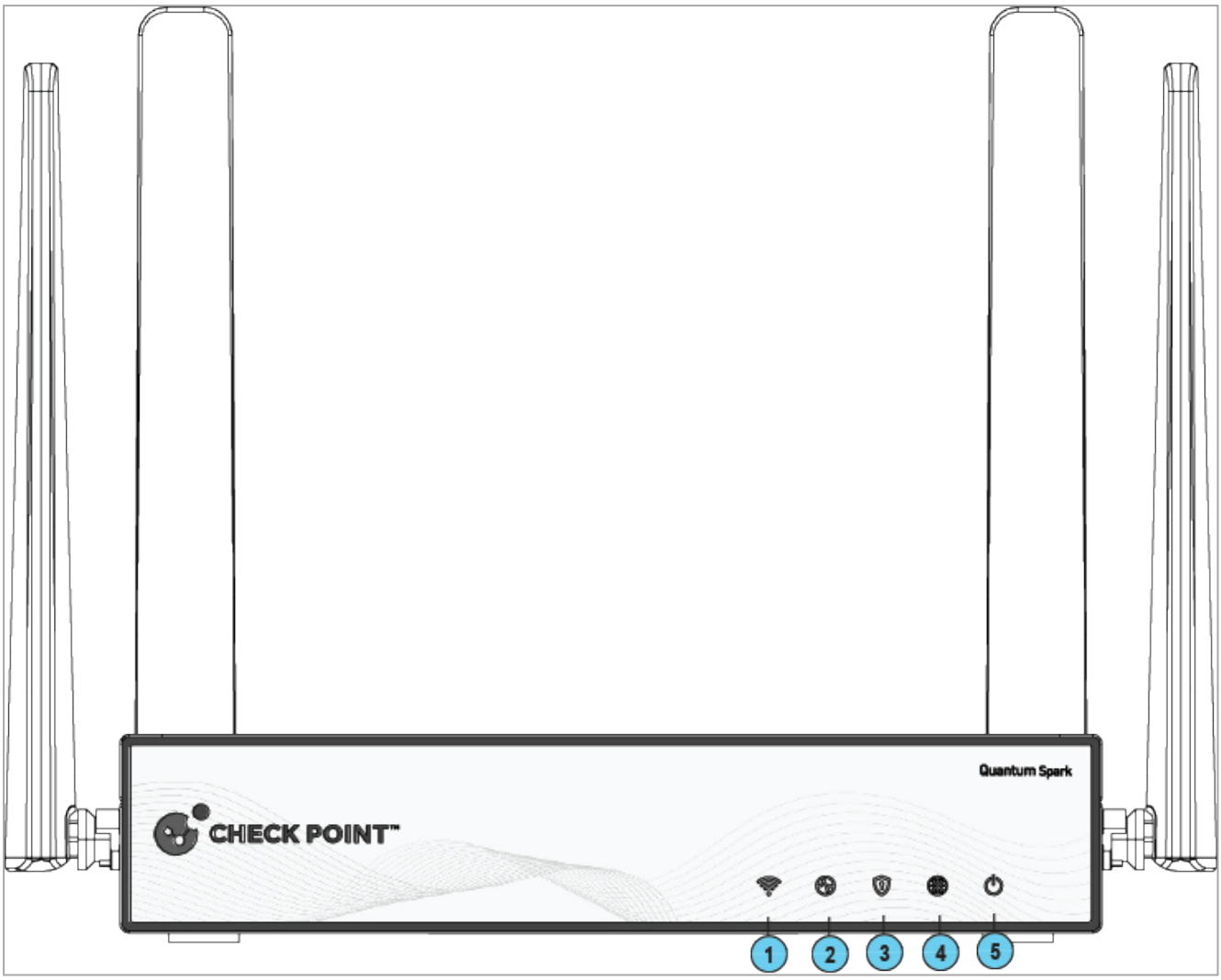
WiFi + Cellular


CHECK POINT
Quantum Spark

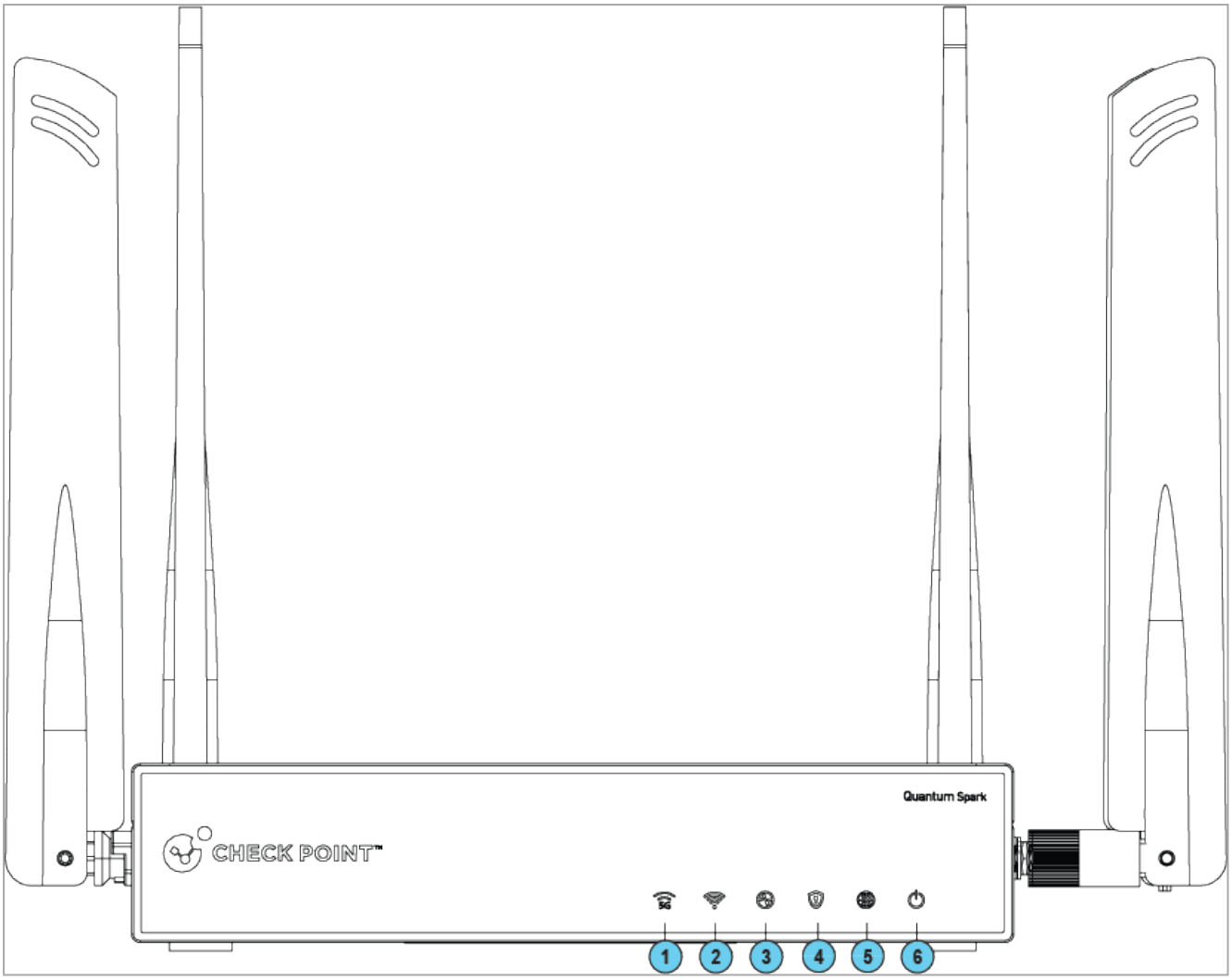
Front Panel

Wired

WiFi



WiFi + Cellular



Note - There is only one set of LEDs. The LED color (blue / red / purple) depends on what activity occurs.

