Check Point 600 Appliance

Locally Managed
Getting Started Guide
© 2017 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 http://www.checkpoint.com/copyright.html for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.
Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=40946

To learn more, visit the Check Point Support Center

Feedback

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

Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point 600 Appliance Locally Managed Getting Started Guide.
Health and Safety Information

Read these warnings before setting up or using the appliance.

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

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

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

- When handling the board, use a grounded wrist strap designed for static discharge elimination.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the board by its edges only. Do not touch its components, peripheral chips, memory modules or gold contacts.
• When handling processor chips or memory modules, avoid touching their pins or gold edge fingers.

• 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 even though the power is switched off.

• Under no circumstances should the lithium battery cell used to power the real-time clock be allowed to short. The battery cell may heat up under these conditions and present a burn hazard.

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

• Do not dispose of batteries in a fire or with household waste.

• Contact your local waste disposal agency for the address of the nearest battery deposit site.

• Disconnect the system board power supply from its power source before you connect or disconnect cables or install or remove any system board components. Failure to do this can result in personnel injury or equipment damage.

• Avoid short-circuiting the lithium battery; this can cause it to superheat and cause burns if touched.

• Do not operate the processor without a thermal solution. Damage to the processor can occur in seconds.
Power Supply Information

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

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

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

<table>
<thead>
<tr>
<th>Manufacturer' Name:</th>
<th>Check Point Software Technologies Ltd.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer's Address:</td>
<td>5 Ha'Solelim Street, Tel Aviv Tel Aviv 67897, Israel</td>
</tr>
</tbody>
</table>

Declares that under our sole responsibility the products

<table>
<thead>
<tr>
<th>Model Number:</th>
<th>L-50, L-50D, L-50W, L-50WD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Options:</td>
<td>All</td>
</tr>
<tr>
<td>Date First Applied:</td>
<td>2013</td>
</tr>
</tbody>
</table>
Conforms to the following Product Specifications:

<table>
<thead>
<tr>
<th>Certification</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE EMC</td>
<td>EMC</td>
</tr>
<tr>
<td>EN61000-3-2:2014 Class A</td>
<td></td>
</tr>
<tr>
<td>EN61000-3-3:2013</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-2:2009</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-4:2012</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-5:2014</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-6:2014</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-11:2004</td>
<td></td>
</tr>
<tr>
<td>FCC EMI (P15B)+ICES-003</td>
<td>EMC</td>
</tr>
<tr>
<td>Japan VCCI</td>
<td>EMC</td>
</tr>
<tr>
<td>C-Tick</td>
<td>EMC</td>
</tr>
<tr>
<td>CE LVD (EN 60950-1)</td>
<td>Safety</td>
</tr>
<tr>
<td>UL/c-UL (UL 60950-1)</td>
<td>Safety</td>
</tr>
<tr>
<td>CB IEC 60950-1</td>
<td>Safety</td>
</tr>
<tr>
<td>TBR21 (DSL EUR)</td>
<td>DSL</td>
</tr>
<tr>
<td>Certification</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Part 68 + CS-03 (DSL USA)</td>
<td>DSL</td>
</tr>
<tr>
<td>A-Tick</td>
<td>DSL</td>
</tr>
<tr>
<td>CE RF</td>
<td>RF/Wi-Fi</td>
</tr>
<tr>
<td>Draft EN 301 489-1 V2.2.0 (2017-03)</td>
<td></td>
</tr>
<tr>
<td>Draft EN 301 489-17 V3.2.0 (2017-02)</td>
<td></td>
</tr>
<tr>
<td>EN 300 328 V2.1.1 (2016-11)</td>
<td></td>
</tr>
<tr>
<td>EN 62311 : 2008</td>
<td></td>
</tr>
<tr>
<td>FCC RF Part 15B_ Subpart E</td>
<td>RF/Wi-Fi</td>
</tr>
<tr>
<td>IC RSS210 (Wi-Fi Canada)</td>
<td>RF/Wi-Fi</td>
</tr>
<tr>
<td>Japan Telec (Wifi)</td>
<td>Rf/Wi-Fi</td>
</tr>
<tr>
<td>WPC India radio approval</td>
<td>RF/Wi-Fi</td>
</tr>
</tbody>
</table>

**European Union (EU) Directives**

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 of Radio Equipment Directive 2014/30/EU.

