QUANTUM

12 May 2024

QUANTUM SPARK 1600 / 1800 APPLIANCE

Getting Started Guide

CHECK POINT™

Check Point Copyright Notice

© 2020 - 2024 Check Point Software Technologies Ltd.

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 1600 / 1800 Appliance Getting Started Guide
For more about 1600 / 1800 appliances, 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
12 May 2024	Reformatting changes
03 October 2023	Updated *"Front Panel" on page 15* - added link to sk92755
20 April 2023	Updated *"Front Panel" on page 15*
28 July 2022	Updated URL link
21 March 2021	Clarified central management by Security Management Server
02 February 2021	Rebranded from "SMB" Appliances to "Quantum Spark" Appliances
10 December 2020	First release of this document

Table of Contents

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 configuration instructions, see the:

- *R81.10.X Quantum Spark Release Notes for 1500, 1600, 1800, 1900, 2000 Appliances*.

- *R81.10.X Quantum Spark Locally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- *R81.10.X Quantum Spark Centrally Managed Administration Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- *R81.10.X Quantum Spark CLI Reference Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

- *R81.10.X Quantum Spark Dynamic Routing CLI Guide for 1500, 1600, 1800, 1900, 2000 Appliances*.

Important Links:

- *sk178604 - Quantum Spark R81.10.X Known Limitations*.

- *sk181134 - Quantum Spark R81.10.X Resolved Issues*.

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

Quantum Spark 1600 / 1800 Appliance

The Quantum Spark 1600 / 1800 Security Appliances, part of the new 1500 / 1600 / 1800 Appliance family, deliver enterprise-grade security and run the R80 code base in an all-in-one security solution to protect Medium Business employees, network and data from cyber-theft.

The 1600 / 1800 Security Gateways offer integrated, multi-layered security in a 1U form factor, a high performance platform which is easy and simple to configure and manage. The Security Gateway offers firewall, VPN, Anti-Virus, Application Visibility and Control, URL Filtering, Email Security, and SandBlast Zero-Day Protection.

Quantum Spark 1600 / 1800 Security Appliances can be managed:

- Locally - In a Web interface

- Centrally - The Security Gateway is managed by a remote Security Management Server in SmartConsole, or by means of a cloud-based Quantum Spark Security Management Portal (SMP).

Shipping Carton Contents

Item	Quantity	Description
Appliance	1	1600 or 1800 Appliance.
LAN cable	1 (1600) 2 (1800)	1.8m - RJ45 to RJ45, CAT5e (for 1600) or CAT6e (for 1800), shielded, STP, black color.
Console cable	1	1m, USB type-C to USB-2.0 type-A, black color.
Power cord	1 (1600) 2 (1800)	Plug types: US, UK, EU and AUS/NZ, India, China, Japan.
Rubber feet	4	Not assembled.
AC cord tie	1 (1600) 2 (1800)	Cable ties to hold the power cords. Thread these ties directly into the back panel of the appliance.
Rack Mount kit	1	Brackets + screws, side ears.
Guides	1	*Quantum Spark 1600/1800 Appliance Quick Start Guide.*
License Agreement	1	End user license agreement.

Setting up the Appliance

1. Remove the Quantum Spark 1600 / 1800 Appliance from the shipping carton and place it on a tabletop.

   For other mounting options, see below.

2. **Optional** - Remove the transparent protective sticker from the front panel of the appliance.

3. Identify the network interface marked as LAN1. This interface is preconfigured with the IP address `192.168.1.1`.

Connecting the Cables

1. Connect the power cord.

   Note - Quantum Spark 1800 appliance has 2 power cords and both must be 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 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.

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

First Time Deployment Options
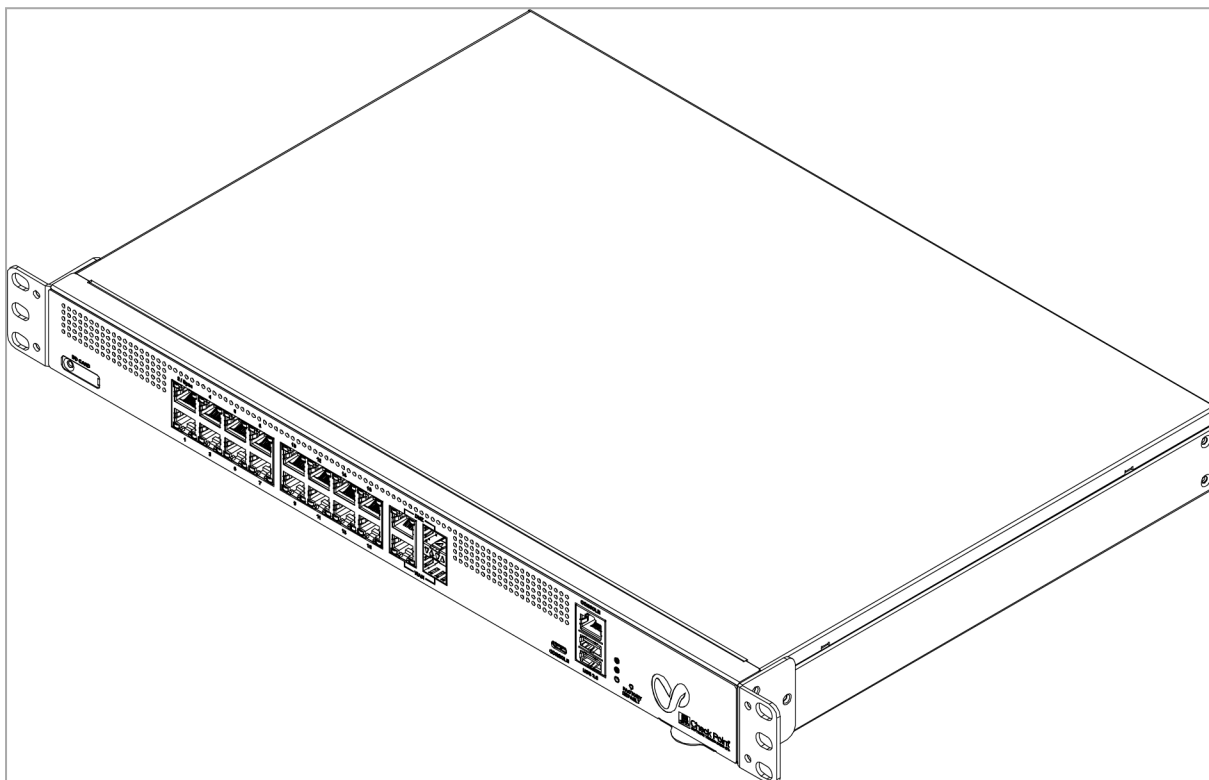
There are different options for first time deployment of your gateways:

