Check Point®
SOFTWARE TECHNOLOGIES LTD.

# Check Point 1430/1450 Appliance

## Centrally Managed Getting Started Guide

***Models: L-71, L-71W, L-71WD***

***Classification: [Protected]  P/N 707410***

## Latest Documentation

The latest version of this document is at:
http://downloads.checkpoint.com/dc/download.htm?ID=46106

To learn more, visit the Check Point Support Center
http://supportcenter.checkpoint.com.

## 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 1430/1450 Appliance Centrally 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.

## Power Supply Information

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

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

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

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

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

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

## 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 Ha'Solelim Street, Tel Aviv 67897, Israel |

Declares under our sole responsibility, that the products:

| | |
|---|---|
| **Model Number:** | L-71, *L-71W , **L-71WD |
| **Product Options:** | 1430 Wired, 1430 WiFi, 1430 WiFi + DSL, 1450 Wired, 1450 WiFi, 1450 WiFi + DSL |
| **Date First Applied:** | January 2016 |

Conform to the following Product Specifications:

RF/Wi-Fi (* marked model)

Telecom (** marked model)

| Certification | Type |
| --- | --- |
| EN 55032:2015 + AC:2016, Class B | EMC, |
| EN 55032:2012 + AC:2013, Class B | *RF/WiFi, **Telecom |
| EN 55024:2010 / A1:2015 | |
| EN 55024:2010 | |
| EN61000-3-2:2014 | |
| EN61000-3-3:2013 | |
| EN61000-4-2:2009 | |
| EN61000-4-3:2006+A1:2008+A2:2010 | |
| EN61000-4-4:2012 | |
| EN61000-4-5:2014 | |
| EN61000-4-6:2014 | |
| EN61000-4-11:2004 | |
| *EN 300 328 V2.1.1 (2016-11) | |
| *EN 301 893 V2.1.1 (2017-05) | |
| *EN 301 489-1 V2.1.1 (2017-02) | |
| *EN 301 489-17 V3.1.1 (2017-02) | |
| *EN 62311:2008 (SAR) | |
| *EN 50386:2002, EN50383:2010 (SAR) | |
| **ITU-T K.21 (04-2008) | |

| Certification | Type |
| --- | --- |
| AS/NZS CISPR 32:2015, Class B | EMC, |
| AS/NZS CISPR 32:2013, Class B | *RF, **Telecom |
| * AS/NZS 4268:2017 | |
| * ARPANSA Radiation Protection Standard No.3:2002AS/NZS 2772.2:2011 (SAR) | |
| **AS/CA S041.1-2015 & AS/CA S041.2-2015 | |
| **AS/CA S043.1:2015 / AS/CA S043.2:2015 | |

| Certification | Type |
| --- | --- |
| 47 CRF FCC Part 15, Subpart B, Class B | EMC, |
| ANSI C63.4:2009 | *RF, **Telecom |
| ANSI C63.4:2014 | |
| ICES-003:2012 Issue 5 Class B | |
| ICES-003:2016 Issue 6, Class B | |
| *47 CFR FCC Part15, Subpart C | |
| (section 15.247) ANSI C63.10:2013 | |
| *FCC Part 15, Subpart E (Section 15.407) | |
| *KDB 905462 D02 UNII DFS Compliance Procedures New Rules v02 | |
| *FCC Part 2 (Section 2.1091) | |
| KDB 447498 D01 | |
| *RSS-247 Issue 1(1015-05) | |
| *RSS-247 Issue 2 (2017-02) | |
| *RSS-Gen Issue 4 (2014-11) | |
| *RSS-102 Issue 5:2015 | |
| *IEEE C95.3-2002 | |
| *FCC KDB 447498 D01 | |
| **FCC Part 68, ANSI/TIA-968-B-3-2016 | |
| **CS-03 Part I Issue 9, Amendment 5, March 2016 | |
| **CS-03, Part VIII, Issue 9, Amendment 5, March 2016 | |

| Certification | Type |
| --- | --- |
| VCCI, V-3/2015.4 Class B, V4/2012.04<br>VCCI-CISPR 32:2016, Class B<br>JP ARIB STD-T66 (V3.7), MIC notice 88 Appendix 43<br>JP ARIB STD-T71 (V6.1), MIC notice 88 Appendix 45 | EMC,<br>*RF |
| EN 60950-1<br>IEC 60950-1<br>UL/ULc 60950-1,<br>AS/NZS 60950-1 | Safety |

Date and Place of Issue: January 2016, Tel Aviv, Israel

## Federal Communications Commission (FCC) Statement:

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful

interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

### FCC Caution:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

### 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.

## For Country Code Selection Usage (WLAN Devices)

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

## Canadian Department Compliance Statement

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

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

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

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

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

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

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

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

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

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

**FOR WLAN 5 GHz DEVICE:**

Caution :

1. The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
2. The maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and
3. The maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.
4. The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) shall be clearly indicated. (For 5G B2 with DFS devices only)
5. Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

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

## Japan Class B Compliance Statement:

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい

VCCI-B

## European Union (EU) Electromagnetic Compatibility Directive

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

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

## Product Disposal

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

# Informations relatives à la santé et à la sécurité (Class B)



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

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

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

## Information pour l'alimentation

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

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

Pour éviter d'endommager tout système, il est important de manipuler les éléments avec soin. Ces mesures sont

généralement suffisantes pour protéger votre équipement contre les décharges d'électricité statique :

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

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

- Ne pas jeter les piles au feu ni avec les déchets ménagers.
- Pour connaître l'adresse du lieu le plus proche de dépôt des piles, contactez votre service local de gestion des déchets.
- Débrancher l'alimentation de la carte système de sa source électrique avant de connecter ou déconnecter des câbles ou d'installer ou retirer des composants. À défaut, les risques sont d'endommager l'équipement et de causer des blessures corporelles.
- Ne pas court-circuiter la pile au lithium : elle risque de surchauffer et de causer des brûlures en cas de contact.

- Ne pas faire fonctionner le processeur sans refroidissement. Le processeur peut être endommagé en quelques secondes.

## 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 Ha'Solelim Street, Tel Aviv 67897, Israël |

Déclare sous son entière responsabilité que les produits :

| | |
|---|---|
| Numéro de modèle : | L-71, *L-71W , **L-71WD |
| Options de produit : | 1430, 1430 Wi-Fi, 1430 Wi-Fi + DSL, 1450, 1450 Wi-Fi, 1450 Wi-Fi + DSL |
| Date de demande initiale : | Janvier 2016 |

Sont conformes aux normes produit suivantes :

RF/Wi-Fi (modèle signalé par *)

Telecom ((modèle signalé par **)

| Certification | Type |
| --- | --- |
| EN 55032:2015 + AC:2016, Classe B | EMC, |
| EN 55032:2012 + AC:2013, Classe B | *RF/WiFi, |
| EN 55024:2010 / A1:2015 | **Telecom |
| EN 55024:2010 | |
| EN61000-3-2:2014 | |
| EN61000-3-3:2013 | |
| EN61000-4-2:2009 | |
| EN61000-4-3:2006+A1:2008+A2:2010 | |
| EN61000-4-4:2012 | |
| EN61000-4-5:2014 | |
| EN61000-4-6:2014 | |
| EN61000-4-11:2004 | |
| *EN 300 328 V2.1.1 (2016-11) | |
| *EN 301 893 V2.1.1 (2017-05) | |
| *EN 301 489-1 V2.1.1 (2017-02) | |
| *EN 301 489-17 V3.1.1 (2017-02) | |
| *EN 62311:2008 (SAR) | |
| *EN 50386:2002, EN50383:2010 (SAR) | |
| **ITU-T K.21 (04-2008) | |

| Certification | Type |
| --- | --- |
| AS/NZS CISPR 32:2015, Classe B | EMC, |
| AS/NZS CISPR 32:2013, Classe B | *RF, |
| * AS/NZS 4268:2017 | **Telecom |
| * ARPANSA Radiation Protection Standard No.3:2002AS/NZS 2772.2:2011 (SAR) | |
| **AS/CA S041.1-2015 & AS/CA S041.2-2015 | |
| **AS/CA S043.1:2015 / AS/CA S043.2:2015 | |