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

This product is in conformity with the Radio Equipment Directive 2014/53/EU Frequency and maximum transmitted power: 2412 - 2472 MHz: 18.84 dBm

FW Version R77.20.60 990171471. For updates, see sk117732 http://supportcontent.checkpoint.com/solutions?id=sk117732.

**Federal Communications Commission (FCC) Statement:**

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.
To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

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:

(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 and RSS210 rules. Cet appareil est conforme aux normes NMB003 et RSS210 d’Industrie Canada.

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
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.
Informations relatives à la santé et à la sécurité

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

* Avertissement : ne pas obtruer 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.

Pour éviter d’endommager les cartes système, il est important de les manipuler avec soin. Les mesures suivantes sont généralement suffisantes pour protéger votre équipement contre les décharges d’électricité statique :

- Avant de manipuler la carte, portez aux poignet un bracelet antistatique relié à la terre.
- Touchez un objet métallique relié à la terre avant d’extraire la carte de son sachet antistatique.
- Ne tenez la carte que par ses bords. Ne touchez aucun composant, puce périphérique, module mémoire ou contact plaqué or.
• Lorsque vous manipulez des processeurs ou des modules mémoire, évitez de toucher leurs broches ou les pistes de contact dorées.

• 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 même si l’appareil est éteint.

• Il ne faut jamais court-circuiter la pile au lithium qui alimente l’horloge temps-réel. Elle risque de s’échauffer et de causer des brûlures.

Avertissement : DANGER D’EXPLOSION SI LA PILE EST MAL REMPLACÉE. NE REMPLACER QU’AVEC UN TYPE IDENTIQUE OU ÉQUIVALENT, RECOMMANDÉ PAR LE CONSTRUCTEUR. LES PILES DOIVENT ÊTRE MISES AU REBUT CONFORMÉMENT AUX INSTRUCTIONS DE LEUR FABRICANT.

• Ne pas jeter les piles au feu ni avec les déchets ménagers.

• Pour connaître l’adresse du lieu le plus proche de dépôt des piles, contactez votre service local de gestion des déchets.

• Débranchez l’alimentation de la carte système de sa source électrique avant de connecter ou déconnecter des câbles ou d'installer ou retirer des composants. À défaut, les risques sont d’endommager l’équipement et de causer des blessures corporelles.

• Ne pas court-circuiter la pile au lithium : elle risque de surchauffer et de causer des brûlures en cas de contact.
• Ne pas faire fonctionner le processeur sans refroidissement. Le processeur peut être endommagé en quelques secondes.

**Information pour l’alimentation**

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

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

**Pour la Californie :**


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 »**

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

<table>
<thead>
<tr>
<th>Nom du constructeur:</th>
<th>Check Point Software Technologies Ltd.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adresse du constructeur:</td>
<td>5 Ha‘Solelim Street, Tel Aviv</td>
</tr>
<tr>
<td></td>
<td>Tel Aviv 67897, Israel</td>
</tr>
</tbody>
</table>

Déclare sous son entière responsabilité que les produits

<table>
<thead>
<tr>
<th>Numéro de modèle:</th>
<th>L-50, L-50D, L-50W, L-50WD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options de produit:</td>
<td>All</td>
</tr>
<tr>
<td>Date de demande initiale:</td>
<td>2013</td>
</tr>
</tbody>
</table>
Sont conformes aux normes produit suivantes:

<table>
<thead>
<tr>
<th>Certification</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE EMC</td>
<td>EMC</td>
</tr>
<tr>
<td>European Standard EN 55032 :</td>
<td></td>
</tr>
<tr>
<td>EN61000-3-2:2014 Class A</td>
<td></td>
</tr>
<tr>
<td>EN61000-3-3:2013</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-2:2009</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-4:2012</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-5:2014</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-6:2014</td>
<td></td>
</tr>
<tr>
<td>EN61000-4-11:2004</td>
<td></td>
</tr>
<tr>
<td>FCC EMI (P15B)+ICES-003</td>
<td>EMC</td>
</tr>
<tr>
<td>Japan VCCI</td>
<td>EMC</td>
</tr>
<tr>
<td>C-Tick</td>
<td>EMC</td>
</tr>
<tr>
<td>CE LVD (EN 60950-1)</td>
<td>Safety</td>
</tr>
<tr>
<td>UL/c-UL (UL 60950-1)</td>
<td>Safety</td>
</tr>
<tr>
<td>CB IEC 60950-1</td>
<td>Safety</td>
</tr>
<tr>
<td>TBR21 (DSL EUR)</td>
<td>DSL</td>
</tr>
<tr>
<td>Certification</td>
<td>Type</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Part 68 + CS-03 (DSL USA)</td>
<td>DSL</td>
</tr>
<tr>
<td>A-Tick</td>
<td>DSL</td>
</tr>
<tr>
<td>CE RF</td>
<td>RF/Wi-Fi</td>
</tr>
<tr>
<td>Draft EN 301 489-1 V2.2.0 (2017-03)</td>
<td></td>
</tr>
<tr>
<td>Draft EN 301 489-17 V3.2.0 (2017-02)</td>
<td></td>
</tr>
<tr>
<td>EN 300 328 V2.1.1 (2016-11)</td>
<td></td>
</tr>
<tr>
<td>EN 62311 : 2008</td>
<td></td>
</tr>
<tr>
<td>FCC RF Part 15B_Subpart E</td>
<td>RF/Wi-Fi</td>
</tr>
<tr>
<td>IC RSS210 (Wi-Fi Canada)</td>
<td>RF/Wi-Fi</td>
</tr>
<tr>
<td>Japan Telec (Wifi)</td>
<td>Rf/Wi-Fi</td>
</tr>
<tr>
<td>WPC India radio approval</td>
<td>RF/Wi-Fi</td>
</tr>
</tbody>
</table>

**European Union (EU) Directives**

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 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.

Ce produit est conforme à l’équipement radio Directive 2014/35/UE fréquence et puissance maximale transmise: 2412 - 2472 MHz: 18.84 dBm


Déclaration à la Federal Communications Commission (FCC) :

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.

Pour garantir le respect des réglementations, toute modification non approuvée expressément par la partie responsable de la conformité doit annuler le droit de faire fonctionner l'équipement. (Exemple : n'utiliser que des câbles d'interface blindés pour la connexion à l'ordinateur ou aux périphériques).

**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. Ce dispositif est conforme à la section 15 des réglementations de la FCC. Son fonctionnement est soumis aux deux conditions suivantes :

(1) Cet appareil ne doit pas causer d'interférence préjudiciable et
(2) Cet appareil doit tolérer toute interférence reçue, y compris celles qui pourraient causer un fonctionnement indésirable.

Cet émetteur ne doit pas être installé ou utilisé en conjonction avec d'autres antennes ou émetteurs.
Déclaration de conformité du département Canadien :

This device complies with Industry Canada ICES-003 and RSS210 rules. Cet appareil est conforme aux normes NMB003 et RSS210 d’Industrie Canada.

Déclaration de conformité de classe B pour le 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
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.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health and Safety Information</td>
<td>4</td>
</tr>
<tr>
<td>Informations relatives à la santé et à la sécurité</td>
<td>13</td>
</tr>
<tr>
<td>Introduction</td>
<td>25</td>
</tr>
<tr>
<td>Welcome</td>
<td>25</td>
</tr>
<tr>
<td>Shipping Carton Contents</td>
<td>27</td>
</tr>
<tr>
<td>Check Point 600 Appliance Overview</td>
<td>28</td>
</tr>
<tr>
<td>Security Gateway Software Blades</td>
<td>28</td>
</tr>
<tr>
<td>This Getting Started Guide Includes:</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Check Point 600 Appliance</td>
<td>31</td>
</tr>
<tr>
<td>About the Appliance</td>
<td>31</td>
</tr>
<tr>
<td>Workflow</td>
<td>32</td>
</tr>
<tr>
<td>Setting up the Check Point 600 Appliance</td>
<td>32</td>
</tr>
<tr>
<td>Connecting the Cables</td>
<td>33</td>
</tr>
<tr>
<td>Using the First Time Configuration Wizard</td>
<td>34</td>
</tr>
<tr>
<td>Starting the First Time Configuration Wizard</td>
<td>34</td>
</tr>
<tr>
<td>Welcome</td>
<td>36</td>
</tr>
<tr>
<td>Authentication Details</td>
<td>37</td>
</tr>
<tr>
<td>Appliance Date and Time Settings</td>
<td>38</td>
</tr>
<tr>
<td>Appliance Name</td>
<td>39</td>
</tr>
<tr>
<td>Internet Connection</td>
<td>40</td>
</tr>
<tr>
<td>Local Network</td>
<td>43</td>
</tr>
<tr>
<td>Wireless Network (for Wireless Network Models)</td>
<td>45</td>
</tr>
<tr>
<td>Administrator Access</td>
<td>47</td>
</tr>
</tbody>
</table>
Introduction