Table: Wired LEDs

Key	Item	Icon	Description
1	WiFi LED (WiFi models only)		▪ **Off** - WiFi off ▪ **Blue** - WiFi on and operates normally ▪ **Red** - WiFi error/alert
2	Power Redundancy LED		Shows the status of the two internal PSUs. Single red LED. ▪ The two Power Supplies are active - Off ▪ Failure in one of the Power Supplies - On
3	Management LED		▪ **Off** - No management ▪ Colors - See below

Table: Wired LEDs (continued)

Key	Item	Icon	Description
4	Internet LED		▪ **Off** - No internet connection ▪ **Blinking Blue** - Connecting to the Internet. ▪ **Blue** - Connected ▪ **Blinking Red** - Connection failure
5	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.
5	LTE LED (WiFi LTE model only)		▪ **Off** - Cellular off ▪ **Solid blue** - Cellular modem available (operating SIM must be inserted and activated) ▪ **Blinking blue** - Cellular data transfer ▪ **Red** - Cellular modem issue (no SIM, modem off, no signal, etc.)
6	5G LED (2570 WiFi Cellular model only)		▪ **Off** - Cellular is off ▪ **Slowly Blinking Blue** - Connecting to the cellular network ▪ **Solid Blue** - Cellular internet connection is up and running on the 5G network ▪ **Rapidly Blinking Blue** - Traffic on the 5G network ▪ **Solid Purple** - Cellular internet connection is up and running on the 3G/4G/LTE network ▪ **Rapidly Blinking Purple** - Traffic on the 3G/4G/5G network ▪ **Red** - Cellular modem issue (no SIM, SIM error, SIM tray open etc.)

Management LED

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

Network LEDs

The table below describes the network LEDs (RJ45 WAN and LAN ports and the SFP).

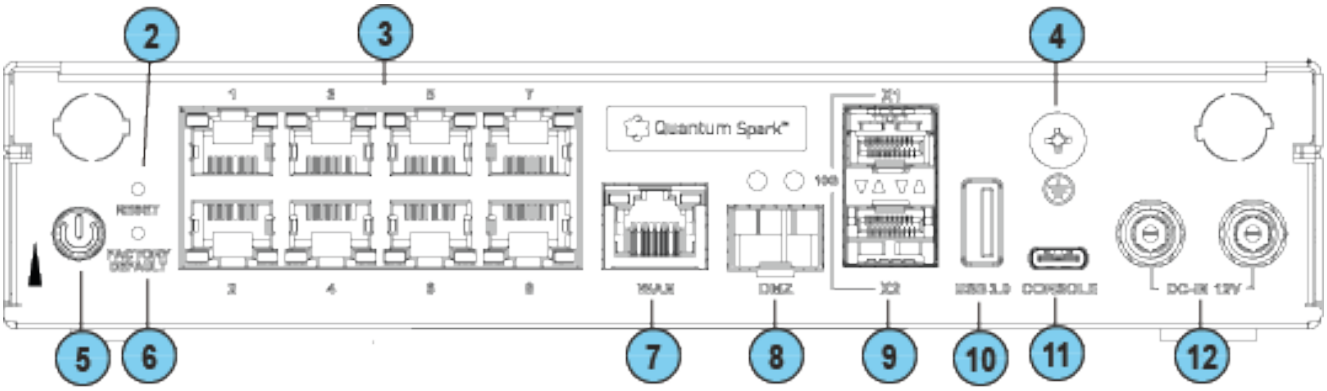
Each port uses a bi-color LED to reflect the link/activity and speed, from 10M to 1GbE.

Speed	Link	Activity	Link/Act LED1 Left	Speed LED2 Right
No link			No LED	No LED
1G	Yes	No	Solid Green	Solid Amber
1G	Yes	Yes	Blinking Green	Solid Amber
100M	Yes	No	Solid Green	No LED
100M	Yes	Yes	Blinking Green	No LED
10M	Yes	No	Solid Green	No LED
10M	Yes	Yes	Blinking Green	No LED

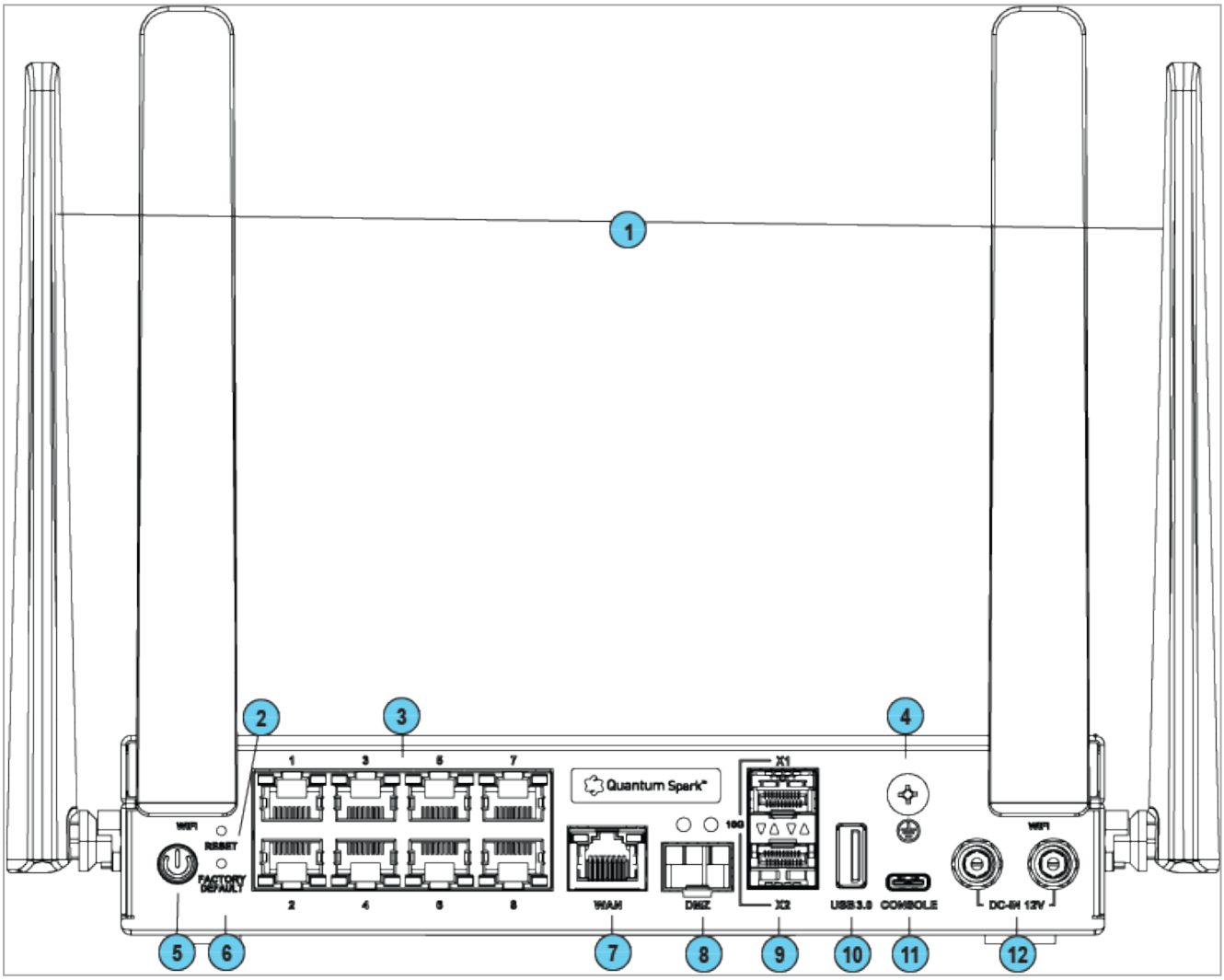
Speed	Link	Activity	Link/Act LED1 Left	Speed LED2 Right
No link			No LED	No LED
10G	Yes	No	Solid Green	Solid Amber
10G	Yes	Yes	Solid Green	Solid Amber
1G	Yes	No	Solid Green	Solid Green
1G	Yes	Yes	Solid Green	Solid Green