| Certification | Type |
| --- | --- |
| 47 CRF FCC Partie 15, Sous-partie B, Classe B | EMC, |
| ANSI C63.4:2009 | *RF, **Telecom |
| ANSI C63.4:2014 | |
| ICES-003:2012 Issue 5 Classe B | |
| ICES-003:2016 Issue 6, Classe B | |
| *47 CFR FCC Partie15, Sous-partie C (section 15.247) ANSI C63.10:2013 | |
| *FCC Partie 15, Sous-partie E (Section 15.407) | |
| *KDB 905462 D02 UNII DFS Procédure de conformité Nouvelles règles v02 | |
| *FCC Partie 2 (Section 2.1091) | |
| KDB 447498 D01 | |
| *RSS-247 Issue 1(1015-05) | |
| *RSS-247 Issue 2 (2017-02) | |
| *RSS-Gen Issue 4 (2014-11) | |
| *RSS-102 Issue 5:2015 | |
| *IEEE C95.3-2002 | |
| *FCC KDB 447498 D01 | |
| **FCC Part 68, ANSI/TIA-968-B-3-2016 | |
| **CS-03 Partie I Issue 9, Amendement 5, Mars 2016 | |
| **CS-03, Partie VIII, Issue 9, Amendement 5, Mars 2016 | |

| Certification | Type |
|---|---|
| VCCI, V-3/2015.4 Classe B, V4/2012.04<br>VCCI-CISPR 32:2016, Classe B<br>JP ARIB STD-T66 (V3.7), avis MIC 88 Annexe 43<br>JP ARIB STD-T71 (V6.1), avis MIC 88 Annexe 45 | EMC,<br>*RF |
| EN 60950-1<br>IEC 60950-1<br>UL/ULc 60950-1,<br>AS/NZS 60950-1 | Sécurité |

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

**Déclaration à la Federal Communications Commission (FCC) :**

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 équipement a été testé et déclaré conforme aux limites pour appareils numériques de classe B, selon la section 15 des règlements de la FCC. Ces limitations sont conçues pour fournir une protection raisonnable contre les interférences nocives dans un environnement résidentiel. Cet appareil génère, et peut diffuser des fréquences radio et, dans le cas d'une installation et d'une utilisation non conforme aux instructions, il peut provoquer des interférences nuisibles aux

communications radio. Cependant, il n'existe aucune garantie qu'aucune interférence ne se produira dans le cadre d'une installation particulière. Si cet appareil provoque des interférences avec un récepteur radio ou un téléviseur, ce qui peut être détecté en mettant l'appareil sous et hors tension, l'utilisateur peut essayer d'éliminer les interférences en suivant au moins l'une des procédures suivantes :

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

## FCC Attention

- Tout changement ou modification non expressément approuvé par la partie responsable de la conformité pourrait empêcher l'utilisateur autorisé de faire fonctionner cet appareil.
- Cet émetteur ne doit pas être installé ou utilisé en conjonction avec d'autres antennes ou émetteurs.

## 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.

## Concernant la sélection du code pays (appareils WLAN)

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

**Déclaration de conformité du département Canadien :**

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

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

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

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

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

**POUR WLAN 5 GHz DISPOSITIF:**

Avertissement:

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

## 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

## Directive de l'Union européenne relative à la compatibilité électromagnétique

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

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

## Mise au rebut du produit

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

# Contents

# Introduction

Review these documents before doing the procedures in this guide:

- Release Notes
- Known Limitations

For more information about the Check Point 1430/1450 Appliance, see the relevant *Check Point Appliance Administration Guide.*

## Welcome

Thank you for choosing Check Point's Internet Security Product Suite. Check Point 1430/1450 Appliance delivers integrated unified threat management to protect your organization from today's emerging threats.

Check Point 1430/1450 Appliance supports the Check Point Software Blade architecture and provides independent, modular, and centrally managed security building blocks.

Check Point 1430/1450 Appliance runs an embedded version of the Gaia operating system. Embedded Gaia supports built-in network switches, wireless networks, 4G/LTE Internet connectivity, multiple Internet connections (more than 2) in High Availability or Load Sharing mode, Policy Based Routing, DDNS support, and quick deployment (with USB).

# Shipping Carton Contents

| Item | Description |
|---|---|
| Appliance | A single Check Point 1430/1450 Appliance |
| Power Supply and Accessories | • 1 power adapter<br>• 1 power cord<br>• 2 standard network cables<br>• 1 serial console cable<br>• 1 mini USB console cable<br>• Wall mount kit (screws and plastic anchors)<br>• 1 telephone cable (only in DSL models) |
| Guides | • *Check Point 1430/1450 Appliance Quick Start Guide*<br>• *Check Point 1430/1450 Appliance Getting Started Guide* |
| Wireless Network Antennas | 3 wireless network antennas (only in wireless network models) |
| Sticker | LEDs behavior |
| License Agreement | End user license agreement |

# Check Point 1430/1450 Appliance Hardware

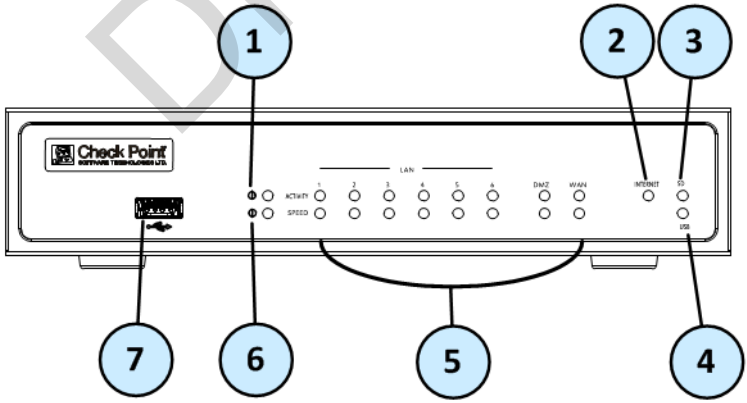
These are the Check Point 1430/1450 Appliance models:

- Wired
- Wireless (WiFi)
- Wireless + DSL

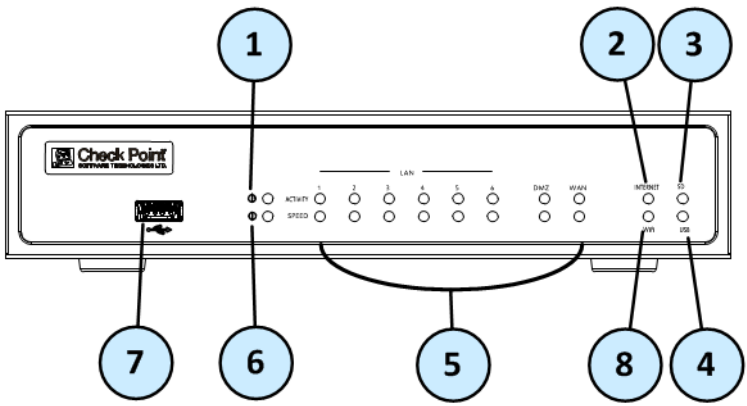
The differences in the front and back panels are described in this section.

# Front Panel

## Wired Model

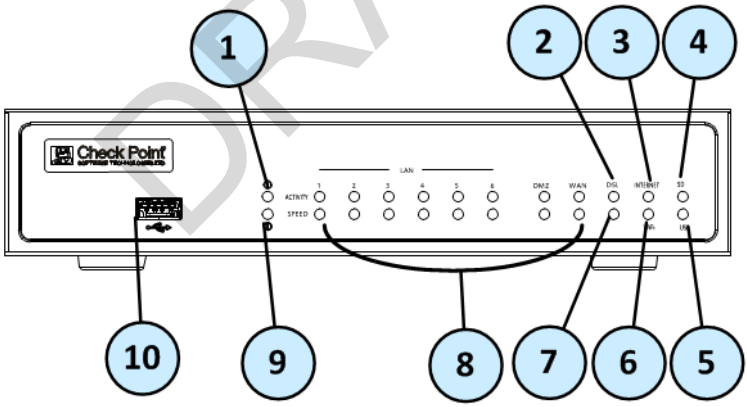



## WiFi Model



| Key | Item | Description |
|---|---|---|
| 1 | Alert LED | • Blinking green during boot.<br>• Red when the appliance has a resource problem such as memory shortage. |
| 2 | Internet LED | • Green when connected to the Internet.<br>• Blinking red when the Internet connection is configured but fails to connect. |
| 3 | SD LED | Green when SD card is inserted. |
| 4 | USB LED | Green when a USB device is connected. |
| 5 | LAN1 - LAN6, DMZ, WAN LEDS | Speed Indicator<br>• Orange when the port speed is 1000 Mbps.<br>• Green when the port speed is 100 Mbps.<br>• Not lit when the port speed is 10 Mbps.<br>Activity Indicator<br>• Not lit when there is no link.<br>• Green when there is a link but no traffic encountered.<br>• Blinking green when encountering traffic. |
| 6 | Power LED | • Green when the appliance is turned on.<br>• Red when there is a boot error or the appliance is in maintenance mode. |
| 7 | USB port | USB port that is used for:<br>• Cellular and analog modems.<br>• Reinstalling the appliance with new firmware.<br>• Running a first-time configuration script. |
| 8 | WiFi LED | (Only in WiFi and WiFi + VDSL models).<br>• Blinking green when there is WiFi activity.<br>• Green when there is no WiFi activity. |