In This Section:

Welcome .......................................................................................................................... 25
Shipping Carton Contents ........................................................................................ 27

Important - Before reading this Getting Started Guide, make sure that you have read and understood the information in the version’s release notes http://supportcenter.checkpoint.com and the Check Point R77.20 for 600/1100 Appliance Known Limitations http://supportcontent.checkpoint.com/solutions?id=sk105380.

Welcome

Thank you for choosing Check Point’s Internet Security Product Suite. We hope that you will be satisfied with this solution and our support services. 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 additional information on the Check Point Internet Security Product Suite and other security solutions, refer to: http://www.checkpoint.com (http://www.checkpoint.com). 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). For additional technical information, refer to: http://support.checkpoint.com (http://supportcenter.checkpoint.com).

Welcome to the Check Point family. We look forward to meeting all of your current and future network, application and management security needs.
Shipping Carton Contents

This section describes the contents of the shipping carton.

Contents of the Shipping Carton

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td>A single Check Point 600 Appliance</td>
</tr>
</tbody>
</table>
| Power Supply and Cables       | • 1 power supply unit  
• 1 standard network cable  
• 1 serial console cable  
• 1 telephone cable (only in ADSL models)                                                                                                                                                           |
| Guides                        | • Check Point 600 Appliance Quick Start Guide  
• Check Point 600 Appliance Getting Started Guide                                                                                                                                                   |
| Wireless Network Antennas     | • A pair of wireless network antennas (only in wireless network models)                                                                                                                             |
| Sticker                       | • LEDs behavior                                                                                                                                                                                      |
| License Agreement             | • End User License Agreement                                                                                                                                                                         |
Check Point 600 Appliance Overview

Check Point 600 Appliance delivers integrated unified threat management to protect your organization from today’s emerging threats. Based on proven Check Point security technologies such as Stateful Inspection, Application Intelligence, and SMART (Security Management Architecture), Check Point 600 Appliance provides simplified deployment while delivering uncompromising levels of security.

Check Point 600 Appliance supports the Check Point Software Blade architecture that gives independent and modular security building blocks. Software Blades can be quickly enabled and configured into your solution based on specific security needs.

Security Gateway Software Blades

These Software Blades are included in Check Point 600 Appliance:

- **Firewall**: World’s most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box. The firewall also performs Network Address Translation and intelligent VoIP security.

- **IPSec VPN**: Allows secure (encrypted) connectivity between different offices through sophisticated yet easy to manage site-to-site VPN.
• **Remote Access**: Allows secure (encrypted) connectivity to your organization from any remote user PC, laptop, or mobile device.

• **Application Control**: Signature-based granular control of thousands of Internet applications and Web 2.0 widgets.

• **URL Filtering**: Best of breed URL filtering engine, based on a central database, located in the Check Point data center. This ensures excellent coverage of URLs, while maintaining minimal footprints on devices. Check Point 600 Appliance provides cut-through performance, as URL categorization queries are done asynchronously.

• **Identity Awareness**: Gives user and machine visibility across network blades. Enables the creation of identity-based access policies for application and resource control.

• **IPS (More than 2000 protections)**: Best in class integrated IPS with leading performance and unlimited scaling. IPS protections are updated with IPS updates.

• **Anti-spam & Email Security (based on IP Reputation and content)**: Comprehensive and multidimensional protection for organizations’ email infrastructure. This includes updates.