Back Panel

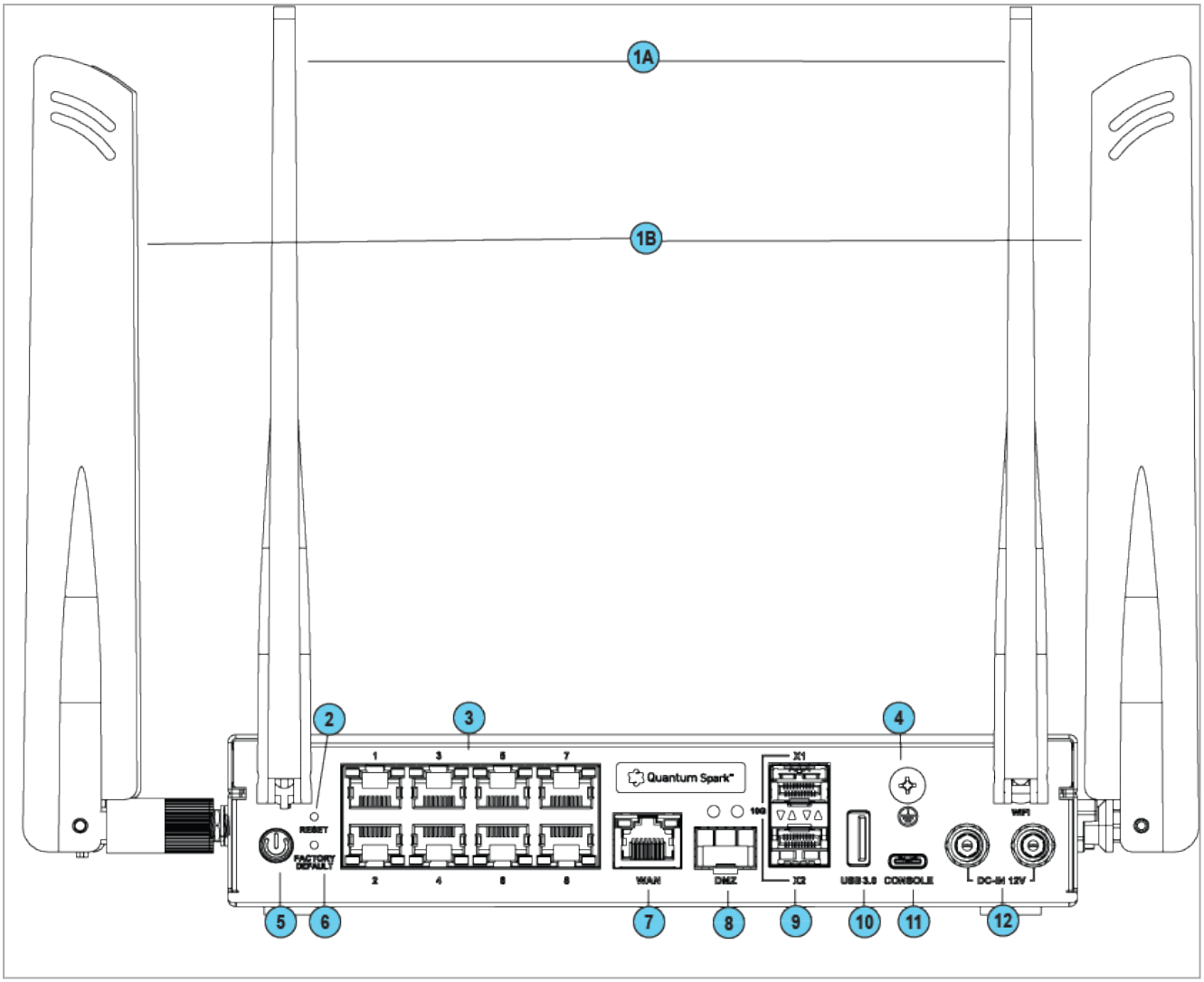
Wired



WiFi



WiFi + Cellular



Wired and WiFitable

Key	Item	Description
1	Antennas	WiFi models only
2	Reset	Short press resets the system but does not remove any user parameters.
3	LAN ports RJ45 1GBE	LAN ports 1-8.
4	Ground screw	Functional grounding.
5	Power button	Push to turn the appliance on or off

Key	Item	Description
6	Factory default	Press the button continuously for 12 seconds to restore the appliance to its factory default. All user parameters previously configured are removed.
7	WAN port	
8	DMZ port	
9	SFP Cage 10GbE	X1-X2 ports 2
10	USB port 3.0 (Type-A)	USB port 3.0 for software download.
11	Console	Plug in the serial console cable here. Baud rate: 115200.
12	12-60V, -48VDC input	Connects to the power source cable from your power infrastructure

WiFi + Cellular table

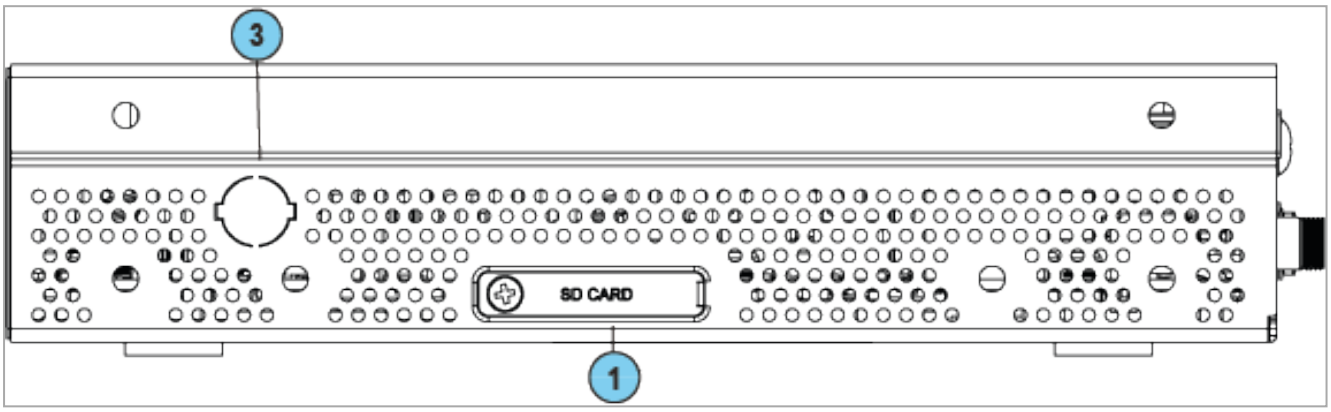
Key	Item	Description
1	Antennas	▪ 1A - WiFi antennas ▪ 1B - WiFi + Cellular antennas
2	Reset	Short press resets the system but does not remove any user parameters.
3	LAN ports RJ45 1GBE	LAN ports 1-8.
4	Ground screw	Functional grounding.
5	Power button	Push to turn the appliance on or off
6	Factory default	Press the button continuously for 12 seconds to restore the appliance to its factory default. All user parameters previously configured are removed.
7	WAN port	
8	DMZ port	
9	SFP Cage 10GbE	X1-X2 ports 2

Key	Item	Description
10	USB port 3.0 (Type-A)	USB port 3.0 for software download.
11	Console	Plug in the serial console cable here. Baud rate: 115200.
12	12-60V, -48VDC input	Connects to the power source cable from your power infrastructure

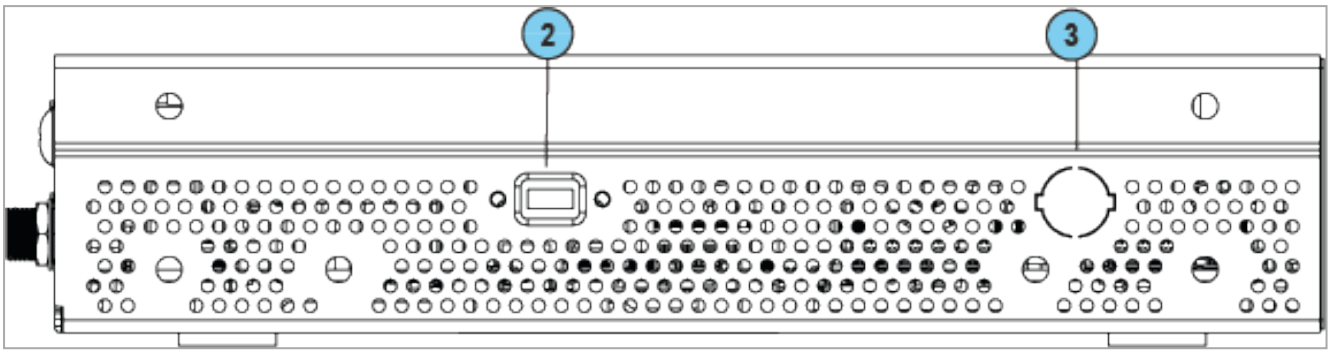
Side Panels

Wired, WiFi:

Side 1

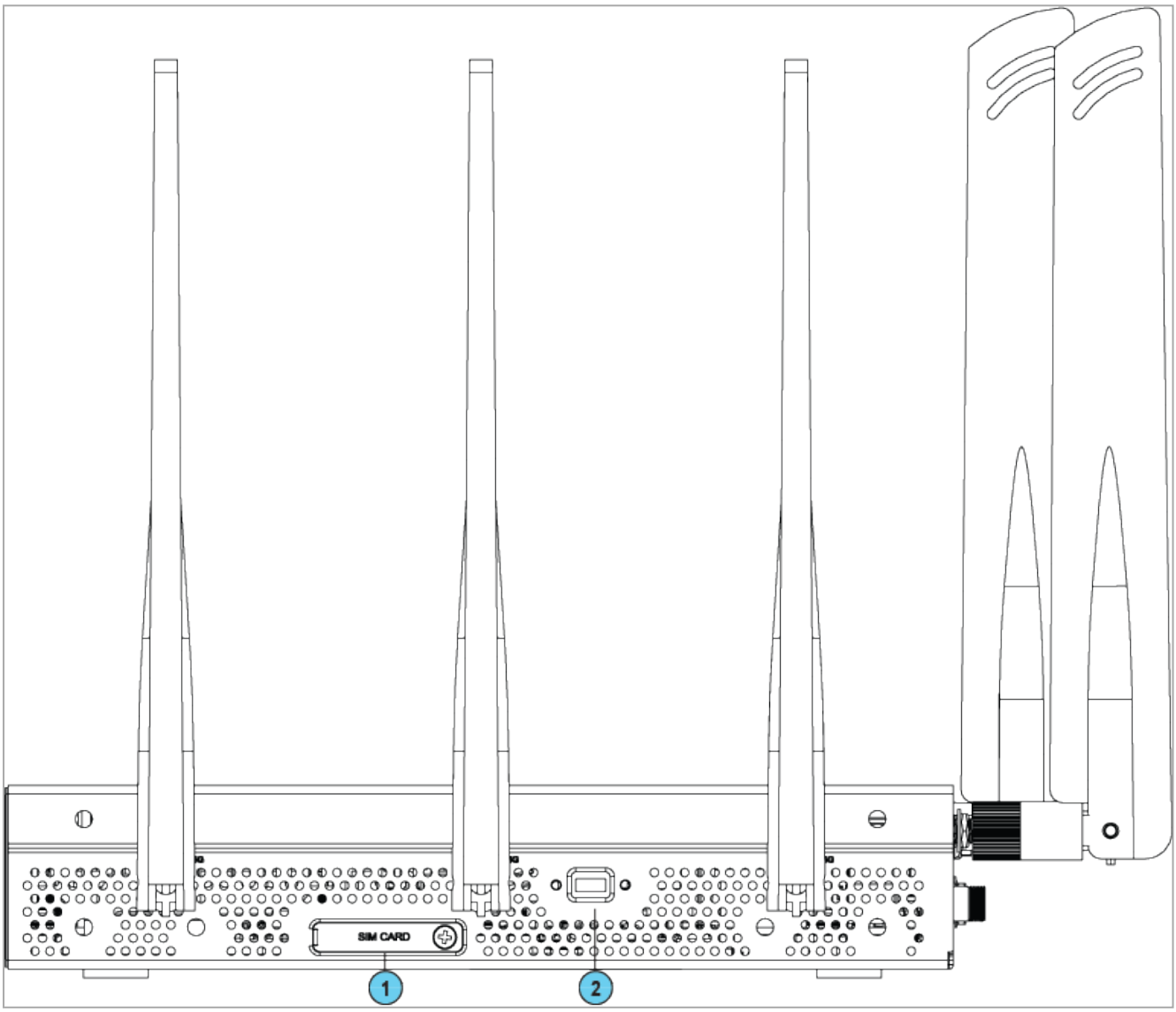


Side 2

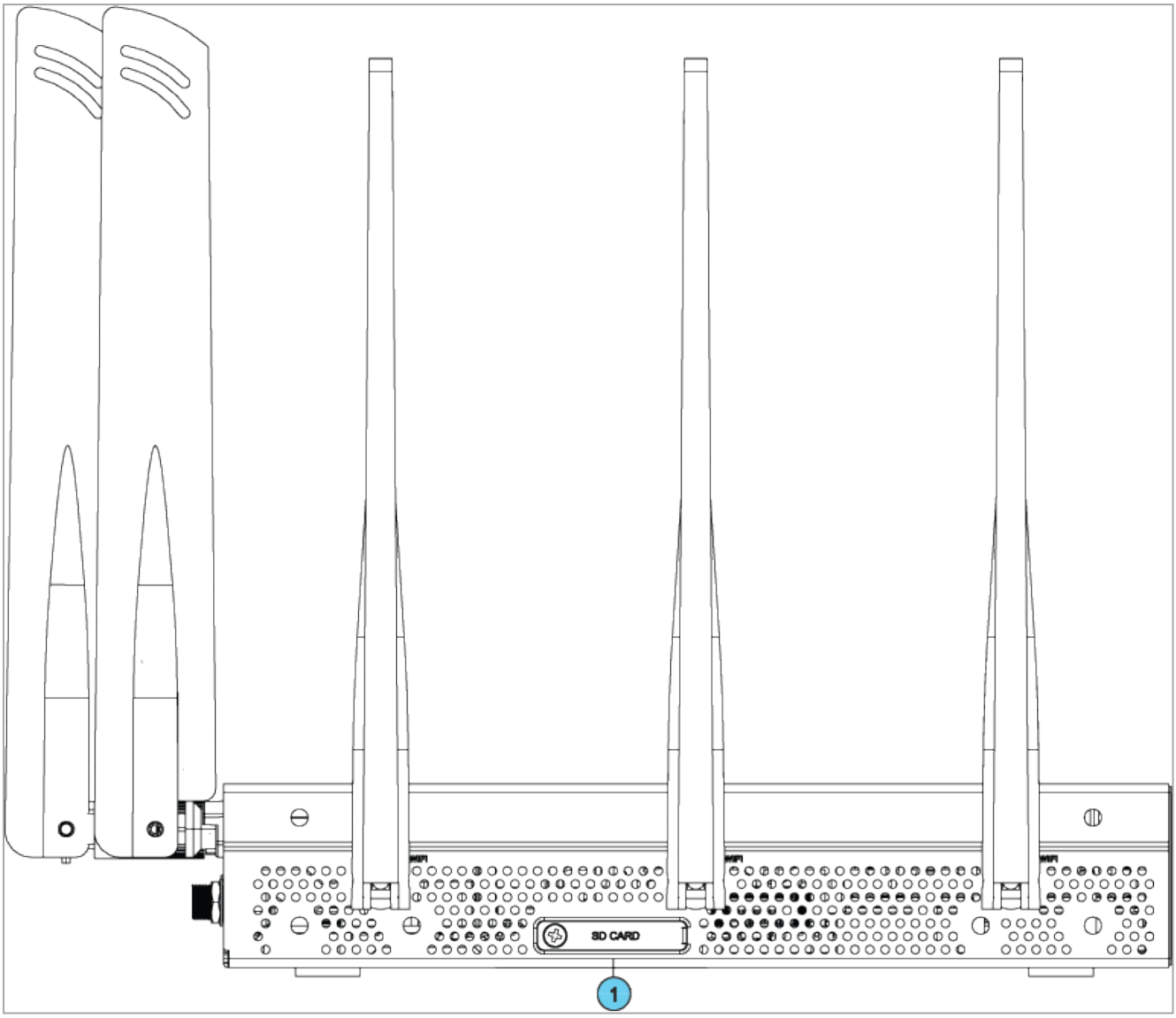


WiFi + Cellular

Side 1



Side 2



Wired and WiFi table

Key	Item	Description
1	SD slot	Insert micro-SD card here.
2	Anti-theft slot	Insert anti-theft cable here. Use Kensington and Sunbox TL-623M cable as a reference.
3	Antenna attachment	WiFi model only

WiFi + Cellular table

Key	Item	Description
1	SIM card slot	Insert SIM card here.
2	Anti-theft slot	Insert anti-theft cable here. Use Kensington and Sunbox TL-623M cable as a reference.
3	SD slot	Insert micro-SD card here.

SD Card Notes:

- Micro-SD card supports the format `ext4`, up to 256GB size.
- Insert or remove SD card only when the appliance is powered down.
- While inserting the micro-SD card, make sure the golden pins are facing upward:

Dual SIM Card Notes:

- Activation is done manually in Gaia Portal or Gaia Clish. The user selects the preferred SIM.
- The modem supports automatic failover between SIM cards.

Using the First Time Configuration Wizard

Configure the Quantum Spark 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 Appliance for the first time after you complete the hardware setup, use the First Time Configuration Wizard.

WiFi models with a special device label only:

If you did not yet run the First Time Configuration Wizard, you can connect through WiFi using the SSID and WiFi password that appears on the sticker. This is unique for each appliance.

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 Appliance WebUI, enter one of these addresses in a web browser:

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

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

The **First Time Configuration Wizard** starts.

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 appliance WebUI, 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 8 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 checkbox.

- **Confirm Password** - Enter the password again.

  Optional - Select to **Enforce the password history mechanism**.

- Enter the Administrator **Email**. Used to receive Notifications and for Two-Factor Authentication.
- Enter the Administrator **Phone number**. Used to receive Notifications and for Two-Factor Authentication.
- **Country** - Select a country from the list **(for wireless network models only)**.

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

  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.

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.