- *"Using the First Time Configuration Wizard" on page 23*

- *"Zero Touch Cloud Service" on page 44*
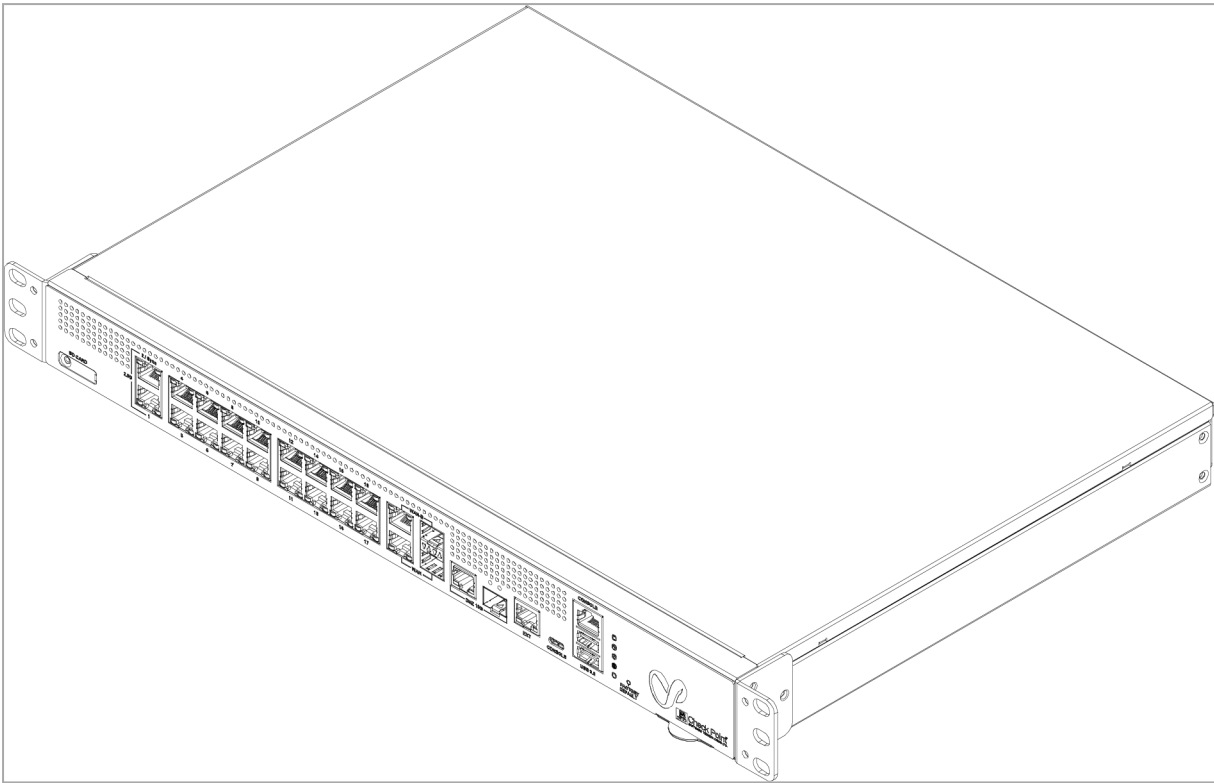
- *"USB Drive" on page 46*

Appliance Diagrams and Specifications

This structure describes the different features in the front and back panels of these appliances:
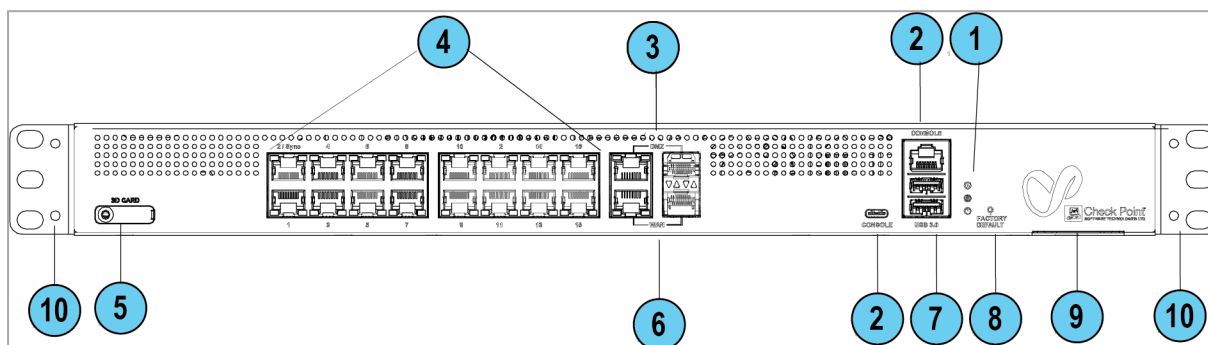
1600 Appliance

1800 Appliance

Front Panel

This section describes the Front Panel on 1600 and 1800 Appliances - LEDs, ports, and buttons.

Front Panel on a 1600 Appliance

ℹ️ **Note** - There is only one set of LEDs. These LEDs show different colors depending on what activity is occurring.