• **Traditional Anti-Virus**: Leading Anti-virus protection using state-of-the-art Anti-virus engine by Kaspersky. The Anti-virus engine runs in stream (network) mode, supporting high performance and concurrency.
• **Advanced Networking and Clustering**: For dynamic routing and Multicast support. Wire speed packet inspection with SecureXL and high availability or load sharing with ClusterXL.

• **QoS**: Quality of Service is a set of intelligent network protocols and services for bandwidth control. These are used to manage the movement of information through local or wide area networks.

**This Getting Started Guide Includes:**

- A brief overview of essential Check Point 600 Appliance concepts and features.
- A step by step guide to getting Check Point 600 Appliance up and running.
About the Appliance

This appliance is a Security Gateway. Its Security Policy is managed by a local web application (WebUI).

After you configure the appliance with the First Time Configuration Wizard, the default Security Policy is enforced automatically. Using the WebUI, you can configure the software blades you activated in the First Time Configuration Wizard and fine tune the Security Policy.
Workflow

The workflow for configuring a locally managed Check Point 600 Appliance is:

1. Set up the Check Point 600 Appliance and connect the cables.
2. Do the initial configuration with the First Time Configuration Wizard.
3. Define a security policy using the WebUI.

Setting up the Check Point 600 Appliance

1. Remove the Check Point 600 Appliance from the shipping carton and place it on a tabletop.
2. Identity the network interface marked as LAN1. This interface is preconfigured with the IP address 192.168.1.1.
Connecting the Cables

1. Connect the power supply unit to the appliance and to a power outlet.
   The appliance is turned on when the power supply unit is connected to an outlet.
   The Power LED on the front panel (on page 56) lights up. This indicates that the appliance is turned on.
   The Notice LED on the front panel starts blinking. This indicates that the appliance is booting up.
   When the Notice LED turns off, the appliance is ready for login.

2. Connect the standard network cable to the LAN1 port on the appliance and to the network adapter on your PC.

3. Connect another standard network cable to the WAN port on the appliance and to the external modem, external router, or network point.
Using the First Time Configuration Wizard

Configure the Check Point 600 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 Check Point 600 Appliance model and the options you select.

Starting the First Time Configuration Wizard

To configure the Check Point 600 Appliance for the first time after you complete the hardware setup, you use the First Time Configuration Wizard.

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

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

After you complete the wizard, you can use the WebUI (Web User Interface) to change settings configured with the First Time Configuration Wizard and to configure advanced settings.
To open the WebUI, enter one of these addresses in the browser:

- http://my.firewall
- http://192.168.1.1

If a security warning message is shown, confirm it and continue. For more details, see Appendix A: Browser Security Warnings (on page 64).

To start the First Time Configuration Wizard:

Initiate a connection from a browser to http://my.firewall and confirm the security message.

The **First Time Configuration Wizard** runs.
Welcome

The Welcome page introduces the product.

To change the language of the WebUI application:
Select the necessary language link at the top of the page.

Note that the First Time Configuration Wizard pages are NOT localized to the specified language and remain in English. Only English is allowed as the input language.
Authentication Details

In the **Authentication Details** page, enter these details necessary for logging in to the Check Point 600 Appliance WebUI application or if the wizard terminates abnormally:

- **Administrator Name** - We recommend that you change the default "admin" login name of the administrator. The name is case sensitive.

- **Password** - You can use the **Password strength** meter to measure the strength of your password. This meter is only used as an indicator and does not enforce creation of a password with a specified number of characters or character combination.
  
The minimum length for a strong password is 6 characters that contain at least one capital letter, one lower case letter and a special character. If you specify such a password, a green bar in the last section of the meter is shown. It is strongly recommended to create a password using both uppercase and lowercase letters.

- **Confirm Password** - Retype the password.

- **Country** - Select a country from the list (for wireless network models).
Appliance Date and Time Settings

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

When you set the time manually, the host computer’s settings are used for the default date and time values. If necessary, change the time zone setting to reflect your correct location. Note that although not specified, Daylight Savings Time is automatically enabled by default. You can change this in the WebUI application on the **Device > Date and Time** page.
When you use the NTP option, there are two default servers you can use. These are ntp.checkpoint.com and ntp2.checkpoint.com.

Appliance Name

In the **Appliance Name** page, enter a name for the appliance that is used to identify the Check Point 600 Appliance and a domain name.