## WiFi + DSL

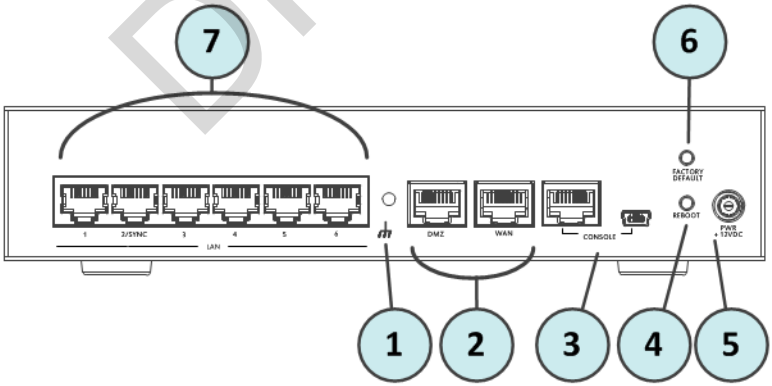



| Key | Item | Description |
|---|---|---|
| 1 | Alert LED | • Blinking green during boot.<br>• Red when the appliance has a resource problem such as memory shortage. |
| 2 | DSL LED | • Off – DSL Modem is off.<br>• Blinking green - DSL modem is performing synchronization.<br>• Steady green – DSL is synchronized. |
| 3 | Internet LED | • Off – DSL Modem is off.<br>• Blinking green - DSL modem is performing synchronization.<br>• Steady green – DSL is synchronized. |
| 4 | SD LED | Green when SD card is inserted. |
| 5 | USB LED | Green when a USB device is connected. |

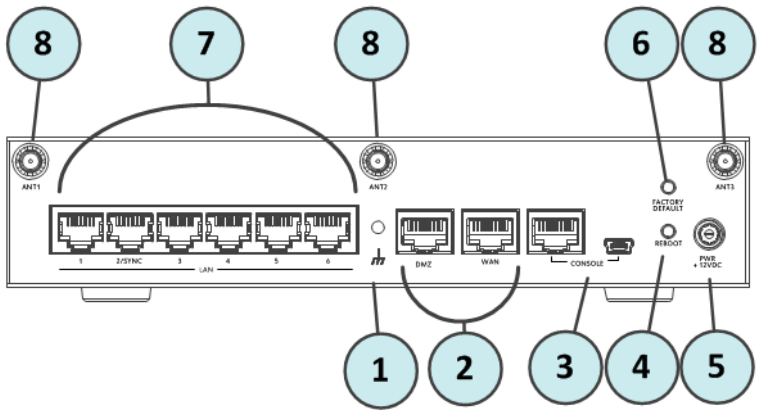
| Key | Item | Description |
|---|---|---|
| 6 | WiFi LED | (Only in WiFi and WiFi + DSL models).<br>• Blinking green when there is WiFi activity.<br>• Green when there is no WiFi activity. |
| 7 | DSL Traffic LED | • Off - DSL connection has not been established.<br>• Blinking Green - DSL connection is established. The blinking rate is proportional to the internet traffic rate. |
| 8 | LAN1 - LAN6, DMZ, WAN LEDS | Speed Indicator<br>• Orange when the port speed is 1000 Mbps.<br>• Green when the port speed is 100 Mbps.<br>• Not lit when the port speed is 10 Mbps.<br>Activity Indicator<br>• Not lit when there is no link.<br>• Green when there is a link but no traffic encountered.<br>• Blinking green when encountering traffic. |
| 9 | Power LED | • Green when the appliance is turned on.<br>• Red when there is a boot error or the appliance is in maintenance mode. |
| 10 | USB port | USB port that is used for:<br>• Cellular and analog modems.<br>• Reinstalling the appliance with new firmware.<br>• Running a first-time configuration script. |

# Back Panel

## Wired Model



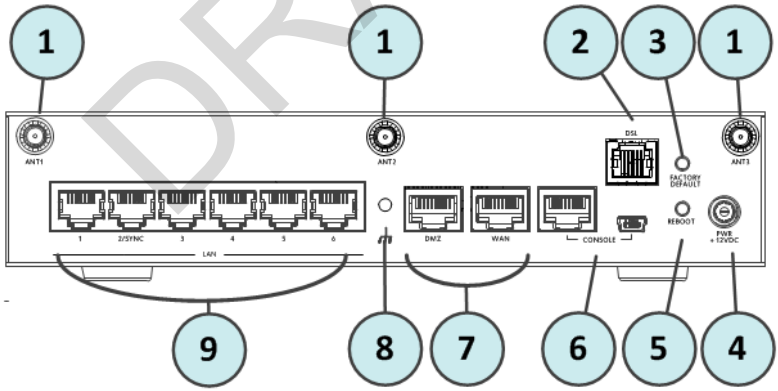

## WiFi Model



| Key | Item | Description |
|---|---|---|
| 1 | Ground (Earth) | Functional grounding. |
| 2 | DMZ and WAN ports | Built in Ethernet ports. |
| 3 | Console port | RJ45 or Mini USB Serial connection configured to 115200 bps by default. **Note** - When both the RJ45 and Mini USB cables are connected, the Mini USB takes precedence. |
| 4 | Reboot button | Lets you forcibly reboot the appliance. The button is recessed into the appliance chassis to prevent accidental reboot. The appliance reboots after you press the button. |
| 5 | PWR+12VDC | Connects to the power supply unit's cable. **Note -** The power unit cable must be securely screwed in to the appliance. |
| 6 | Factory Default button | 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 81). |

| Key | Item | Description |
|---|---|---|
| 7 | LAN1-LAN6 ports | Built in Ethernet ports. |
| 8 | ANT1, ANT2 and ANT3 | Ports for attaching wireless network antennas. (Only in WiFi and WiFi + VDSL models). |

## WiFi + DSL




| Key | Item | Description |
|---|---|---|
| 1 | ANT1, ANT2 and ANT3 | Ports for attaching wireless network antennas. (Only in WiFi and WiFi + DSL models). |
| 2 | DSL | Port for attaching telephone cable (only in WiFi + DSL models). |
| 3 | Factory Default button | 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 81). |

| Key | Item | Description |
|---|---|---|
| 4 | PWR+12VDC | Connects to the power supply unit's cable. **Note -** The power unit cable must be securely screwed in to the appliance. |
| 5 | Reboot button | Lets you forcibly reboot the appliance. The button is recessed into the appliance chassis to prevent accidental reboot. The appliance reboots after you press the button. |
| 6 | Console port | RJ45 or Mini USB Serial connection configured to 115200 bps by default. You can also use this port to connect an analog modem. **Note** - When both the RJ45 and Mini USB cables are connected, the Mini USB takes precedence. |
| 7 | DMZ and WAN ports | Built in Ethernet ports. |
| 8 | Ground (Earth) | Functional grounding. |
| 9 | LAN1 - LAN6 ports | Built in Ethernet ports. |

# Security Gateway Software Blades

Check Point 1430/1450 Appliance has these Software Blades:

- **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 -** Sophisticated (but simple to manage) Site-to-Site VPN and flexible Remote Access working seamlessly with a variety of VPN agents.
- **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 1430/1450 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.

- **Anti-virus -** Provides superior Anti-virus protection against modern malware multiple attack vectors and threats. It offers powerful security coverage by supporting millions of signatures. In addition, it leverages the Check Point ThreatCloud repository to identify and block incoming malicious files from entering the organization.
- **Anti-Bot** - Detects bot-infected machines and prevents bot damages by blocking bot Command and Control (C&C) communications.
- **Threat Emulation** - Protects networks against unknown threats in files that are downloaded from the internet or attached to emails.
- **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 optimizes network performance by prioritizing business-critical applications and end-user traffic. It guarantees bandwidth and control latency for streaming applications, such as VoIP and video conferencing.

# Configuring Check Point 1430/1450 Appliance

The appliance is a Security Gateway. A remote Security Management Server manages the Security Gateway in SmartDashboard with a network object and security policy. We recommend that you define a gateway object and prepare the policy before you configure the appliance with the First Time Configuration Wizard.