Key	Item	Description
1	LEDs	From top to bottom: ■ Management • No management - Off • Colors - See below ■ Internet • No internet connection - Off • Connecting to the internet - Blinking blue • Connected - Blue • Connection failure - Blinking red ■ Power/Status • Normal operation - Solid blue • Boot in progress or installing firmware - Blinking blue • Error/Alert - Red
2	Console	There are two console ports for the serial console cable: USB Type-C and RJ45. USB Type-C has priority when both are connected. Baud rate: 115200

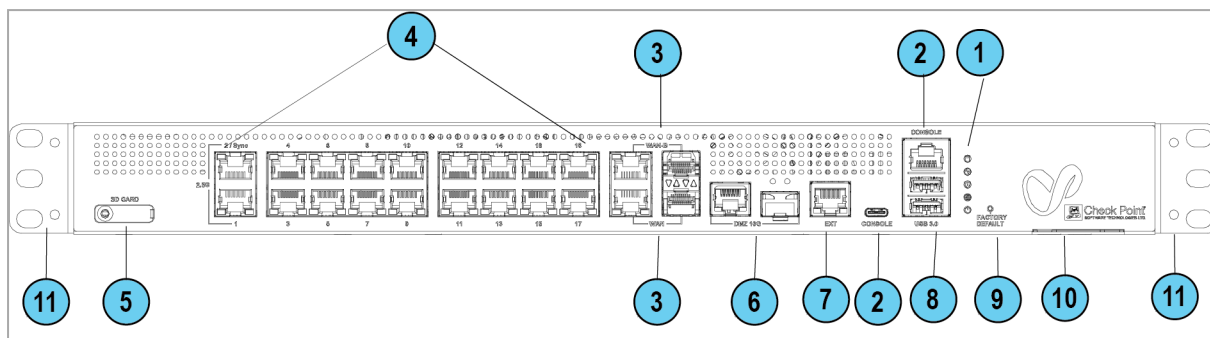| Key	Item	Description
3	DMZ ports	The DMZ is a combo port of fiber SFP and RJ45 (on the right). Only one can operate a time when plugged in and connected. The RJ45 port supports 10 / 100 MbE and 1 GbE. The SFP port supports only 1 GbE. ℹ️ **Note** - For information about supported SFP transceivers, see sk92755.
4	LAN ports	LAN ports 1-16. Support 10 / 100 MbE and 1 GbE. LAN 1 and LAN 2 (Sync in a cluster) also support 2.5 GbE.
5	SD card slot	Insert micro-SD card here.
6	WAN ports	Two WAN ports, each of which is a combo port of SFP and RJ45 (on the right). Only one can operate a time when plugged in and connected. The RJ45 port supports 10 / 100 MbE and 1 GbE. The SFP port supports only 1 GbE. ℹ️ **Note** - For information about supported SFP transceivers, see sk92755.
7	USB 3.0 (Type-A)	Two USB ports 3.0 for software download.
8	Factory Default	Press the button continuously for 12 seconds to restore the appliance to its factory default. All user parameters previously configured are removed.
9	Service tag	Shows the regulated module, serial number, and the MAC address.
10	Side brackets	For rack mount.

Front Panel on a 1800 Appliance

Note - There is only one set of LEDs. These LEDs show different colors depending on what activity is occurring.

Key	Item	Description
1	LEDs	From top to bottom: ■ Storage memory - SSD storage memory. Bi-color blue/red displays SSD status. • No SSD access - Blue Off, Red Off • SSD failure - Blue Off, Red On ■ Power redundancy - 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 ■ Management - See below ■ Internet • No internet connection - Off • Connecting to the internet - Blinking blue • Connected - Blue • Connection failure - Blinking red ■ Power/Status • Normal operation - Solid blue • Boot in progress or installing firmware - Blinking blue • Error/Alert - Red
2	Console	There are two console ports for the serial console cable: USB Type-C and RJ45. USB Type-C has priority when both are connected. Baud rate: 115200.

Key	Item	Description
3	DMZ ports	The DMZ is a combo port of fiber SFP and RJ45 (on the right). Only one can operate a time once plugged in and connected. The RJ45 port supports 10 / 100 MbE and 1 / 2.5 / 5 / 10 GbE. The SFP port supports only 10 GbE. ℹ **Note** - For information about supported SFP transceivers, see sk92755.
4	LAN ports	LAN ports 1-18. Support 10 / 100 MbE and 1 GbE. LAN 1 and LAN 2 (Sync in a cluster) also support 2.5 GbE.
5	SD card slot	Insert micro-SD card here.
6	WAN and WAN-B ports	Two WAN ports each of which is a combo port of SFP and RJ45 (on the right). Only one can operate a time once plugged in and connected. The RJ45 port supports 10 / 100 MbE and 1 / 2.5 / 5 / 10 GbE. The SFP port supports only 1 GbE. ℹ **Note** - For information about supported SFP transceivers, see sk92755.
7	EXT port	Management port. Supports 10 / 100 MbE and 1 GbE.
8	USB3.0	USB port 3.0 for software download.
9	Factory Default	Press the button continuously for 12 seconds to restore the appliance to its factory default. All user parameters previously configured are removed.
10	Service tag	Shows the regulated module, serial number, and the MAC address.
11	Side brackets	For rack mount.

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.	Off
Activation sleeping time.	Blinks blue (slowly)
Reactivation.	Blinks blue (rapidly)
SMP is connected.	Solid blue
SMP mode is off.	off
Gateway failed to connect to the SMP and will exit from the retry script.	Solid 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 (green/amber) to reflect the link/activity and speed.

This also applies to the DMZ port of the 1600 appliance.

RJ45 and 1G SFP	Link/Act LED1 (Green)	Speed LED2 (Amber)
No link	Off	*Off*
1G link	On	*Off*
1G Act	Blink	On
100M link	On	*Off*
100M Act	Blink	*Off*
10M link	On	*Off*
10M Act	Blink	*Off*

For 1800 appliances only:

2xRJ45 2.5GbE ports

Two bi-color (green and amber) LEDs per ports

2.5GbE RJ45	Link/Act LED #1 (bi-color)		Speed LED #2 (bi-color)	
	Green	Amber	Green	Amber
No link	*Off*	*Off*	*Off*	*Off*
2.5G link	On		*Off*	—
2.5G Act	Blink		*Off*	—
1G link	—	On	—	On
1G Act	—	Blink	—	On
100M link	—	On	—	Blink
100M Act	—	Blink	—	Blink
10M link	—	On	—	*Off*
10M Act	—	Blink	—	*Off*

RJ45 and SFP 10GbE port

10GbE RJ45	Link/Act LED1 (Bi-color)		Speed LED2 (Bi-color)	
	Green	Amber	Green	Amber
10G link	On	—	On	—
10G Act	Blink	—	On	—
5G link	On	—	Blink	—
5G Act	Blink	—	Blink	—