- **Appliance name** - Enter a name for the appliance.
- **Domain name** - When the gateway performs DNS resolving for a certain object's name, the domain name is appended to the object name. This enables hosts in the network to lookup hosts by using only their internal names. This field is not mandatory.
Internet Connection

In the Internet Connection page, configure your Internet connectivity details or select the Configure Internet connection later option and then configure connectivity through the WebUI application at a later time.
To configure Internet connection now:

1. Select **Configure Internet connection now**.
2. From the **Connection Protocol** drop down list, select the protocol used for connecting to the Internet.
3. Fill in 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 in plain Metro Ethernet networks.
   - **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing 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 by itself. It relies on an encryption protocol that it passes within the tunnel to provide privacy.
   - **Cellular Modem** - Connect to the Internet using a wireless modem to a cellular ISP through the USB port or Express Card slot.
• **Analog Modem** - Connect to the Internet using an analog modem through a USB port. In the WebUI application, you can configure to use an analog modem through the serial port.

• **ADSL** - Connect to the Internet using ADSL protocols PPPoE, PPPoA, EoA, or IPoA.

• **Bridge** - Connects multiple network segments at the data link layer (Layer 2).

4. In the **DNS Server** field (shown for Static IP and Bridge connections), enter the DNS server address information in the relevant fields. For DHCP, PPPoE, PPTP, L2TP, ADSL, Analog Modem, and Cellular Modem, the DNS settings are supplied by your service provider. You can override these settings later in the WebUI application under the Device > DNS page.

   It is recommended to configure the DNS since Check Point 600 Appliance needs to perform DNS resolving for different functions. For example, for connecting to Check Point User Center during license activation or when Application Control, Web Filtering, Anti-Virus or Anti-Spam services are enabled.

5. Click **Connect** to connect to your ISP now and test your connection's status.

Indication regarding success or failure of the connection appears at the bottom of the page.
To configure the Internet connection at a later time:
Select **Configure Internet connection later**.

![Check Point 600 Appliance Wizard Internet Connection](image)

**Local Network**

In the **Local Network** page, select whether 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.

DHCP is enabled by default and a default range is configured. Make sure to set the range accordingly and be careful not to include predefined static IPs in your network. Set the exclusion range for IP addresses that should not be defined by the DHCP server.
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 will exclude 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 Wireless Network Models)

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 wireless network 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. **Allow access from this network to the local network (Wireless network is trusted)** is selected by default. Clear if it is not necessary. Selecting this option makes the wireless network part of the local network. The wireless network is considered in this case trusted and access by default is allowed from it to the local network.

6. Click Hide to conceal the password.
To configure the wireless network at a different time:

Select **Configure wireless network later**.
Administrator Access

In the Administrator Access page, configure if administrators can use Check Point 600 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** - Wireless networks that are allowed access to the LAN by default. This field is only shown in wireless network modes.
   - **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 Check Point 600 Appliance:
   - **Any IP address**
   - **Specified IP addresses only**
   - **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.
3. To specify IP addresses, click **New**.

   a) 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**.

   b) 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.

In most cases, you must first register the appliance in your Check Point User Center account. If you don’t already have an account, you must create one. A User Center account is necessary to receive support and updates for service blades, for example IPS and Anti-Virus.

If you have Internet connectivity configured:

The First Time Configuration Wizard tries to connect to the Check Point User Center and activate the appliance.

If the appliance is successfully activated, the wizard shows the Software Blades Activation page.

If the appliance fails to get activated, read the notifications on the page and click **Activate License**.

If the appliance has not been registered, choose one of these registration options to register the appliance in the User Center.
1. If you have a Check Point User Center account, select **Already have a User Center account** and do these steps:
   a) Click **Next**.
   b) Enter your **Email** and **Password**. If you forgot your password, click the **forgot your password** link and follow the instructions. Upon successful registration, the appliance is listed under the SMB Gateways account attached to your user account.

2. If you must create a new user account, select **Create a new User Center account** and do these steps:
   a) Click **Next**.
   b) Enter the information for a new account: **First name**, **Last name**, **Email**, **Confirm email** and **Company**. Note that the Company name will be used as the Account name to which the appliance is associated.
3. If you want to use a trial license, select **Register later (30 day trial license will be used)**.