If you select the option **Set the time manually**, the appliance uses the date and time from your computer as the initial 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 date on your computer appears by default. If required, set a different date.
- **Time** - The time on your computer appears by default. If required, set a different time.
- **Time Zone** - The time zone on your computer 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 SmartConsole 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 appliance 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.

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 one of these:

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

  When you provide a host name, it will be saved, and the Security Gateway will automatically update the resolved IP address if any changes occur. You can edit this configuration 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.

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.

Internet Connection

On 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.
   - **Cellular** - This is only for appliances with an internal LTE modem. Both SIM cards are used for the internet connection with a failover between them.
   - **Cellular Modem** - This does not apply to Wired models. Connect to the Internet with a cellular modem to the ISP through a 3G or 4G network. For this option, select the USB/Serial option in the Interface name.

     Note - Only one cellular modem is supported. Appliances with an internal LTE modem do not support an external USB modem. Only customers with an approved RFE will be supported with the external modem specified in the RFE.
   - **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, Cellular, and 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.

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. The **Hide** password option is selected by default.
6. **Allow access from this network to the local network** is selected by default. This means the wireless network is considered trusted and access is allowed from it to the local network.
7. Radio Band - Varies according to model.
   - 2.4GHz: 2414-2462 MHz
   - 5GHz: 5180-5240, 5260-5320, 5500-5720, 5745- 5825MHz

   Or:
   - 2.4GHz: 2.412~2.472GHz
   - 5GHz: 5.150~5.850GHz / 4.920~5.850GHz

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**.

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 Software Blade.

If you are working offline while configuring the appliance:

1. From a computer with authorized access to the *Check Point User Center*, follow *one* of these procedures:

   Note - If you do not have a User Center account, select **Create a new User Center account**.

   - **Use your User Center account**

     a. Log in to your User Center account.

     b. Select the specified container of your appliance.

     c. From the **Product Information** tab, click **License** > **Activate**.

     This message appears: "*Licenses were generated successfully*".

     d. Click **Get Activation File** and save the file locally.

   - **Register your appliance**

     a. Go to: https://smbregistration.checkpoint.com

     b. Enter your appliance details and click **Activate**.

     This message appears: "*Licenses were generated successfully*".

     c. 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 in the WebUI from the **Device** > **License** page.

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

To create a new User Center account (for Locally Managed appliances 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.

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 *Check Point 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.

For more information on how to use Zero Touch, see sk116375.

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 the 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 appliance 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.

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 17* section.

USB Drive or SD Card

The configuration file lets you configure more settings and parameters than are available in the First Time Configuration Wizard

You can deploy configuration files only on these appliances:

- You did not run the First Time Configuration Wizard yet.
- You restored an appliance to factory defaults.

To use rapid deployment files through a USB stick or an SD card:

1. On your computer, in plain-text editor, create a file named `autoconf.clish`.
2. In this file, write the applicable Gaia Clish commands, with each command in a separate line.

   Refer to the *R82.00.X Quantum Spark Appliances CLI Reference Guide* .
3. Save this file in the UNIX format.
4. Format the USB drive or SD card in FAT32.
5. Copy this file to the USB drive.
6. Power off the Quantum Spark appliance.
7. Insert the USB stick into the USB 3.0 port in the Quantum Spark appliance.
8. Optional: To see more information, you can connect to the console port on the Quantum Spark appliance.
9. Power on the Quantum Spark appliance.
10. The appliance:
    a. Starts.
    b. Automatically mounts the USB drive.
    c. Searches the root directory for this configuration file.
    d. Executes the Gaia Clish commands from this configuration file.
11. Wait for the applicable LEDs to light up on the front panel.

    See *"Front Panel" on page 17*.
12. Power off the Quantum Spark appliance.
13. Remove the USB drive from the Quantum Spark appliance.
14. Power on the Quantum Spark appliance.

Health, Safety, and Compliance 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.

Grounding Procedure

Warning - The equipment has a separate protective grounding terminal on the chassis that must be permanently connected to the earth ground to adequately ground the chassis and protect the operator from electrical hazards.

Caution - Before starting the equipment installation, ensure that a service technician has securely attached the grounding lug to the provided grounding cable.

To connect the ground to the equipment:

1. Connect one end of the grounding cable to a proper earth ground.
2. Place the ground lug attached to the ground cable over the protective grounding terminal.
3. Secure the grounding lug to the protective grounding terminal with washers and screws
4. Arrange the grounding cable neatly and ensure that it does not touch or block access to other components.

Warning - Before powering on the equipment, connect the frame of the equipment to the ground. For the grounding wire, green and yellow insulation is required and the cross-sectional area of the conductor must be more than 0.75mm2 or 18 AWG.

Warning - The protective grounding terminal with washers and screws where a screw is threaded into it should not be less than twice the pitch of the screw thread, at least 3.5mm diameter; Star washers or Spring washers can be used.

Warning - After you power off and are disconnected from the equipment, disconnect the frame of the equipment to the ground.

Power Supply Information

This product is intended to be supplied by a UL listed (Certificate) power supply, output rated 12Vdc, 5.0A minimum, Tma 40 degree C minimum. The altitude of operation of the power supply should comply with the altitude of the installation area. If you need further assistance, contact manufacture or brand owner further 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. CAUTION: RISK OF EXPLOSION IF THE BATTERY IS REPLACED BY AN INCORRECT TYPE. 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.

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 operate the processor without a thermal solution. Damage to the processor can occur in seconds.
- 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.
- 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.
- Ground cable must be 18AWG minimum (color green-yellow).
- Never open the equipment. For safety reasons, the equipment should be opened only by a qualified skilled person authorized by Check Point.
- Devices with optical option: Use only Laser Class 1 CDRH certified optical transceiver.

Fiber module warning message:

Laser Class 1 optical transceiver shall be used only.

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.

Declaration of Conformity

Manufacturer's Name:	Check Point Software Technologies Ltd.
Manufacturer's Address:	5 Shlomo Kaplan Street, Tel Aviv 67897, Israel
Regulated Model Number:	T91, T91W, T91WC
Marketing Model	SG2560 SG2570
Product Options:	2560 / 2570 Wired, WiFi , WiFi + Cellular
Date and Place of Issue	April 2025, Tel Aviv, Israel

Model	WiFi	Cellular
T91	Not supported	Not supported

Model	WiFi	Cellular
T91W	Supported	Not supported
T91WC	Supported	Supported

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

Certification	Type
EN 55032 : 2015+A11:2020 BS EN 55032: 2015+A11:2020 EN IEC 61000-3-2 : 2019+A1:2021 BS EN IEC 61000-3-2 : 2019+A1:2021 EN 61000-3-3 : 2013+A1:2019+A2:2021+AC:2022-01 BS EN 61000-3-3 : 2013+A1:2019+A2:2021 EN 55035 : 2017+A11:2020 BS EN 55035: 2017+A11:2020 IEC 61000-4-2 : 2008 IEC 61000-4-3 : 2020 IEC 61000-4-4 : 2012 IEC 61000-4-5 : 2014+A1:2017 IEC 61000-4-6 : 2023 IEC 61000-4-8 : 2009 IEC 61000-4-11 : 2020+COR1:2020 EN 301 489-1 V2.2.3:2019-11 EN 301 489-17 V3.3.1:2024-09 EN 300 328 V2.2.2:2019 EN 301 893 V2.2.1:2017 EN 300 440 V2.2.1:2017 EN 303 687 V1.1.1 EN 62311:2008 EN IEC 62311:2020 EN 50665:2017 AS/NZS CISPR 32 : 2015+A1:2020 AS/NZS 4268:2017 AS/NZS 4268:2017 Amd 1:2021 AS/NZS 2772.2:2016 ARPANSA RPS S-1(Rev.1):2021 47 CFR FCC Part 15 Subpart B ICES-003 Issue 7 : October 2020 ANSI C63.4 : 2014 SS-Gen Issue 5; April 2018 (Canada) FCC Part 15C (2.4 GHz) FCC Part 15E (5 GHz, 6 GHz) RSS-247 Issue 3; Aug. 2023 (Canada) RSS-248 Issue 3; Oct. 2024 (Canada) FCC KDB 996369	EMI (Electromagnetic Interference) and EMC (Electromagnetic Compatibility) RF Radio/Wi-Fi/RF exposure

Certification	Type
Mobile RF exposure requirements (FCC) RSS-102 Issue 6; December 2023 (Canada) VCCI-CISPR 32 : 2017	
CE LVD EN62368-1 CB IEC /EN62368-1 2nd and 3rd edition. AS/NZS 62368.1:2022 CSA C22.2 No. 62368-1:2019 GB 4943.1-2022 EN IEC 62368-1:2020+A11:2020, BS EN IEC 62368-1:2020+A11:2020 J62368-1 (2023) National standard SASO-IEC 62368-1:2020 UL 62368-1:2019 KC 62368-1 (2021-08) UL62368-1	Electrical Safety

Testing lab

Name	Address
Prodigy Technology Consultant Co., Ltd.	No. 12, Gong 7th Rd., Linkou District, New Taipei City 24450, Taiwan Chinese Taipei
SGS Taiwan Ltd.	Electromagnetic Compatibility LaboratoryNo.2, Keji 1st Rd., Guishan District, Taoyuan City, Taiwan

Physical and environmental reliability	Description
Operating Conditions	Vibrations and Shock Based on EN 300 019-2-3.
Storage Conditions	Temperature: (-40)°C ~ 60°C. Humidity: 95%, non-condensed. Vibrations and Shock based on EN 300 019-2-1.
Transportation Conditions	Temperature: (-40)°C ~ 85°C. Humidity: 95%, non-condensed. Vibrations and Shock based on EN 300 019-2-2.