Back Panel

1600 Appliance
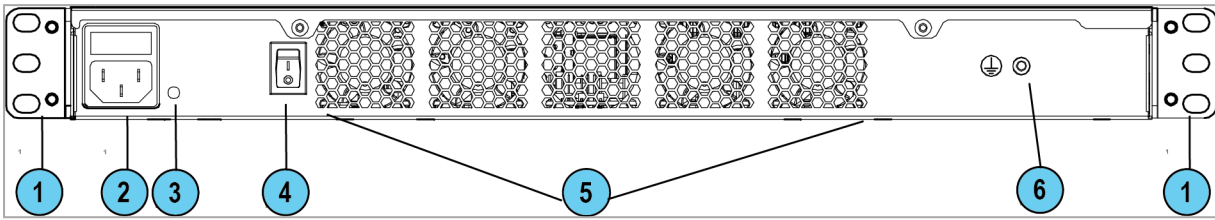
1800 Appliance
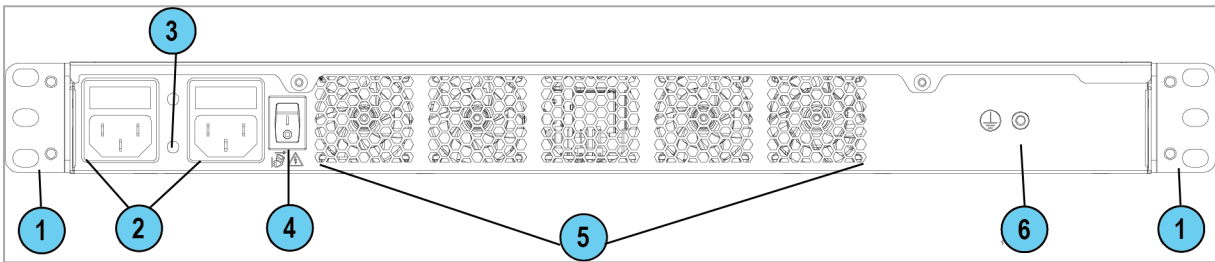
Key	Item	Description
1	Side brackets	For rack mount.
2	Power cord socket	Plug the power adapter cord in here.
3	Cable tie holes	Thread cable tie through these holes.
4	Power on/off switch	0 - Off 1 - On
5	Fans	Cooling function.
6	Ground screw	Protective earthing. For more information, refer to the *"Health and Safety Information" on page 47*.

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 1600 / 1800 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 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.
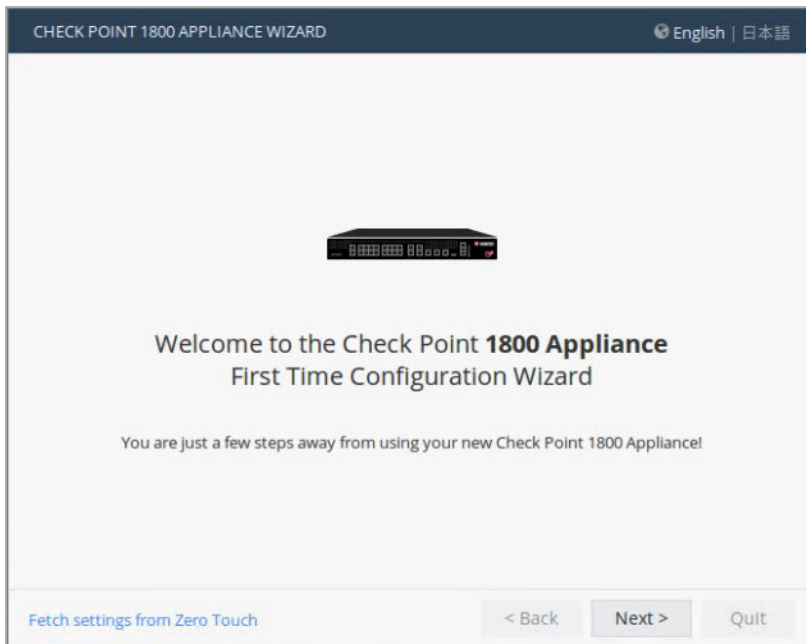
You can connect to the Zero Touch server to fetch settings automatically from the cloud.

To change the language of the WebUI application:

Select the language link at the top of the page.

ℹ️ **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.

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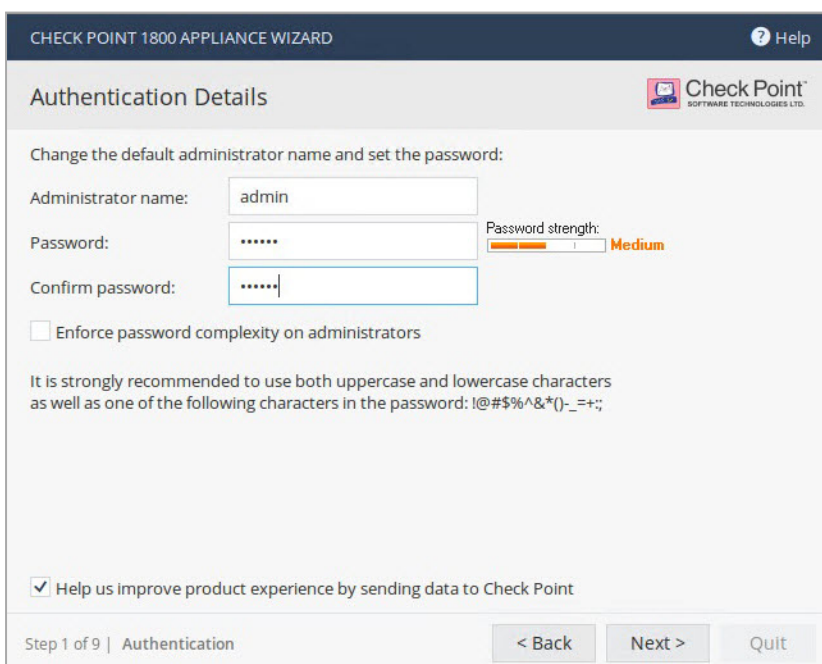
- **Confirm Password** - Enter the password again.