4. Click **Next**.

   The Software Blades Activation page shows you the status of your license for each blade.

   **Note** - If the wizard was not successful in registering the appliance for an existing or new User Center account, when you click Next in step 4 a trial license is automatically issued.

   To register the appliance after you complete the First Time Configuration Wizard, go to the WebUI **Home > License page**.

---

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

1. Register the appliance by browsing to http://smbregistration.checkpoint.com and filling out the requested information. You will have to enter the appliance’s credentials, MAC address and registration key. This information can be found on the Appliance Registration page.

2. After you complete the registration wizard, you will be prompted to download the activation file. Download it to a local location. This is necessary for the next step.

3. In the Appliance Registration page, click **Offline**. The Import from File window opens.

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

   You will be notified that you successfully activated the appliance. The next page will show you 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 from the WebUI Home > License page at a later time.
Locally Managed - Software Blades Activation

Select the software blades to activate on this Check Point 600 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.

**Note** - You should back up the system configuration in the WebUI. Go to the **Device > System Operations > Backup** page.
Check Point 600 Appliance Hardware

In This Section:

Front Panel .................................................................56
Back Panel ....................................................................58

These are the Check Point 600 Appliance models:

• Wired
• Wireless Network
• Wireless Network + ADSL

The differences in the front and back panels are described in this section.
Front Panel

Wireless Network + ADSL Model

<table>
<thead>
<tr>
<th>Key</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Express Card</td>
<td>Express card slot that is used for cellular modems in Express Card form factor.</td>
</tr>
<tr>
<td>2</td>
<td>USB1 port</td>
<td>USB1 port that is used for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cellular and analog modems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reinstalling the appliance with new firmware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Running a first-time configuration script.</td>
</tr>
<tr>
<td>3</td>
<td>Power LED</td>
<td>Green when the appliance is turned on.</td>
</tr>
<tr>
<td>4</td>
<td>Notice LED</td>
<td>• Blinking green during boot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Red when the appliance has a resource problem such as memory shortage.</td>
</tr>
<tr>
<td>Key</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 5   | LAN1 - LAN8, DMZ, WAN LEDs | **Link Indicator**  
• Orange when the port speed is 1000 Mbps.  
• Green when the port speed is 100 Mbps.  
• Not lit when the port speed is 10 Mbps.  
**Activity Indicator**  
• Blinking green when encountering traffic. |
|     | DSL LED | **Link Indicator**  
• Green when an ADSL connection is established.  
• Blinking green when establishing an ADSL connection.  
• Not lit when an ADSL connection is not established.  
**Activity Indicator**  
• Blinking green when encountering traffic.  
• Not lit when the ADSL line is idle. |
|     | Internet LED | **Link Indicator**  
• Green when connected to the Internet.  
• Blinking red when the Internet connection is configured but fails to connect.  
**Activity Indicator**  
• Blinking green when encountering traffic. |
|     | WLAN LED | Blinking green when encountering traffic.  
(Only in Wireless Network and Wireless Network + ADSL models) |
|     | USB1, USB2 LEDs | Orange when a USB device is connected. |
## Back Panel

### Wireless Network + ADSL Model

![Back Panel Diagram](image)

<table>
<thead>
<tr>
<th>Key</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANT1 and ANT2</td>
<td>Ports for attaching wireless network antennas. (Only in Wireless Network and Wireless Network + ADSL models)</td>
</tr>
<tr>
<td>2</td>
<td>Power outlet</td>
<td>Connects to the power supply unit’s cable.</td>
</tr>
<tr>
<td>3</td>
<td>Reboot button</td>
<td>Lets you forcibly reboot the appliance. The button is recessed into the appliance chassis to prevent accidental reboot. The appliance reboots immediately after you press the button.</td>
</tr>
<tr>
<td>4</td>
<td>LAN1 - LAN8 ports</td>
<td>Built in Ethernet ports.</td>
</tr>
<tr>
<td>Key</td>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LAN2/SYNC port</td>
<td>In a cluster configuration, you must connect a cable between this port on both appliances that take part in the cluster. You can configure the cluster sync port to a port other than LAN2.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>DMZ and WAN ports</td>
<td>Built in Ethernet ports.</td>
</tr>
<tr>
<td>6</td>
<td>USB2 port</td>
<td>Second USB port. Same functionality as the USB1 port on the Front Panel.</td>
</tr>
<tr>
<td>7</td>
<td>Console port</td>
<td>Serial connection configured to 115200 bps by default. You can also use this port to connect an analog modem.</td>
</tr>
<tr>
<td>8</td>
<td>Factory Defaults button</td>
<td>Lets you restore the appliance to its factory defaults. The button is recessed into the appliance chassis to prevent accidental restoring of factory default settings. See Restoring Factory Defaults (on page 60).</td>
</tr>
<tr>
<td>9</td>
<td>ADSL port</td>
<td>Port for attaching ADSL cable. (Only in Wireless Network + ADSL model)</td>
</tr>
</tbody>
</table>
Restoring Factory Defaults