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.

This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

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 35 centimeters between the radiator and your body.

Japan Class B Compliance Statement

この装置は、クラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

ＶＣＣＩ－Ｂ

European Union (EU) CE declaration of conformity: Electromagnetic Compatibility Directive, Low voltage Directive and Radio directive RED

We Check Point Software Technologies Ltd. hereby declares; that the following equipment (model T91, T91W, T91WC) are in compliance with:

- Model T91, T91W, T91WC: 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).
- Model T91, T91W, T91WC: 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."
- Model T91W, T91WC: confirmed to comply with the requirements Directive 2014/53/EU article 10.8 requirement.

According to the CE report of T91WC

Radio Type	Description	Frequency	Maximum EIRP (dBm)
WIFI	2.4GHz Band	2400-2483.5MHz	16.64
	5GHz Band	5150-5350MHz	19.52
		5470-5725MHz	26.24
		5725-5875MHz	10.34
	6GHz Band	5945-6425MHz	19.59

According to the Sierra EM9291 specifications

Radio Type	Description	Frequency	Maximum Output Power (dBm)
WCDMA	Band I	1920 - 1980 MHz	23.5
	Band VIII	880 - 915 MHz	23.5

Radio Type	Description	Frequency	Maximum Output Power (dBm)
LTE	B1	1920 - 1980 MHz	23
	B3	1710 - 1785 MHz	23
	B7	2500 - 2570 MHz	23
	B8	880 - 915 MHz	23
	B20	832 - 862 MHz	23
	B28	703 - 748 MHz	23
	B34	2010 - 2025 MHz	23
	B38	2570 - 2620 MHz	23
	B40	2300 - 2400 MHz	23
	B41_HPUE	2496 - 2690 MHz	25
	B42_HPUE	3400 - 3600 MHz	25
	B43_HPUE	3600 - 3800 MHz	25
5G NR	n1	1920 - 1980 MHz	24
	n3	1710 - 1785 MHz	24
	n7	2500 - 2570 MHz	24
	n8	880 - 915 MHz	24
	n20	832 - 862 MHz	24
	n28	703 - 748 MHz	24
	n38	2570 - 2620 MHz	24
	n40	2300 - 2400 MHz	24
	n41_PC2	2496 - 2690 MHz	26
	n77_PC2	3300 - 4200 MHz	26
	n78_PC2	3300 - 3800 MHz	26

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.

1. Devices shall not be used for control of or communications with unmanned aircraft systems.
2. Operation shall be limited to indoor use only.
3. Operation on oil platforms, automobiles, cars, trains, boat, maritime vessels and aircraft shall be prohibited except for operating in the 5925-6425 MHz on large aircraft flying above 3,048 m (10,000 ft). Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

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.

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.

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

Canadian Department Declaration of Conformity

This radio transmitter [IC: 7849A-WLE3000HX] 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.

Sample statement for antennas: Manufacturer: INPAQ, MPN: RFDPA171300SBLB801

Frequency Band	Antenna Type	Max Gain	Impedence Ω
2414-2462 MHz	Dipole Antenna (RP-SMA)	2.22 dBi	50Ω
5180-5240, 5260-5320, 5500-5720, 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 35 cm between the radiator & your body.

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.

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

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.

The County Code Selection feature is disabled for products marketed in the US/ 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. For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;
3. 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
4. For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate;
5. 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.
6. 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)
7. Where applicable, antenna type(s), antenna models(s), 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.
8. 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.

Industry Canada Statement

FOR MOBILE DEVICE USAGE (>35cm/low power)

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.

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 35 cm between the radiator & your body.

Detachable Antenna Usage

This radio transmitter (IC: 2417C-EM91) 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. **Note** - This paragraph is valid for V91WC models only.

This radio transmitter (IC: 2417C-EM75T) 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. **Note** - This paragraph is valid for V91WL models only.

Antenna Gain Table

Model	Part Name	IEI Part Number	Frequency Band	Max Gain	Impedence Ω	Antenna Type
T1.2 WiFi	WiFi antenna	CKP-32505-012500-100-HF	2412-2472 MHz	2.83 dBi	50Ω	Dipole Antenna (Undetachable)
			5945-7125MHz	4.53 dBi	50Ω	
			5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.98 dBi	50Ω	
	WiFi antenna	CKP-32505-012600-100-HF	2412-2472 MHz	2.83 dBi	50Ω	Dipole Antenna (Undetectable)
			5945-7125MHz	5.43 dBI	50Ω	
			5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.98 dBi	50Ω	
	WiFi antenna	CKP-32505-012700-100-HF	5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.49 dBi	50Ω	Dipole Antenna (Undetectable)
	WiFi antenna	CKP-32505-012800-100-HF	5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.49 dBi	50Ω	Dipole Antenna (Undetectable)

Model	Part Name	IEI Part Number	Frequency Band	Max Gain	Impedence Ω	Antenna Type
T1.2 WiFi + 5GNR	WiFi antenna	CKP-32505-012900-100-RS	2412-2472 MHz	1.27 dBi	50Ω	Dipole Antenna (Undetectable)
			5945-7125MHz	3.62 dBi	50Ω	
			5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.68 dBi	50Ω	
	WiFi antenna	CKP-32505-013000-100-RS	2412-2472 MHz	1.27 dBi	50Ω	Dipole Antenna (Undetectable)
			5945-7125MHz	3.62 dBi	50Ω	
			5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.68 dBI	50Ω	
	WiFi antenna	CKP-32505-013100-100-RS	5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.51 dBi	50Ω	Dipole Antenna (Undetectable)
	WiFi antenna	CKP-32505-013200-100-RS	5180-5240, 5260-5320, 5500-5720, 5745-5825MHz	3.51 dBi	50Ω	Dipole Antenna (Undetectable)
	5GNR antenna	CKP-32513-000800-100-RS	617-960MHz	1.98 dBI	50Ω	Dipole Antenna (RP-SMA)
			1710-2690MHz	3.95 dBi	50Ω	
			3300-5925MHz	3.24 dBi	50Ω	

Common security requirements for radio equipment

The European standard, EN 18031 series, deals with cybersecurity for radio equipment that is connected to the internet.

To comply with the standard which requires log persistence, the device shall not be used in a live production environment unless one of these options is true:

- Extended Monitoring is enabled
- Spark Management is configured
- An external Log Server is configured

Informations relatives à la santé, à la sécurité, et à la conformité

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

Avertissement : ne pas obturer les aérations. Un dégagement minimum de 1,3 cm est nécessaire.

Avertissement : cet appareil ne contient aucune pièce remplaçable par l'utilisateur. Ne retirez aucun couvercle et n'essayez pas d'accéder à l'intérieur du produit. 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.

Procédure de mise à la terre

Avertissement : L'appareil est équipé d'une borne de mise à la terre séparée sur le châssis et qui doit être en permanence connectée à la terre de manière adéquate afin de protéger l'opérateur contre les risques électriques.

Attention : Avant de commencer l'installation de l'équipement, assurez-vous qu'un technicien a bien fixé la cosse de mise à la terre au câble de mise à la terre fourni.

Pour effectuer la mise à la terre de l'équipement :

1. Connectez une extrémité du câble de mise à la terre à une prise de terre appropriée.
2. Placez la cosse de mise à la terre attachée au câble de mise à la terre sur la borne de mise à la terre.
3. Fixez la cosse de mise à la terre à la borne de mise à la terre à l'aide de rondelles et de vis.
4. Disposez soigneusement le câble de mise à la terre et veillez à ce qu'il ne touche pas ou ne bloque pas l'accès à d'autres composants.