- **Country** - Select a country from the list **(for wireless network models 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`
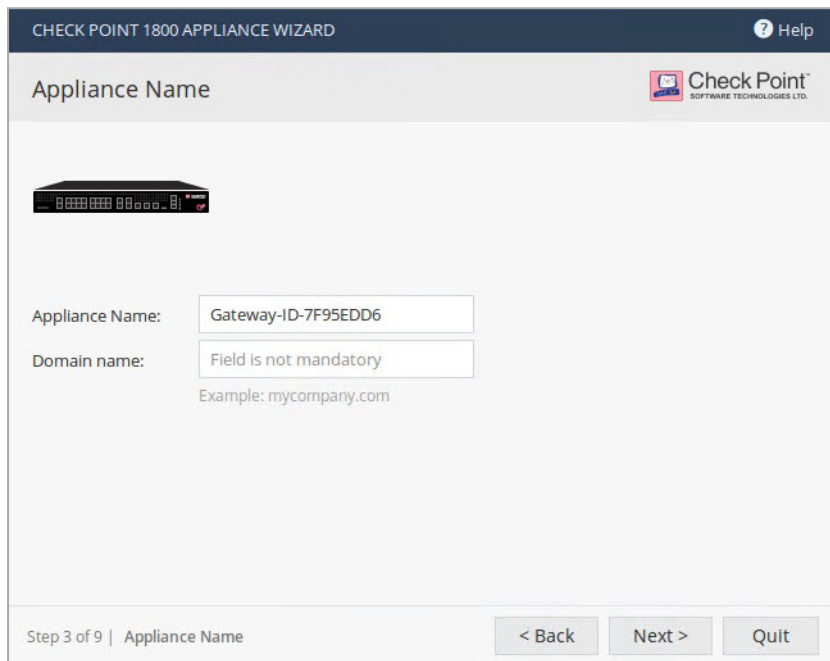
Appliance Name

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.
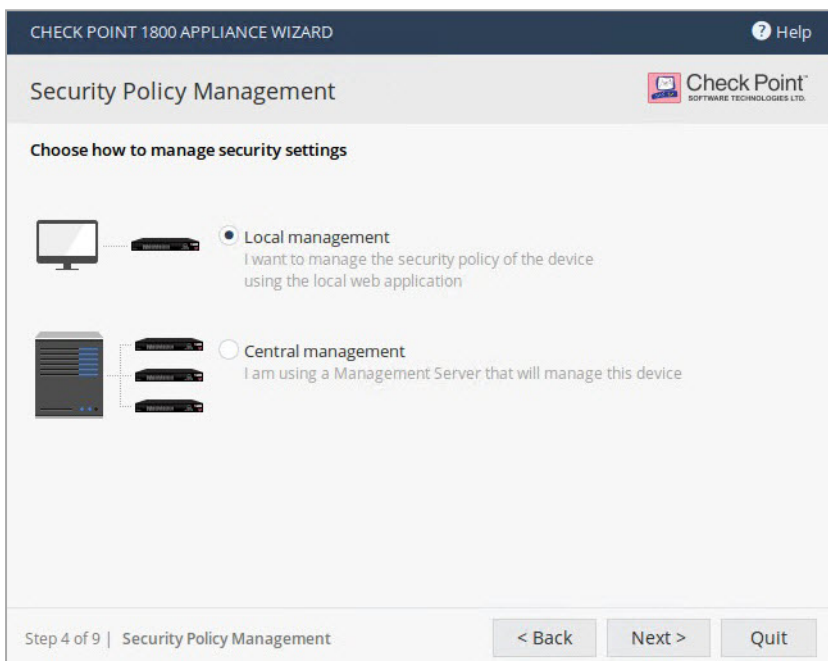
Internet Connection

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.
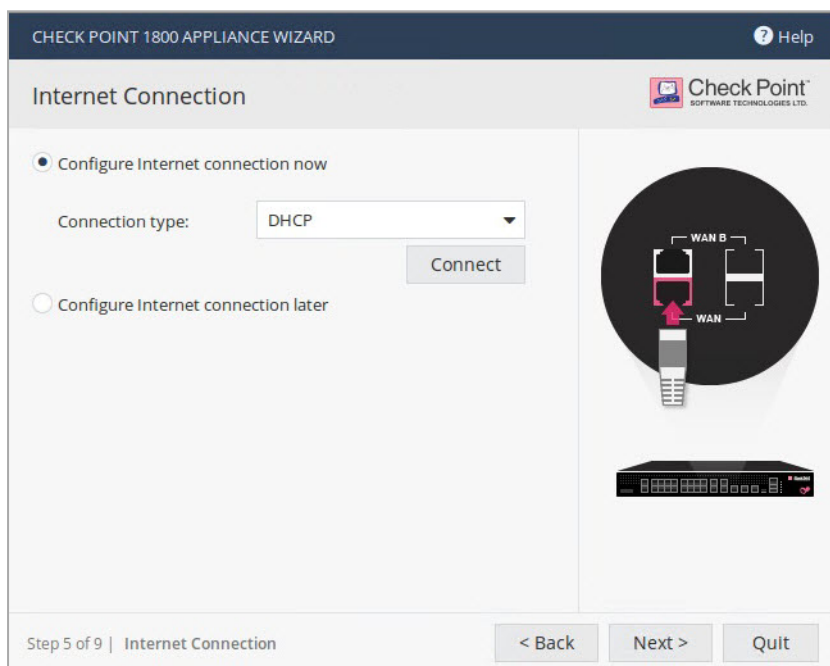
Local Network

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**.