## Recommended Workflow

There are two types of centrally managed deployments:

**Small-scale deployment** - Where you configure between 1 and 25 Check Point 1430/1450 Appliance gateways.

**Large-scale deployment** - Where you configure over 25 Check Point 1430/1450 Appliance gateways using a SmartLSM profile and SmartProvisioning.

In small-scale deployment, you configure multiple Check Point 1430/1450 Appliance gateways.

1. Install a Security Management Server and SmartConsole client that operate with Check Point 1430/1450 Appliance.
2. Define the Check Point 1430/1450 Appliance object in SmartDashboard and prepare a policy for it.
3. Set up the Check Point 1430/1450 Appliance and connect the cables.

4. Use the First Time Configuration Wizard to do the initial Check Point 1430/1450 Appliance configuration.
5. Optional: You can manage settings such as DNS, host names, and routing through SmartProvisioning. For more information, see the SmartProvisioning section in the appliance *Administration Guide*.

To define a large-scale deployment (on page 79) (recommended workflow:

1. Install a Security Management Server and SmartConsole clients that operate with Check Point 1430/1450 Appliance.

2. Define a SmartLSM profile in SmartDashboard.

3. Deploy with SmartProvisioning.

# Deployment

To manage the Check Point 1430/1450 Appliance in a centrally managed deployment, you must install a Security Management Server and SmartConsole clients that operate with Check Point 1430/1450 Appliance.

The Security Management Server versions that operate with Check Point 1430/1450 Appliance are versions R77.30 and higher.

For installation instructions, see the version's release notes.

After you install the SmartConsole clients you can define the Check Point 1430/1450 Appliance object in SmartDashboard (in small-scale deployments) or create a SmartLSM profile (in large-scale deployments) and prepare the security policy.

## Defining the Object in SmartDashboard

You can define the Check Point 1430/1450 Appliance in SmartDashboard before or after configuration of the appliance on site. The options are:

- **Management First** - The gateway object is defined in SmartDashboard before you configure and set up the actual appliance on site. This is used for remotely deployed appliances or appliances that connect to the Security Management Server with a dynamic IP, as the IP is not known at the time of the configuration of the object in SmartDashboard. You can prepare a policy that the appliance will fetch when it is configured.

- **Gateway First** – You first configure and set up the Check Point 1430/1450 Appliance. It will then try to communicate with the Security Management Server (if this is configured) at one hour intervals. If the gateway is connected when you create the object in SmartDashboard, the wizard retrieves data from the gateway and helps in configuration.

  **Note** - We recommend that you use the Management First option using the steps below.

To define the Check Point 1430/1450 Appliance object:

1. Log in to SmartDashboard with your Security Management credentials.
2. From the Network Objects tree, right click **Check Point** and select **Security Gateway/Management**.

   The Check Point Security Gateway Creation window opens.
3. Select **Wizard Mode**.

   The wizard opens to General Properties.
4. Enter a name for the Check Point 1430/1450 Appliance object and select the hardware type for the hardware platform.

   If the Check Point 1430/1450 Appliance does not appear in the hardware list in the R77.30 SmartDashboard, refer to sk111292 http://supportcontent.checkpoint.com/solutions?id=sk111292.
5. Set the Security Gateway **Version** to R77.20.
6. Select **Static IP address** or **Dynamic IP address** to get the gateway's IP address.
7. Click **Next**.

To configure a static IP address:

1. In the Authentication section, select **Initiate trusted communication securely by using a one-time password** or **Initiate trusted communication without authentication (less secure)**.
2. If you selected **Initiate trusted communication securely by using a one-time password,** enter a **one-time password** and confirm it. This password is only used to establish the initial trust. Once established, trust is based on security certificates.

   **Important** - This password must be identical to the one-time password you define for the appliance in the First Time Configuration Wizard.

3. In the Trusted Communication section, select **Initiate trusted communication automatically when the Gateway connects to the Security Management server for the first time** or **Initiate trusted communication now.**
4. Click **Connect**.

   A status window appears.
5. Click **Next**.

To configure a dynamic IP address:

1. In the Gateway Identifier section, select one identifier: **Gateway name**, **MAC address** or **First to connect**.
2. In the Authentication section, select **Initiate trusted communication securely by using a one-time password** or **Initiate trusted communication without authentication (less secure).**
3. If you select **Initiate trusted communication securely by using a one-time password**, enter a **one-time password**

and confirm it. This password is only used for establishing the initial trust. Once established, trust is based on security certificates.

**Important** - This password must be identical to the one-time password you define for the appliance in the First Time Configuration Wizard.

4. Click **Next**.

### To configure the software blades:

In the Blade Activation page, select the software blades that you want to activate and configure.

### To configure blades later:

1. Select **Activate and configure software blades later**.
2. Click **Next**.

### To configure blades now:

1. Select **Activate and configure software blades now**.
2. Select the check boxes next to the blades you want to activate and configure.
3. Configure the required options:
   - **NAT -** the **Hide internal networks behind the Gateway's external IP** checkbox is selected by default.
   - **QoS -** Set the inbound and outbound bandwidth rates.
   - **IPSec VPN -** Make sure that the VPN community has been predefined. If it is a star community, Check Point 1430/1450 Appliance is added as a satellite gateway. Select a VPN community that the Gateway participates in from the **Participate in a site to site community** list.

- **IPS** - Select a profile from the **Assign IPS Profile** list or click **Manage** to create/edit an IPS profile.
- **Identity Awareness -** Complete the wizard pages that open to define the Identity Awareness acquisition sources. In the Active Directory Servers page of the wizard, make sure to select only AD servers that your gateway works with.

4. Click **Next**.

To hide the VPN domain:

Select **Hide VPN domain behind this gateway's external IP**.

Select this option only if you want to hide all internal networks behind this gateway's external IP. All outgoing traffic from networks behind this gateway to other sites that participate in VPN community will be encrypted.

With this option, connections that are initiated from other sites that are directed to hosts behind this gateway will **not be encrypted**. If you need access to hosts behind this gateway, choose other options (define VPN topology) or make sure all traffic from other sites is directed to this gateway's external IP and define corresponding NAT port-forwarding rules, such as: Translate the destination of incoming HTTP connections that are directed to this gateway's external IP to the IP address of a web server behind this gateway.

To create a new VPN domain group:

1. Make sure that the **Create a new VPN domain** option is selected.
2. In the **Name** field, enter a name for the group.
3. From the **Available objects** list, select the applicable objects and click **Add**. The objects are added to the VPN domain members list.

To select a predefined VPN domain:

1. Click **Select an existing VPN domain**.
2. From the **VPN Domain** list, select the domain.
3. Click **Next**.

   In the Installation Wizard Completion page, you see a summary of the configuration parameters you set.
4. If you want to configure more options of the Security Gateway, select **Edit Gateway properties for further configuration**.
5. Click **Finish.**

The General Properties window of the newly defined object opens.

## Preparing to Install the Security Policy

To prepare the policy for automatic installation when the gateway connects:

1. In the menu, click **Policy** > **Install**.
2. Select the Security Gateways on which to install the policy.

   The Install Policy window opens.
3. Select the policy components.

4. Select how the security policy is installed:
   - On each selected gateway independently
   - On all selected gateways

   If it fails, do not install on gateways of the same version.
5. Click **OK**.

   The Installation Process window shows the status of the Network Security policy for the selected target.

If you used the **Management First** configuration option:

- The Check Point 1430/1450 Appliance object is defined but the appliance is not set up.
- The Installation Process window shows the "Waiting for first connection" status and the message "Installation completed successfully". The policy is successfully *prepared* for installation and not actually installed. When the appliance will be set up and the gateway connects to the Security Management Server, it establishes trust and then attempts to install the policy automatically.

If you used the **Gateway First** configuration option:

- When you successfully complete this step, the policy is pushed to the Check Point 1430/1450 Appliance.
- For a list of possible statuses, see Viewing the Policy Installation Status (on page 86).

You can track the status of the security policy installation with the Policy Installation Status window and the status bar.

## Setting Up the Check Point 1430/1450 Appliance

1. Remove the Check Point 1430/1450 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 lights up. This indicates that the appliance is turned on.
   The Alert LED (called the Notice LED in the 600 appliance) on the front panel starts to blink. This indicates that the appliance is booting up.
   When the Alert 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 1430/1450 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 1430/1450 Appliance model and the options you select.