Avertissement : Avant de mettre l'appareil sous tension, connectez le châssis de l'appareil à la terre. Pour le fil de mise à la terre, une isolation verte et jaune est requise, et la section du conducteur doit être supérieure à 0,75 mm2 ou 18 AWG.

Avertissement : La borne de mise à la terre avec les rondelles et les vis dans lesquelles une vis est vissée ne doit pas être inférieure à deux fois le pas du filetage de la vis, soit un diamètre d'au moins 3,5 mm ; des rondelles en étoile ou des rondelles à ressort peuvent être utilisées.

Avertissement : Après avoir mis l'appareil hors tension et l'avoir débranché, déconnectez la mise à la terre du châssis de l'appareil.

Information pour l'alimentation

Ce produit est destiné à être alimenté par un bloc d'alimentation homologué UL (certificat), avec une sortie de 12 Vdc, 5,0 A minimum, Tma 40 degrés C minimum. L'altitude de fonctionnement de l'alimentation électrique doit être conforme à l'altitude de la zone d'installation. Si vous avez besoin d'aide, contactez le fabricant ou le propriétaire de la marque pour plus d'informations.

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 en temps réel). Elle risque de s'échauffer et de causer des brûlures.

  Avertissement : DANGER D'EXPLOSION SI LA PILE EST MAL REPLACÉE. ATTENTION : RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UN TYPE DE BATTERIE INCORRECT. 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.

CONSIGNES **DE SÉCURITÉ** IMPORTANTES : Lors de l'utilisation de votre équipement téléphonique, des précautions de base doivent toujours être prises afin de réduire les risques d'incendie, d'électrocution et de blessures, notamment celles qui suivent.

- Ne pas faire fonctionner le processeur sans refroidissement. Le processeur peut être endommagé en quelques secondes.
- 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 d'un bac à linge, dans un sous-sol humide ou près d'une piscine.
- N'utiliser que le cordon d'alimentation et les piles indiqués dans ce manuel. Ne pas jeter les piles au feu. Elles risquent d'exploser. Vérifier les réglementations locales pour d'éventuelles instructions spéciales concernant la mise au rebut.
- Cet appareil ne doit pas être utilisé dans des lieux où des enfants sont susceptibles d'être présents.
- Assurez-vous de brancher le cordon d'alimentation sur une prise de courant avec mise à la terre.
- Le câble de mise à la terre (vert et jaune) doit être de 18 AWG minimum.
- Ne jamais ouvrir l'appareil. Pour des raisons de sécurité, l'équipement ne doit être ouvert que par une personne qualifiée et autorisée par Check Point.
- Appareils avec option optique : n'utilisez que des émetteurs-récepteurs optiques laser de classe 1 certifiés CDRH.

Message d'avertissement du module fibre :

Seul un émetteur-récepteur optique laser de classe 1 doit être utilisé.

Attention : Afin de réduire le risque d'incendie, n'utilisez que des cordons de ligne de télécommunication de calibre 26 AWG ou supérieur (par exemple, 24 AWG), répertoriés par l'UL ou certifiés par la CSA.

Déclaration de conformité

Nom du fabricant :	Check Point Software Technologies Ltd.
Adresse du fabricant :	5 Shlomo Kaplan Street, Tel Aviv 67897, Israël
Numéro de modèle régulé :	T91
Modèle de commercialisation	SG2560 SG2570
Options de produit :	2560 / 2570 filaire
Date et lieu d'émission	Avril 2025, Tel Aviv, Israël

Déclare, sous sa seule responsabilité, que les produits sont conformes aux spécifications suivantes :

Certification	Type
EN 55032 : 2015+A11:2020 BS EN 55032 : 2015+A11:2020 EN IEC 61000-3-2 : 2019+A1:2021 BS EN IEC 61000-3-2 : 2019+A1:2021 EN 61000-3-3 : 2013+A1:2019+A2:2021+AC:2022-01 BS EN 61000-3-3 : 2013+A1:2019+A2:2021 EN 55035 : 2017+A11:2020 BS EN 55035 : 2017+A11:2020 IEC 61000-4-2 : 2008 IEC 61000-4-3 : 2020 IEC 61000-4-4 : 2012 IEC 61000-4-5 : 2014+A1:2017 IEC 61000-4-6 : 2023 IEC 61000-4-8 : 2009 IEC 61000-4-11 : 2020+COR1:2020 Pièce 47 CFR FCC Sous pièce 15 B ICES-003 émission 7 : octobre 2020 ANSI C63.4 : 2014 VCCI-CISPR 32 : 2017 AS/NZS CISPR 32 : 2015+A1:2020	EMI (Interférence électromagnétique) et EMC (Compatibilité électromagnétique)
CE LVD EN62368-1 CB IEC /EN62368-1 2e et 3e édition. AS/NZS 62368.1:2022 CSA C22.2 n° 62368-1:2019 GB 4943.1-2022 EN IEC 62368-1:2020+A11:2020, BS EN IEC 62368-1:2020+A11:2020 J62368-1 (2023) Norme nationale SASO-IEC 62368-1:2020 UL 62368-1:2019 KC 62368-1 (2021-08) UL62368-1	Sécurité électrique

Laboratoire d'essais

Nom	Adresse
Prodigy Technology Consultant Co.	12, Gong 7th Rd., Linkou District, New Taipei City 24450, Taïwan
SGS Taiwan Ltd.	Laboratoire de compatibilité électromagnétique No.2, Keji 1st Rd, Guishan District, Taoyuan City, Taiwan

Fiabilité physique et environnementale	Description
Conditions de fonctionnement	Vibrations et chocs sur la base de la norme EN 300 019-2-3.
Conditions d'entreposage	Température : (-40) °C ~ 60 °C. Humidité : 95 %, sans condensation. Vibrations et chocs sur la base de la norme EN 300 019-2-1.
Conditions de transport	Température : (-40) °C ~ 85 °C. Humidité : 95 %, sans condensation. Vibrations et chocs sur la base de la norme EN 300 019-2-2.

Déclaration de la Commission fédérale des communications (FCC)

FCC SDOC

Conformément à la partie 15 de la FCC

Nous, Check Point Software Technologies Ltd.

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

Ce dispositif est conforme à la section 15 des réglementations de la FCC. Le fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas causer d'interférences nuisibles, et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences susceptibles de provoquer un fonctionnement indésirable.

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.

Avertissement de la FCC

- Tout changement ou modification non expressément approuvé par la partie responsable de la conformité peut annuler l'autorité de l'utilisateur à faire fonctionner cet équipement.
- Cet émetteur ne doit pas être installé ou utilisé en conjonction avec d'autres antennes ou émetteurs.
- Les opérations dans la bande 5,15-5,25 GHz sont limitées à une utilisation en intérieur uniquement.

Cet appareil est conforme à toutes les autres exigences spécifiées dans la partie 15E, section 15.407 des règles de la FCC.

Déclaration d'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 35 cm entre l'élément rayonnant et l'utilisateur.

Déclaration de conformité de la classe B au Japon

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI－B

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/UE). Ce produit est certifié conforme aux exigences de la directive RED 2014/53/EU.

Ce produit est conforme à la directive basse tension 2014/35/UE et satisfait aux exigences de la directive 2014/35/UE 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.

1. Les dispositifs ne doivent pas être utilisés pour commander des systèmes d’aéronef sans pilote ni pour communiquer avec de tels systèmes.
2. L'utilisation doit être limitée à un usage intérieur uniquement.
3. L'exploitation sur les plateformes pétrolières, les automobiles, les trains, les navires maritimes et les aéronefs sera interdite, sauf pour les opérations dans la bande de 5925-6425 MHz sur les grands aéronefs volant au-dessus de 3 048 m (10 000 pieds)."

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.

Proposition 65 – Produits chimiques

Produits chimiques identifiés par l'État de Californie, conformément aux exigences du California Safe Drinking Water and Toxic Enforcement Act de 1986, California Health & Safety Code s. 25249.5, et seq. (« Proposition 65 »), qui sont « considérés par l'État comme pouvant provoquer le cancer ou avoir des effets toxiques sur 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.

Pour l'utilisation de la sélection du code pays (appareils WLAN)

Remarque : La sélection du code pays est réservée aux modèles non américains et n'est pas disponible pour tous les modèles américains. Conformément à la réglementation de la FCC, tous les produits WiFi commercialisés aux États-Unis doivent être fixés sur les canaux d'exploitation américains uniquement.