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**.
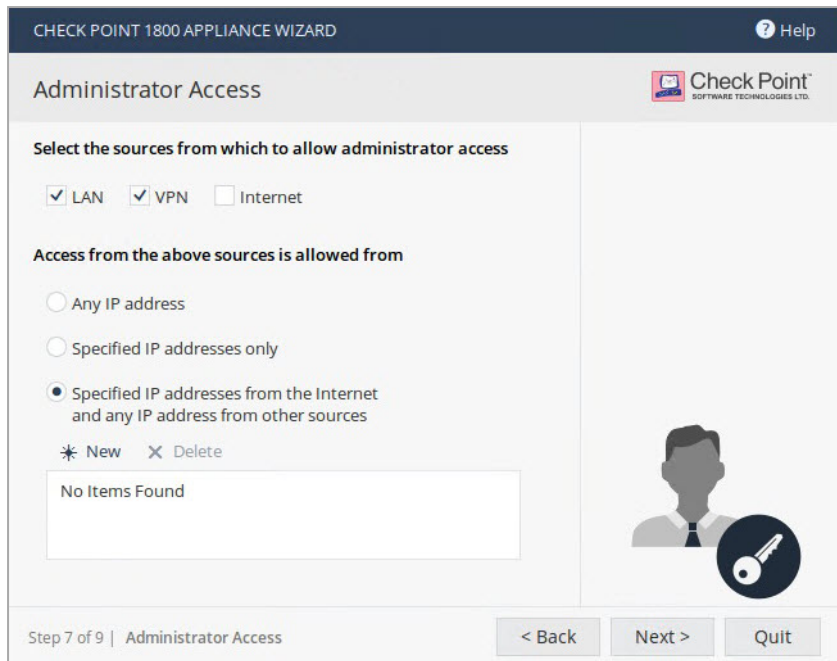
Appliance Registration

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:

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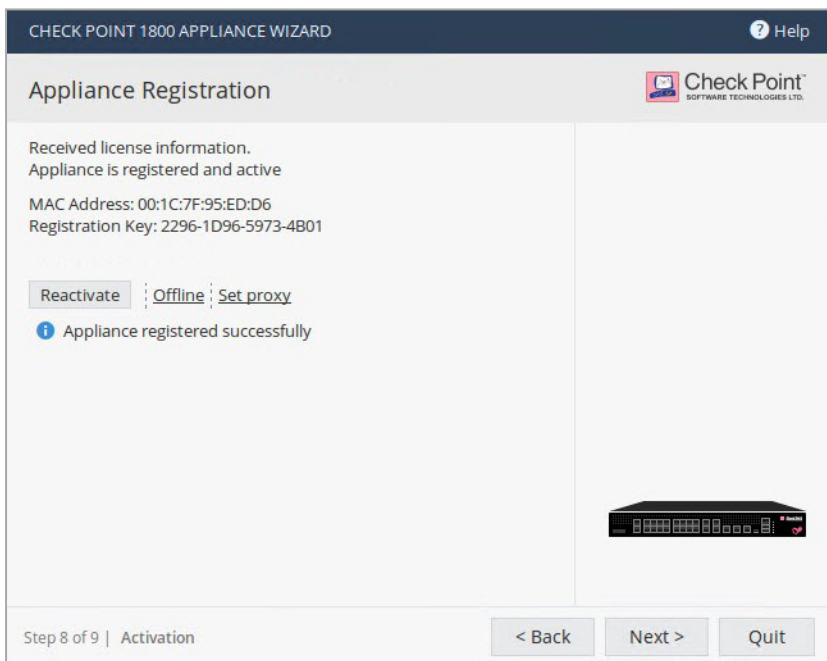
If your device is not paired with a User Center account, you must create an account or ask your company administrator to create one for you.

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.

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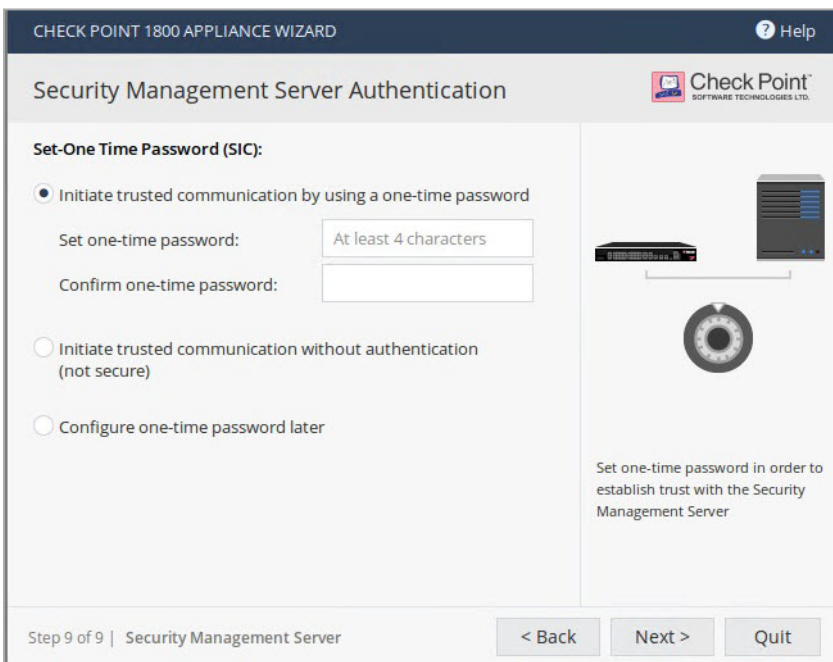
Select an option to authenticate trusted communication with the Security Management Server:

- **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 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.

CHECK POINT 1800 APPLIANCE WIZARD   ② Help

Security Management Server Connection

Check Point®
SOFTWARE TECHNOLOGIES LTD.

○ Connect to the Security Management Server now
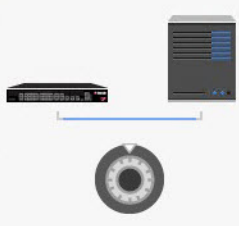
    Management address: [＿＿＿＿＿＿＿]

                [Connect]

    ☐ Customize logs settings:

       ○ Send logs to same address

       ○ Send logs to: [＿＿＿＿]