## *Starting the First Time Configuration Wizard*

To configure the Check Point 1430/1450 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:

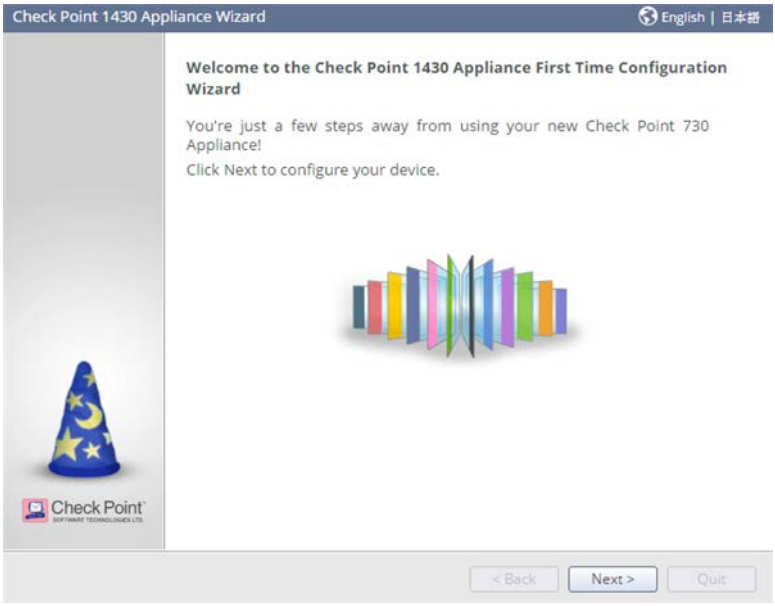
- http://my.firewall
- http://192.168.1.1:4434

If a security warning message shows, confirm it and continue. For more details, see Appendix A: Browser Security Warnings (on page 84).

The **First Time Configuration Wizard** runs.

### *Welcome*

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




To change the language of the WebUI application:

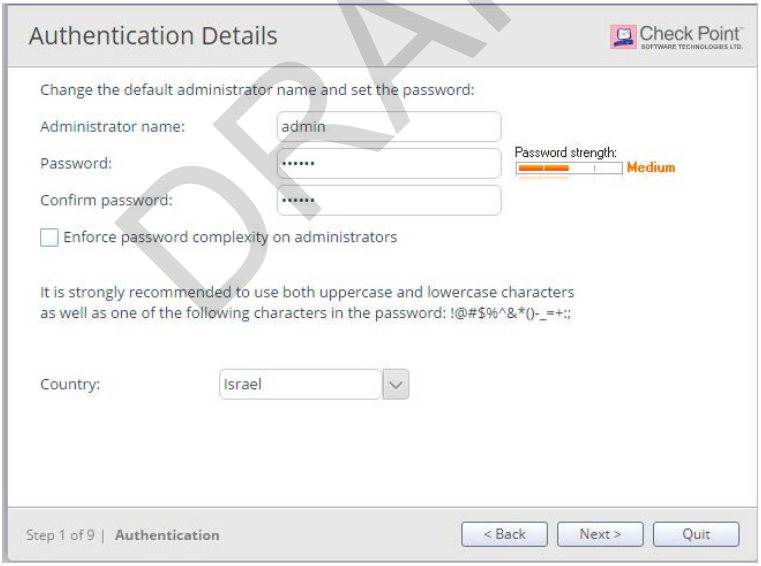
Select the language link at the top of the page.

Note that only English is allowed as the input language.

### *Authentication Details*

In the **Authentication Details** page, enter these details to log in to the Check Point 1430/1450 Appliance WebUI application or if the wizard closes abnormally:

- **Administrator Name -** We recommend that you change the default "admin" login name of the administrator. The name is case sensitive.
- **Password -** A strong password has a minimum of 6 characters with at least one capital letter, one lower case letter, and a special character. Use the **Password strength** meter to measure the strength of your password.
  **Note** - The meter is only an indicator and does not enforce creation of a password with a specified number of characters or character combination. To enforce password complexity, click the check box.
- **Confirm Password -** Enter the password again.
- **Country** - Select a country from the list (for wireless network models).

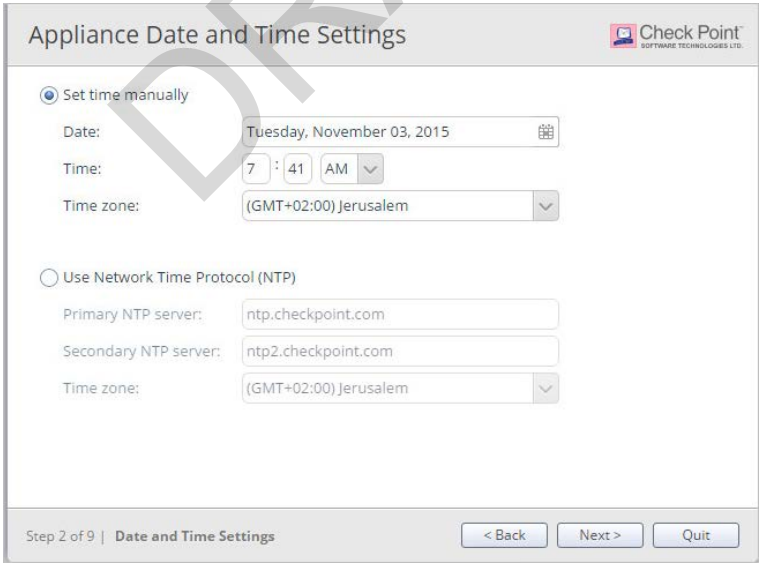



## *Appliance Date and Time Settings*

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. 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.



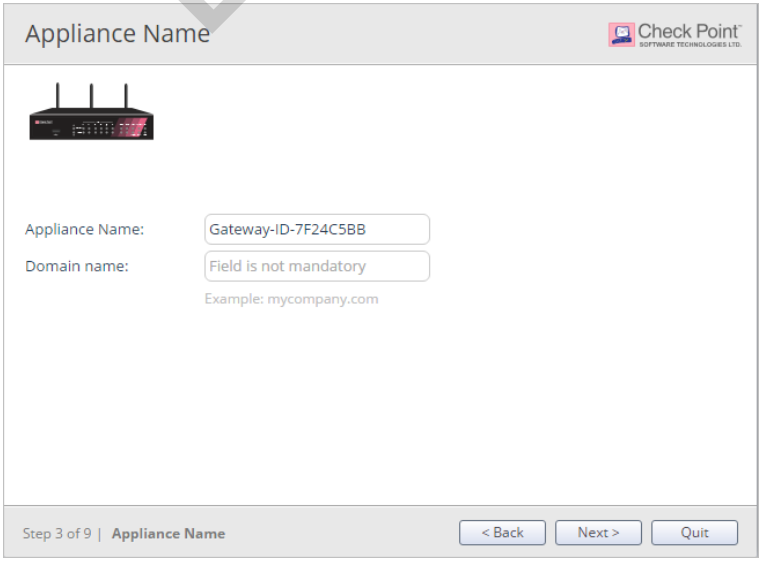

## *Appliance Name*

In the **Appliance Name** page, enter a name to identify the Check Point 1430/1450 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.

The name of the appliance must be identical to the name of the gateway object in the Security Management Server if:

- Check Point 1430/1450 Appliance does not use a static IP and the unique identifier for the gateway in SmartDashboard is set to use the gateway name.
- Check Point 1430/1450 Appliance is managed through SmartProvisioning.

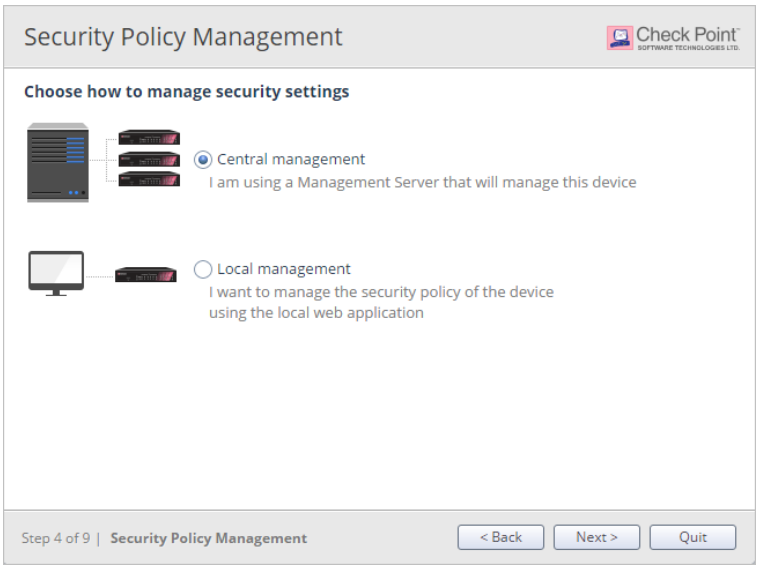


### *Security Policy Management*

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

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

This Getting Started Guide describes how to configure a centrally managed deployment.