The Check Point 600 Appliance contains a default factory image.

When the appliance is turned on for the first time, it loads with the default image.

As part of a troubleshooting process, you can restore the Check Point 600 Appliance to its factory default settings if necessary.

You can restore a Check Point 600 Appliance to the factory default image with the WebUI, Boot Loader, or a button on the back panel.

**Important** - When you restore factory defaults, you delete all information on the appliance and it is necessary to run the First Time Configuration Wizard.

To restore factory defaults with the WebUI:

1. In the Check Point 600 Appliance WebUI, click **Device > System Operations**. The System Operations pane opens.
2. In the Appliance section, click **Factory Defaults**.
3. In the pop-up window that opens, click **OK**.
4. While factory defaults are being restored, all LAN Link and Activity LEDs blink orange and green alternately to show progress.
   This takes some minutes. When this completes, the appliance reboots automatically.
To restore factory defaults with the button on the back panel:

1. Press the Factory Default button with a pin and hold it for at least 3 seconds.
2. When the Power and Notice LEDs are lit red, release the button. The appliance reboots itself and starts to restore factory defaults immediately.
3. While factory defaults are being restored, all LAN Link and Activity LEDs blink orange and green alternately to show progress.
   This takes some few minutes. When this completes, the appliance reboots automatically.

To restore the Check Point 600 Appliance to its default factory configuration using U-boot (boot loader):

1. Connect to the appliance with a console connection (using the serial console connection on the back panel of the appliance).
2. Boot the appliance and press Ctrl-C.
   The Gaia Embedded Boot Menu is shown.
   Welcome to Gaia Embedded Boot Menu:
   1. Start in normal Mode
   2. Start in debug Mode
   3. Start in maintenance Mode
   4. Restore to Factory Defaults (local)
   5. Install/Update Image/Boot-Loader from Network
   6. Install/Update Image from USB
   7. Install/Update Boot-Loader from USB
8. Restart Boot-Loader
Please enter your selection:

3. Enter 4 to select **Restore to Factory Defaults (local).**

4. When you are prompted: "Are you sure? (y/n)" select **y** to continue and restore the appliance to its factory defaults settings.

While factory defaults are being restored, all LAN Link and Activity LEDs will blink orange and green alternately to indicate progress. This will take up to a few minutes. Upon completion, the appliance will boot automatically.
Getting Support

Support

For more technical information about Check Point products, consult the Check Point Support Center at:

http://support.checkpoint.com
(http://supportcenter.checkpoint.com)

Where To From Here?

You have now learned the basics that are necessary to get started.

For more information about the Check Point 600 Appliance and links to the administration guides, see the Check Point site (http://www.checkpoint.com/cp600).

Be sure to also use our Online Help when you operate the Check Point 600 Appliance WebUI and with Check Point SmartConsole clients.
Appendix A: Browser Security Warnings

When you log in to the appliance from the Internet Explorer, Mozilla FireFox, or Google Chrome browser you might see a security warning.

You can safely confirm the warning and continue to log in as usual.

Mozilla FireFox

1. Click **I understand the Risks**.
2. Click **Add Exception**. The Add Security Exception dialog box opens.
3. Click **Confirm Security Exception**.
Internet Explorer

Click Continue to this website (not recommended).

Google Chrome

Click Advanced and then click the Proceed to 192.168.1.1 link that is shown.