       ● Send logs according to policy

○ Connect to the Security Management Service

○ 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.
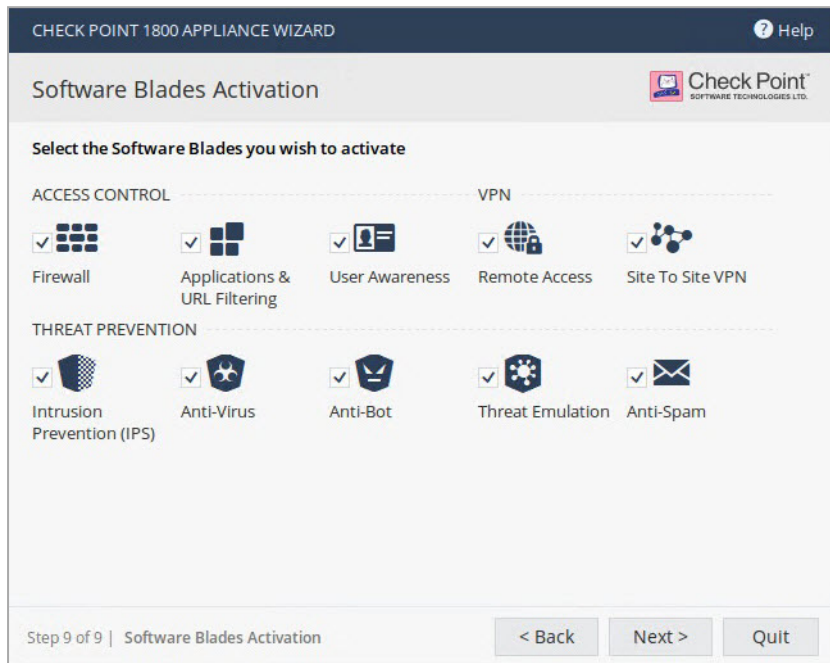
Summary

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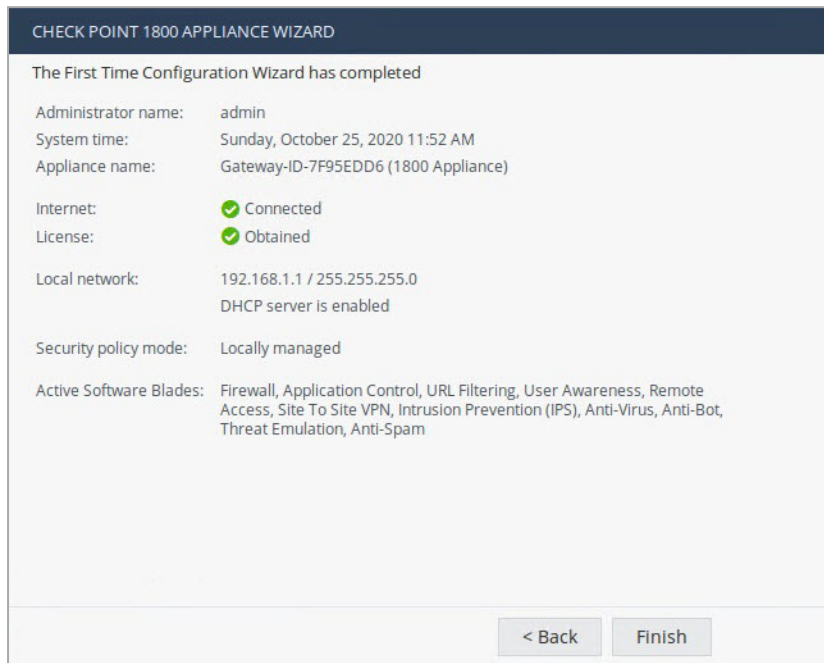
The WebUI opens on the **Home** > **System** page.

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 *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.

USB Drive

The USB drive 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 appliance starts, automatically mounts the USB drive, 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 (1,27 cm) 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

The appliance contains an embedded power supply AC-DC. The 1600 appliance contains a single power supply and the 1800 contains a dual power supply.

To prevent damage to any system, it is important to handle all parts with care.

For 1800 Appliance only:

⚡ **Caution, Shock hazard**
🖐 Disconnect all power sources.

IMPORTANT SAFETY INSTRUCTIONS: 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.

- 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 authorized by Check Point.

Connecting Earth Ground to Equipment

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

⚠️ **Caution** - Before equipment installation begins, ensure that a service personnel has attached an appropriate grounding
lug to the grounding cable supplied.

To connect earth ground to 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 earthing terminal.

3. Secure the grounding lug to the protective earthing terminal with washers and screws

4. Dress the grounding cable 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 earth. For the earthing wire, green and yellow insulation is required and the cross-sectional area of the conductor must be more than $0.75mm^2$ or 18 AWG.

🔴 **Warning** - The protective earthing 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 power is off and disconnected from the equipment, then disconnect the frame of the equipment to earth.

⚠ **Caution** - Risk of explosion if the battery is replaced by an incorrect type.

🛑 **Warning** - This is a class 1 Laser product. Use only IEC 60825-1 certified Optical Fiber Transceiver with minimum operating temperature at 75 degree C.(for EU) Laser Class 1 optical transceiver shall be used only. (for UL)

For North America only

Warning message for using product in ITE environment:

Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.

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-82, V-83
Product Options:	1600 / 1800 Appliance Wired
Date First Applied:	December 2020

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

Certification	Type
CE EN 55032:2015 + AC:2016, Class B CE EN 55032:2012 + AC:2013, Class B CE EN 61000-3-2:2014 CE EN 61000-3-3:2013 CE EN 55024:2010 / A1:2015 CE EN 55024:2010 FCC Part 15B AS/NZS CISPR32 ICES-003 VCCI, V-3/2015.4 , V4/2012.04, Class B VCCI CISPR 32:2016	EMC/EMI
EN 62368-1 CB IEC 62368-1 CSA/UL_ULc 62368-1 (Ed 2/3) AS/NZS 62368.1:2018 J 62368-1	Safety
ROHS10, REACH	Environmental

Date and Place of Issue: Tel Aviv, Israel December 2020

Testing lab

Address:	No 9 Harrison Road, Harrison Industrial Building, #05-01
Issued By:	Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch Ling Kou Laboratories
Lab Address:	No. 47-2, 14th Ling, Chia Pau Vil., Lin Kou Dist., New Taipei City, Taiwan

European Union (EU) Electromagnetic and Safety 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 Directives 2004/108/EC and 2014/30/EU. This product is in conformity with Low Voltage Directives 2006/95/EC and 2014/35/EU. This product complies with the requirements in the Council Directives 2006/95/EC and 2014/35/EU relating to electrical equipment designed for use within certain voltage limits and the Amendment Directive 93/68/EEC.

Federal Communications Commission (FCC) Notice (US)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC 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 20 centimeters between the radiator and your body. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

Compliance Information

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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Canadian Department Compliance Statement

This device complies with Industry Canada ICES-003 rules.