*Internet Connection*

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

To configure Internet connection now:

1. Select **Configure Internet connection now**.
2. From the **Connection Protocol** drop down list, select the protocol used for connecting to the Internet.
3. Fill in the fields for the selected connection protocol. The required information 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.
- **Analog Modem** - Connect to the Internet using an analog modem.
- **Bridge** - Connects multiple network segments at the data link layer (Layer 2).
- **Wireless** - Connects to a wireless network. Connection through the wireless interface in the First Time Configuration Wizard is always DHCP.

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, 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.

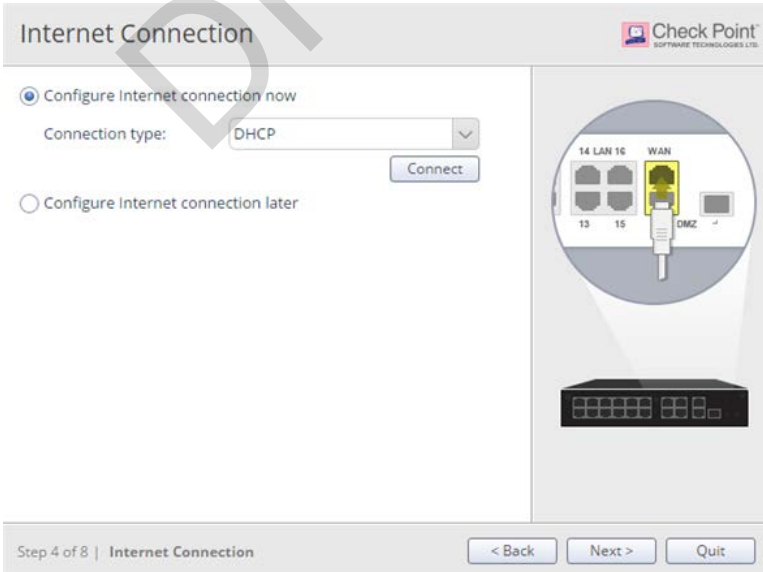
   We recommend you configure the DNS as Check Point 1430/1450 Appliance needs to perform DNS resolving for different functions. For example, to connect to Check Point User Center during license activation or when Application Control, Web Filtering, Traditional Anti-virus or Anti-spam services are enabled.

5. In the **Network names(SSID)** field, click the arrow to select a wireless network.

   If the network is secure, enter a password. Depending on the security type, you might need to enter the user name.

To test your ISP connection status:

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



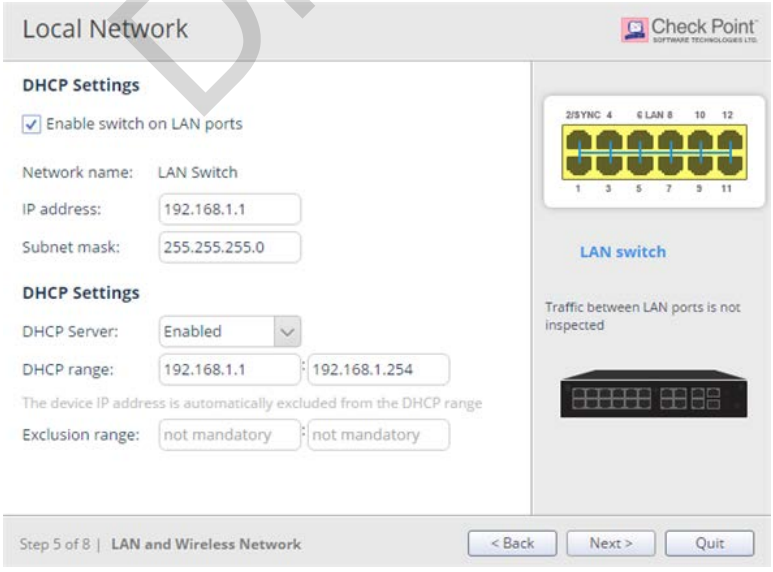

## *Local Network*

In the **Local Network** page, select 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)*

This applies to Wireless Network (WiFi) models only.

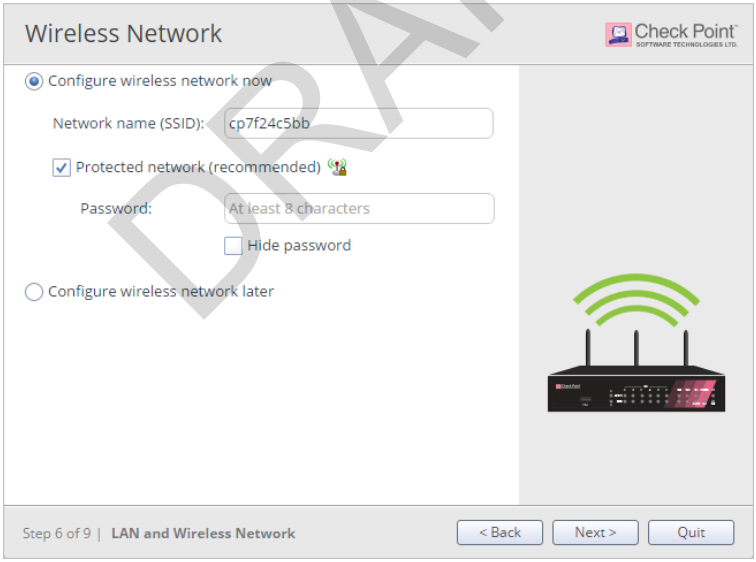
In the **Wireless Network** page, configure wireless connectivity details.

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

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

To configure the wireless network now:

1. Select **Configure wireless network now.**
2. Enter a name in the **Network name (SSID)** field. This is the 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. Click **Hide** to conceal the password.




## *Administrator Access*

In the **Administrator Access** page, configure if administrators can use Check Point 1430/1450 Appliance from a specified IP address or any IP address.

To configure administrator access:

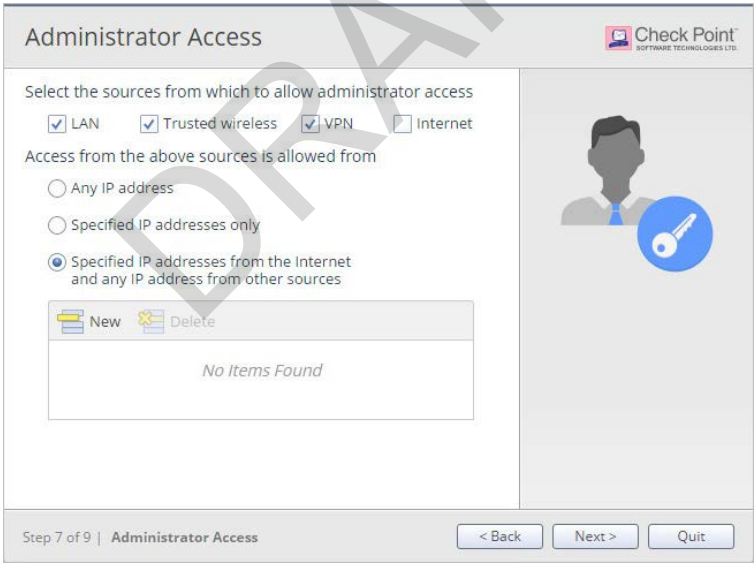
1. Select the sources from where administrators are allowed access:
   - **LAN -** All internal physical ports.
   - **Trusted wireless -** Wireless networks that are allowed access to the LAN by default. This field is only shown in wireless network modes.
   - **VPN -** Uses encrypted traffic through 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 that the administrator can access Check Point 1430/1450 Appliance from:
   - **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.

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 Activation*

In the **Appliance Activation** page, 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 will be notified that you successfully activated the appliance and you will be shown the status of your license for each blade.

If you work offline while you configure the appliance:

On a computer with authorized access to the Check Point User Center http://supportcenter.checkpoint.com, use your User Center account or Register your appliance.

To use your User Center account:

1. Log into your User Center account.
2. Select the specified container of your Check Point 1430/1450 Appliance.
3. From the **Product Information** tab, click **License** > **Activate**.
   This message is shown: "Licenses were generated successfully."
4. Click **Get Activation File** and save the file locally.

To register your appliance:

1. Go to http://register.checkpoint.com (http://register.checkpoint.com/cpapp).
2. Fill in your appliance details and click **Activate**.
   This message is shown: "Licenses were generated successfully."
3. Click **Get Activation File** and save the file locally.

To continue configuring your appliance:

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

   The Import from File window opens.
2. **Browse** to the activation file you downloaded and click **Import**. The activation process starts.