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

Déclaration de conformité du ministère canadien

Cet émetteur radio [IC : 7849A-WLE3000HX] a été approuvé par le ministère de l'Innovation, des Sciences et du Développement économique du Canada pour fonctionner avec les types d'antennes énumérés ci-dessous, avec le gain maximal autorisé indiqué. Les types d'antennes qui ne figurent pas dans cette liste et dont le gain est supérieur au gain maximal indiqué pour tout type répertorié sont strictement interdits pour une utilisation avec cet appareil.

Exemple de déclaration pour les antennes : Fabricant : INPAQ, MPN : RFDPA171300SBLB801

Bande de fréquence	Type d'antenne	Gain maximal	Impédance Ω
2414-2462 MHz	Antenne dipôle (RP-SMA)	2,22 dBi	50 Ω
5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	Antenne dipôle (RP-SMA)	4,29 dBi	50 Ω

Déclaration d'exposition aux rayonnements

Cet appareil est conforme aux limites d'exposition aux rayonnements de l'IC fixées pour un environnement non contrôlé. Cet appareil doit être installé et utilisé en maintenant une distance minimale de 35 cm entre le radiateur et votre corps.

Cet appareil est conforme aux normes RSS exemptes de licence d'Industrie Canada. Son fonctionnement est soumis aux deux conditions suivantes :

1. Cet appareil ne doit pas provoquer d'interférences, et
2. Cet appareil doit accepter toute interférence, y compris les interférences susceptibles d'entraîner un fonctionnement indésirable de l'appareil.

Cet appareil numérique de classe B est conforme à la norme canadienne ICES-003.

Cet appareil et sa ou ses antennes ne doivent pas être installés ou fonctionner en conjonction avec une autre antenne ou un autre émetteur, à l'exception des radios intégrées testées.

La fonction de sélection du code de comté est désactivée pour les produits commercialisés aux États-Unis/au Canada.

POUR LES APPAREILS WLAN 5 GHz :

Attention :

1. L'appareil fonctionnant dans la bande 5150-5250 MHz ne doit être utilisé qu'à l'intérieur des bâtiments afin de réduire les risques d'interférences nuisibles avec les systèmes mobiles par satellite à canal commun ;
2. Pour les appareils à antenne(s) amovible(s), le gain d'antenne maximal autorisé pour les appareils dans les bandes 5250-5350 MHz et 5470-5725 MHz doit être tel que l'équipement reste conforme à la limite de la PIRE ;
3. Le gain d'antenne maximal autorisé pour les appareils dans les bandes 5250-5350 MHz et 5470-5725 MHz doit respecter la limite de la PIRE ; et
4. Pour les appareils à antenne(s) amovible(s), le gain d'antenne maximal autorisé pour les appareils dans la bande 5725-5850 MHz doit être tel que l'équipement reste conforme aux limites de la PIRE, le cas échéant ;
5. Le gain d'antenne maximal autorisé pour les appareils dans la bande 5725-5850 MHz doit être conforme aux limites de la PIRE spécifiées pour le fonctionnement point à point et non point à point, selon le cas.
6. Le ou les angles d'inclinaison les plus défavorables nécessaires pour rester conforme à l'exigence de masque d'élévation de la PIRE énoncée au point 6.2.2 (3) doivent être clairement indiqués. (Pour 5G B2 avec appareils DFS uniquement)
7. Le cas échéant, le ou les types d'antenne, le ou les modèles d'antenne et le ou les angles d'inclinaison les plus défavorables nécessaires pour rester conformes à l'exigence de masque d'élévation de la PIRE énoncée au point 6.2.2.3 doivent être clairement indiqués.
8. Les utilisateurs doivent également savoir que les radars de forte puissance sont des utilisateurs primaires (c'est-à-dire des utilisateurs prioritaires) des bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars peuvent provoquer des interférences et/ou endommager les appareils LE-LAN.

Déclaration d'Industrie Canada

POUR L'UTILISATION D'APPAREILS MOBILES (>35 cm/faible puissance)

Cet appareil est conforme aux RSS exemptés de licence de l'ISED. Le fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas causer d'interférences nuisibles, et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences susceptibles de provoquer un fonctionnement indésirable.

Déclaration **d'exposition** aux rayonnements :

Cet appareil est conforme aux limites d'exposition aux rayonnements fixées par l'ISED pour un environnement non contrôlé. Cet appareil doit être installé et utilisé en maintenant une distance supérieure à 35 cm entre le radiateur et votre corps.

Utilisation de l'antenne détachable

Cet émetteur radio (IC : 2417C-EM91) a été approuvé par l'ISED pour fonctionner avec le type d'antenne listé ci-dessous avec le gain maximum autorisé indiqué. L'utilisation avec cet appareil d'antennes dont le type ne figure pas dans cette liste et dont le gain est supérieur au gain maximal indiqué pour ce type d'antenne est strictement interdite. **Remarque :** Ce paragraphe ne concerne que les modèles V91WC.

Cet émetteur radio (IC : 2417C-EM75T) a été approuvé par l'ISED pour fonctionner avec le type d'antenne listé ci-dessous avec le gain maximum autorisé indiqué. L'utilisation avec cet appareil d'antennes dont le type ne figure pas dans cette liste et dont le gain est supérieur au gain maximal indiqué pour ce type d'antenne est strictement interdite. **Remarque :** Ce paragraphe ne concerne que les modèles V91WL.

Tableau de gain d'antenne

Modèle	Nom de la pièce	Numéro de pièce IEI	Bande de fréquence	Gain maximal	Impédance Ω	Type d'antenne
T1.2 WiFi	Antenne WiFi	CKP-32505-012500-100-HF	2412-2472 MHz	2,83 dBi	50 Ω	Antenne dipôle (non détachable)

Modèle	Nom de la pièce	Numéro de pièce IEI	Bande de fréquence	Gain maximal	Impédance Ω	Type d'antenne
			5945-7125 MHz	4,53 dBi	50 Ω	

Modèle	Nom de la pièce	Numéro de pièce IEI	Bande de fréquence	Gain maximal	Impédance Ω	Type d'antenne
			5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,98 dBi	50 Ω	
	Antenne WiFi	CKP-32505-012600-100-HF	2412-2472 MHz	2,83 dBi	50 Ω	Antenne dipôle (indétectable)
			5945-7125 MHz	5,43 dBI	50 Ω	
			5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,98 dBi	50 Ω	
	Antenne WiFi	CKP-32505-012700-100-HF	5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,49 dBi	50 Ω	Antenne dipôle (indétectable)
	Antenne WiFi	CKP-32505-012800-100-HF	5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,49 dBi	50 Ω	Antenne dipôle (indétectable)

Modèle	Nom de la pièce	Numéro de pièce IEI	Bande de fréquence	Gain maximal	Impédance Ω	Type d'antenne
T1.2 WiFi + 5 GNR	Antenne WiFi	CKP-32505-012900-100-RS	2412-2472 MHz	1,27 dBi	50 Ω	Antenne dipôle (indétectable)

Modèle	Nom de la pièce	Numéro de pièce IEI	Bande de fréquence	Gain maximal	Impédance Ω	Type d'antenne
			5945-7125 MHz	3,62 dBi	50 Ω	

Modèle	Nom de la pièce	Numéro de pièce IEI	Bande de fréquence	Gain maximal	Impédance Ω	Type d'antenne
			5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,68 dBi	50 Ω	

Modèle	Nom de la pièce	Numéro de pièce IEI	Bande de fréquence	Gain maximal	Impédance Ω	Type d'antenne
	Antenne WiFi	CKP-32505-013000-100-RS	2412-2472 MHz	1,27 dBi	50 Ω	Antenne dipôle (indétectable)
			5945-7125 MHz	3,62 dBi	50 Ω	
			5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,68 dBI	50 Ω	
	Antenne WiFi	CKP-32505-013100-100-RS	5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,51 dBi	50 Ω	Antenne dipôle (indétectable)
	Antenne WiFi	CKP-32505-013200-100-RS	5180-5240, 5260-5320, 5500-5720, 5745-5825 MHz	3,51 dBi	50 Ω	Antenne dipôle (indétectable)
	Antenne 5 GNR	CKP-32513-000800-100-RS	617-960 MHz	1,98 dBI	50 Ω	Antenne dipôle (RP-SMA)
			1710-2690 MHz	3,95 dBi	50 Ω	
			3300-5925 MHz	3,24 dBi	50 Ω	

Exigences de sécurité communes pour l'équipement radio

La norme européenne EN 18031 traite de la cybersécurité des appareils radio connectés à Internet.

Pour se conformer à la norme, qui exige la persistance des journaux, l'appareil ne doit pas être utilisé en production, sauf si l'une des conditions suivantes est remplie :

- La surveillance étendue est activée
- Spark Management est configuré
- Un serveur de journaux externe est configuré

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: *Check Point Support Center*.

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