Japan Class B Compliance Statement

This is a Class B product based on the standard of the Voluntary Control Council for Interference (VCCI).

If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

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

Physical and environmental reliability	Description
Operating Conditions	Vibrations and Shock Based on EN 300 019-2-3. Temperature: 0°C ~ 40°C
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.

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 distributor for 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

L'appareil contient une alimentation CA-CC intégrée. L'appareil 1600 contient une seule alimentation et le 1800 contient une double alimentation.

Pour éviter d'endommager tout système, il est important de manipuler toutes les pièces avec soin.

Pour les appareils 1800 uniquement:

⚡ **Attention, Danger de choc**

Déconnecter toutes les sources d'énergie.

INSTRUCTIONS DE SÉCURITÉ IMPORTANTES: 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 autorisé par Check Point.

- N'ouvrez jamais l'équipement. Pour des raisons de sécurité, les équipements ne doivent être ouverts que par un homme de métier qualifié.

Connexion de mise à la terre à l'équipement

⛔ **Avertissement** - L'équipement dispose d'une borne de mise à la terre de protection séparée sur le châssis qui doit être connecté à la terre pour mettre le châssis à la terre de manière adéquate et protéger l'opérateur contre les risques lectriques.

⚠️ **Attention** - Avant de commencer l'installation de l'équipement, assurez-vous qu'un personnel de service a connecté une mise à la terre appropriée cosse au câble de mise à la terre fourni.

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

1. Connectez une extrémité du câble de mise à la terre à une prise de terre appropriée.

2. Placez la cosse de terre attachée au câble de terre sur la borne de mise à la terre de protection.

3. Fixez la cosse de mise à la terre à la borne de mise à la terre de protection avec des rondelles et des vis.

4. Habillez le câble de mise à la terre et assurez-vous qu'il ne touche ni ne bloque l'accès aux autres composants.

⛔ **Avertissement** - Avant de mettre l'équipement sous tension, connectez le châssis de l'équipement à la terre. Pour fil de terre, vert et une isolation jaune est requise et la section transversale du conducteur doit être supérieure à 0,75 mm ou 18 AWG.

⛔ **Avertissement** - La borne de mise à la terre de protection avec rondelles et vis dans lesquelles une vis est vissée ne doit pas être moins de deux fois le pas du filetage de la vis, au moins 3,5 mm de diamètre; Des rondelles en étoile ou des rondelles à ressort peuvent être utilisées.

⛔ **Avertissement** - Après la mise hors tension et la déconnexion de l'équipement, déconnectez le châssis de l'équipement pour mise à la terre

⚠️ **Attention** - Risque d'explosion en cas de remplacement de la pile par une pile de type incorrect.

⛔ **Avertissement** - Ceci est un produit Laser de Classe 1. Utilisez uniquement un émetteur-récepteur à fibre optique certifié CEI 60825-1 avec une température de fonctionnement minimale de 75 degrés C (l'UE)
Ceci est un produit Laser de Classe 1 avec l'émetteur-récepteur à fibre optique, conformément. (UL)

Pour l'Amérique du Nord uniquement

Message d'avertissement pour l'utilisation du produit dans l'environnement ITE:

Peut être installé dans des salles de matériel de traitement de l'information conformément à l'article 645 du National Electrical Code et à la NFPA 75

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-82, V-83
Options de produit:	1600 / 1800 Appliance Wired
Date de demande initiale:	Décembre 2020

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

Certification	Type
CE EN 55032:2015 + AC:2016, Class B CE EN 55032:2012 + AC:2013, Class B CE EN 61000-3-2:2014 CE EN 61000-3-3:2013 CE EN 55024:2010 / A1:2015 CE EN 55024:2010 FCC Part 15B AS/NZS CISPR32 ICES-003 VCCI, V-3/2015.4 , V4/2012.04,Class B VCCI CISPR 32:2016	EMC/EMI
EN 62368-1 CB IEC 62368-1 CSA/UL_ULc 62368-1 (Ed 2/3?) AS/NZS 62368.1:2018 J 62368-1	Sécurité
ROHS10, REACH	Environnement

Date et lieu d'émission: Décembre 2020, Tel Aviv, Israël

Laboratoire d'essais

Adresse:	No 9 Harrison Road, Harrison Industrial Building, #05-01
Délivré par:	Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch Ling Kou Laboratories
Adresse du laboratoire:	No. 47-2, 14th Ling, Chia Pau Vil., Lin Kou Dist., New Taipei City, Taiwan

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 2004/108/EC et 2014/30/EU. Ce produit a été confirmé conforme aux exigences 2006/95/EC et 2014/35/EU. Ce produit est conforme à la directive basse tension 2014/35/EU et satisfait aux exigences de la directive 2006/95/EC et 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/EEC.

Déclaration à la Federal Communications Commission (FCC)

Cet équipement a été testé et déclaré conforme aux limites d'un appareil numérique de classe A, conformément à la partie 15 des règles FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radiofréquence et, s'il n'est pas installé et utilisé conformément au manuel d'instructions, il peut provoquer des interférences nuisibles aux communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles, auquel cas l'utilisateur devra corriger les interférences à ses propres frais.

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 20 cm entre l'élément rayonnant et l'utilisateur. Cet appareil est conforme à la partie 15 des règles FCC. Son fonctionnement est soumis aux deux conditions suivantes:

Informations de conformité

1. Cet appareil ne doit pas causer d'interférences nuisibles, et

2. Cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant entraîner un fonctionnement indésirable.

Cet émetteur ne doit pas être colocalisé ou fonctionner en conjonction avec une autre antenne ou un autre émetteur.

Déclaration de conformité du département Canadien

Cet appareil est conforme aux normes NMB003 d'Industrie Canada.

Déclaration de conformité de classe B pour le Japon

Fiabilité physique et environnementale	Description
Conditions de fonctionnement	Vibrations et chocs selon EN 300 019-2-3.
Conditions de stockage	Température: (- 40) ° C ~ 60 ° C. Humidité: 95%, sans condensation. Vibrations et chocs selon EN 300 019-2-1.

Fiabilité physique et environnementale	Description
Conditions de transport	Température: (-40) ° C ˜ 85 ° C. Humidité: 95%, sans condensation. Vibrations et chocs selon EN 300 019-2-2.

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: *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