   You will be notified that you successfully activated the appliance and you will be 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.**

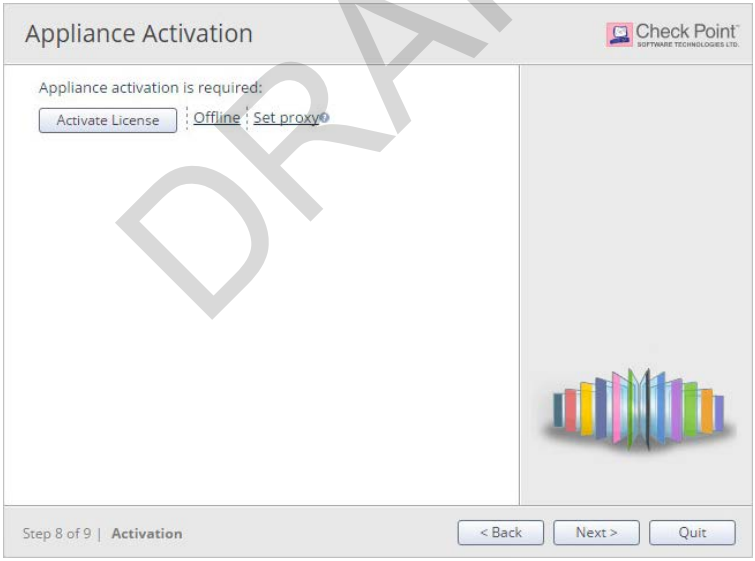
   You will be notified that you successfully activated the appliance and you will be shown the status of your license for each blade.

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

1. Click **Next**.

   The "License activation was not complete" message shows.
2. Click **OK**.

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




### *Security Management Server Authentication*

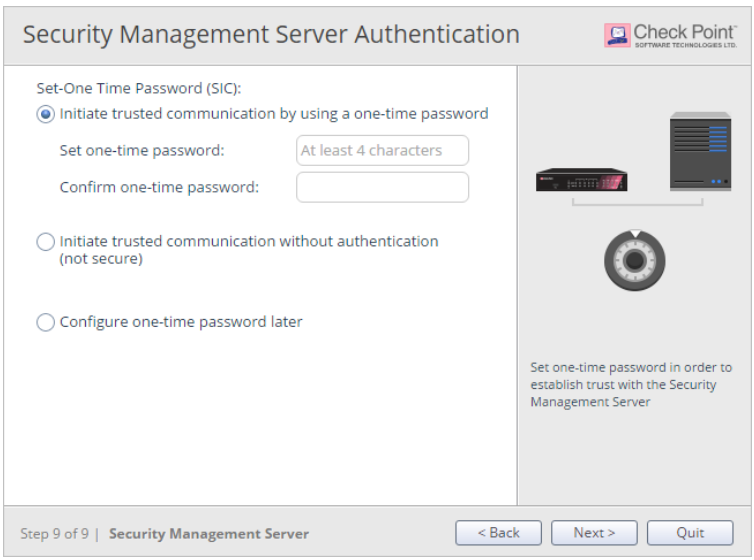
When you select central management as your security policy management method, the **Security Management Server Authentication** page opens.

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 Check Point 1430/1450 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 to the Secure Communication authentication one-time password configured for the Check Point 1430/1450 Appliance object in the SmartDashboard 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*

After you set a one-time password for the Security Management Server and the Check Point 1430/1450 Appliance, you can connect to the Security Management Server to establish trust between the Security Management Server and Check Point 1430/1450 Appliance.

Select **Connect to the Security Management Server now** to connect to the Security Management Server now.

- **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 in order to reach the Security Management Server.

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

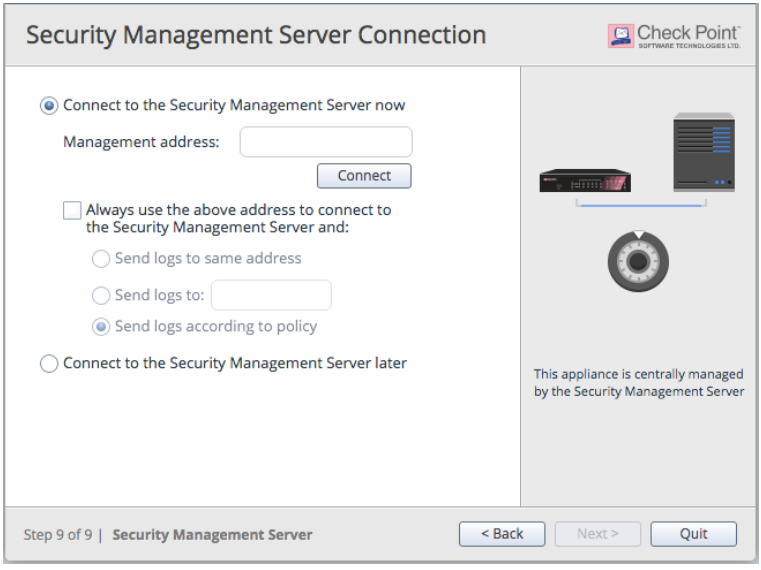
  If you enter a host name, it is saved and the Security Gateway will re-resolve the name if the IP address changes. This configuration can be edited later in the **Home** > **Security Management** page of the WebUI.

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

Select where to send logs:

- **Send logs to same address** - The logs will be 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 will be sent according to the log server definitions that are defined in the policy.

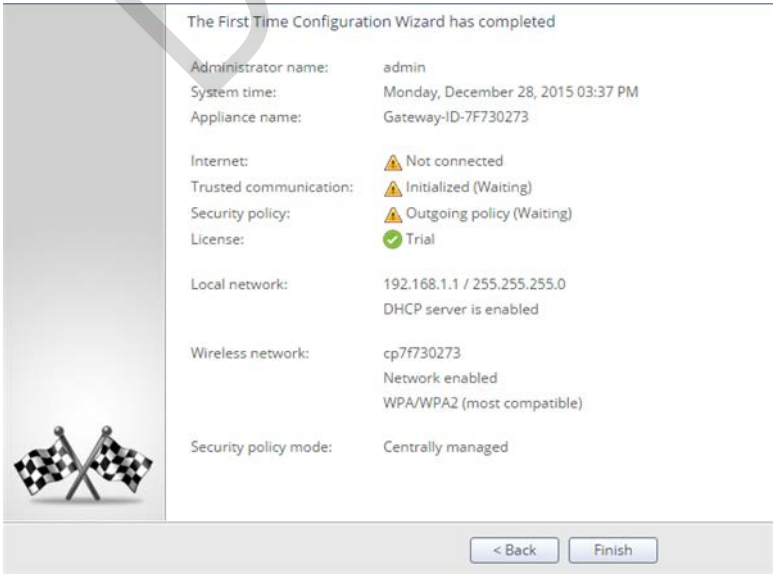
Select **Connect to the Security Management Server later** to connect to the Security Management Server later.



*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** > **Backup** page.

# Large-scale Deployment

## Defining a SmartLSM Gateway Profile for a Large-scale Deployment

SmartLSM lets you manage a large number of Check Point 1430/1450 Appliance gateways from one Security Management Server. When you use a SmartLSM profile, you reduce the administrative overhead per gateway by defining most of the gateway properties, as well as the policy, per profile. The SmartLSM profile is a logical object that contains the firewall and policy components.

Use SmartDashboard to define a single SmartLSM profile for Check Point 1430/1450 Appliance.

### To define a single SmartLSM profile Check Point 1430/1450 Appliance:

1. Log in to SmartDashboard using your Security Management credentials.
2. Open the Security Policy that you want to be enforced on the Check Point 1430/1450 Appliance SmartLSM Security Gateways.
3. From the Network Objects tree, right-click **Check Point** and select **SmartLSM Profile > Small Office Appliance Gateway**.

   The **SmartLSM Security Profile** window opens.
4. Define the SmartLSM security profile using the navigation tree in this window.

   To open the online help for each window, click **Help**.

5. Click **OK** and then install the policy.

**Note** - To activate SmartProvisioning functionality, a security policy must be installed on the LSM profile.

6. Continue in SmartProvisioning.

## Deploying with SmartProvisioning

You can use SmartProvisioning to manage many Check Point 1430/1450 Appliance gateway objects with deployed SmartLSM security profiles. Configure these appliances using the First Time Configuration Wizard (on page 57) or a USB drive configuration file.

For more information about the USB drive configuration file and large-scale deployment using SmartProvisioning, see the relevant *Check Point Appliance Administration Guide*.

# Restoring Factory Defaults

The Check Point 1430/1450 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 1430/1450 Appliance to its factory default settings if necessary.

You can restore a Check Point 1430/1450 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 1430/1450 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 12 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 disable the option for reset to default:

Use this CLI command:

```
>set additional-hw-settings reset-timeout 0
```

### To enable the option for reset to default:

Use this CLI command:

```
>set additional-hw-settings reset-timeout 12
```

To restore the Check Point 1430/1450 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. Restart Boot-Loader
   7. Run Hardware diagnostics
   8.Upload preset configuration file
   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.

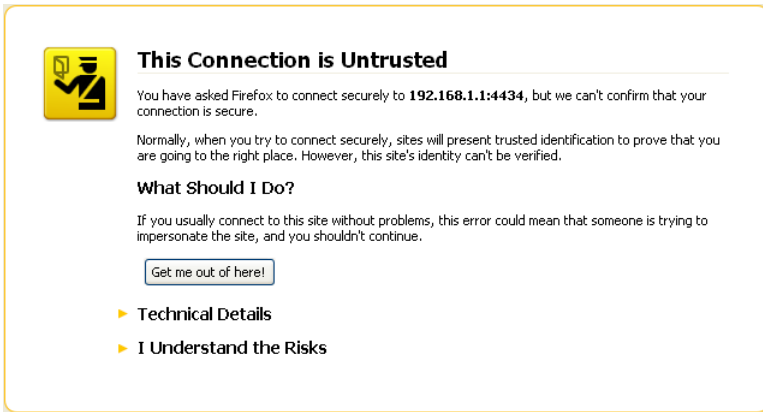
   While factory defaults are being restored, all LAN Link and Activity LEDs blink orange and green alternately to indicate progress. This takes up to a few minutes. When completed, the appliance boots automatically.

# 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.

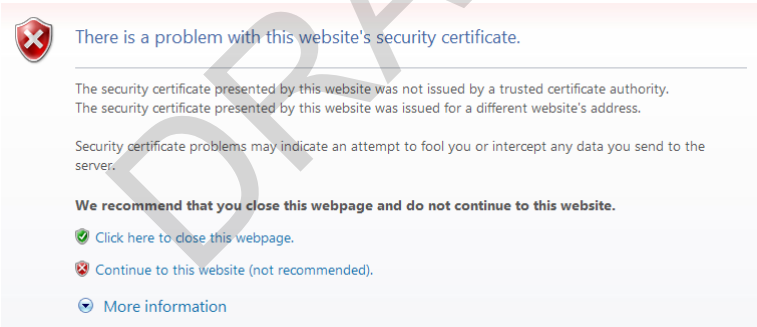
You can safely confirm the warning and continue to log in as usual.

### Mozilla FireFox



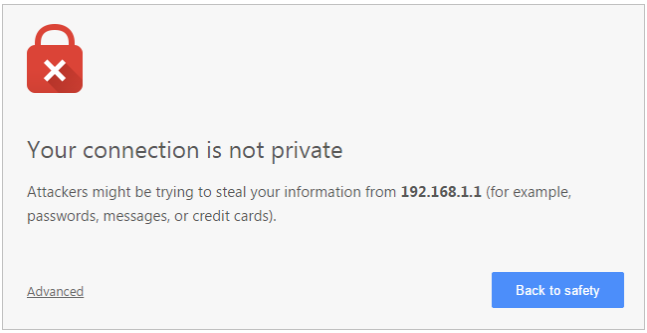

1. Click **I understand the Risks**.
2. Click **Add Exception**. The Add Security Exception dialog box opens.
3. Click **Confirm Security Exception**.

### 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.

# Appendix B: Security Management Issues

## Viewing the Policy Installation Status

You can see the installation status of managed gateways with the status bar that shows at the bottom of the SmartDashboard window. The status bar shows how many gateways are in Pending or Failed mode.

- Pending - gateways that are in the waiting for first connection status or are in the pending status (see below for detailed explanations).
- Failed - gateways that have failed to install the policy.

The status bar is updated dynamically each time a gateway tries to install a policy or tries to connect to the Security Management Server. The results of these actions are also shown in SmartDashboard popup notification balloons when such events occur. You can configure these notifications ("Configuring Notification Settings " on page 90).

To monitor the status of the last policy installed on each gateway, you can use the Policy Installation Status window.

The window has two sections. The top section shows a list of gateways and status details regarding the installed policy. You can use the filter fields to see only policies of interest and hide other details by defining the applicable criteria for each field. After you apply the filtering criteria, only entries that match the

selected criteria are shown. If the system logs trusted communication (SIC) attempts from unknown gateways, a yellow status bar opens below the filter fields.

The bottom section shows details of a row you select in the gateway list (errors that occurred, the date the policy was prepared, verification warnings). If there is a yellow status bar, click **Show details** to show the details of unknown gateways that try to connect to the Security Management Server.

These are the different statuses in this window:

| Icon | Policy status | Description |
|---|---|---|
|  | Succeeded | Policy installation succeeded. |
|  | Succeeded | Policy installation succeeded but there are verification warnings. |
|  | Waiting for first connection | A Check Point 1430/1450 Appliance object is configured, but the gateway is not connected to the Security Management Server (initial trust is not established).<br>• If a policy is prepared, it is pulled when the gateway is connected.<br>• If a policy *is not prepared*, the Policy Type column shows "No Policy Prepared." When the gateway is first connected, only trust is established. |
|  | Waiting for first connection | Same as above, with warnings that attempts to establish trust failed or there are verification warnings. |

| Icon | Policy status | Description |
|---|---|---|
|  | Pending | The policy remains in the pending status until the gateway successfully connects to the Security Management Server and retrieves the policy. This status is shown only if there was at least one successful policy installation.<br>For example, when the Security Management Server has problems connecting to the Gateway (the Gateway is unavailable for receiving communication, as in behind NAT). |
|  | Pending | Same as above but there are verification warnings. |
|  | Warning | Warning. |
|  | Information | Information. |
|  | Failed | Policy not installed due to a verification error. |
|  | Failed | Policy installation failed. |

You can access the Policy Installation Status window in these ways:

- From the menu bar - Click **Policy** > **Policy Installation Status**.
- From the toolbar - Click the Policy Installation Status icon.
- From the status bar - Click **Failed** or **Pending**. The contents of the Policy Installation Status window are shown filtered according to the link clicked.
- From notification balloons - Click **See Details** in the balloon.

# Configuring Notification Settings

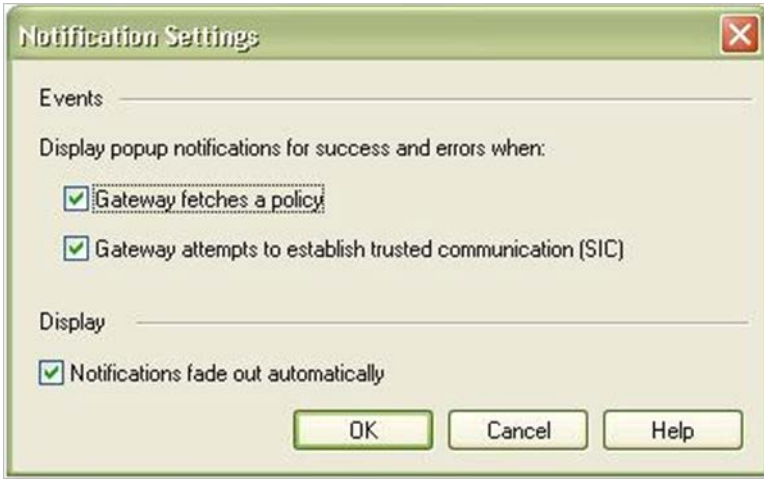
The status bar is updated each time a gateway tries to install a policy or tries to connect to the Security Management Server. You can also configure a popup notification balloon to open in SmartDashboard. You can configure the types of events shown and how notification balloons are shown. By default, notification balloons stay open until they are manually closed.

To configure notification settings:

1. From the Policy Installation Status window, click **Notification Settings**

   or

   From a notification balloon, click **Settings**.




2. To show trials of installing a policy, select **Gateway fetches a policy**.

3. To show trials of connecting to the Security Management Server, select **Gateway attempts to establish trusted communication (SIC)**.
4. To set the notifications to pop-up momentarily in SmartDashboard and then fade out, select **Notifications fade out automatically**. If you do not select this check box, notifications will stay open until you manually close them.

# Getting Support

## Support

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

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

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

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

To learn more about the Check Point Internet Security Product Suite and other security solutions, go to: http://www.checkpoint.com (http://www.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 1430/1450 Appliance and links to the administration guides, see the Check Point site.

Be sure to also use our Online Help when you operate the Check Point 1430/1450 Appliance WebUI and with Check Point SmartConsole clients.