Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point 730/750 Appliance

Locally Managed Getting Started Guide

Models: L-71, L-71W Classification: [Protected] P/N 707409

Latest Documentation

The latest version of this document is at:
http://downloads.checkpoint.com/dc/download.htm?ID=46103

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 730/750 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.

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 *
Product Options:	730, 730 WiFi, 750, 750 Wifi
Date First Applied:	January 2016

Conform to the following Product Specifications:

RF/Wi-Fi (* marked model)

Certification	Type
CE EMC, European Standard EN 55032 & EN 55024. 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	EMC
AS/NZS CISPR 22:2009+A1 2010 Class B	EMC
FCC part 15B , 47 CFR subpart B , Class B ICES-003:2012 Issue 5 Class B ANSI C63.4:2009	EMC
VCCI, V-3/2015.4 Class B, V4/2012.04	EMC
Draft ETSI EN 301 489-1 V2.2.0 (2017-03) Draft ETSI EN 310 489-17 V3.2.0 (2017-03)	EMC

Certification	Type
CE LVD: EN 60950-1	Safety
UL/c-UL: UL 60950-1	Safety
CB IEC 60950-1	Safety
AS/NZS 60950-1	Safety
ETSI EN 300 328 V2.1.1:2006 ETSI EN 300 893 V2.2.2 (2017-05)	RF/Wi-Fi *
RF exposure EN62311:2008, EN62479	RF/Wi-Fi *
RF exposure IC RSS-102 Issue 5:2015 IEEE C95.3-2002 KDB 447498D01	RF/Wi-Fi *
Canada RSS-247 Issue 1 (2015-05) Canada RSS-Gen Issue 4 (2014-11) ANSI C63.10:2013	RF/Wi-Fi *
47 CFR FCC Part15, Subpart C (section 15.247) ANSI C63.10:2013	RF/Wi-Fi *
FCC Part 2 (Section2.1091) KDB 447498 D01	RF/Wi-Fi *

Certification	Type
47 CFR FCC Part 15, Subpart E (Section 15.407) ANSI C63.10:2013	RF/Wi-Fi *
AS/NZS 4268	RF/Wi-Fi *
JP ARIB STD-T66 (V3.7), MIC notice 88 Appendix 43 JP ARIB STD-T71 (V6.1), MIC notice 88 Appendix 45	RF/Wi-Fi *

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 *
Options de produit :	730, 730 Wi-Fi, 750, 750 Wi-Fi
Date de demande initiale :	Janvier 2016

Sont conformes aux normes produit suivantes :

RF/Wi-Fi (modèle signalé par *)

Certification	Type
CE EMC, Norme européenne EN 55032 & EN 55024. 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	EMC
AS/NZS CISPR 22:2009+A1 2010 Classe B	EMC
FCC partie 15B, 47 CFR sous-partie B, Classe B ICES-003:2012 Édition 5 Classe B ANSI C63.4:2009	EMC
VCCI, V-3/2015.4 Classe B, V4/2012.04	EMC

Certification	Type
Draft ETSI EN 301 489-1 V2.2.0 (2017-03) Draft ETSI EN 310 489-17 V3.2.0 (2017-03)	EMC
CE LVD : EN 60950-1	Sécurité
UL/c-UL : UL 60950-1	Sécurité
CB IEC 60950-1	Sécurité
AS/NZS 60950-1	Sécurité
ETSI EN300 328 V2.1.1:2006 ETSI EN 300 893 V2.1.1 (2017-05)	RF/Wi-Fi *
Exposition aux fréquences radio EN62311:2008, EN62479	RF/Wi-Fi *
Exposition aux fréquences radio IC RSS-102 Édition 5:2015 IEEE C95.3-2002 KDB 447498D01	RF/Wi-Fi *

Certification	Type
Canada RSS-247 Édition 1 (2015-05) Canada RSS-Gen Édition 4 (2014-11) ANSI C63.10:2013	RF/Wi-Fi *
47 CFR FCC Partie 15, Sous-partie C (section 15.247) ANSI C63.10:2013	RF/Wi-Fi *
FCC Partie 2 (Section 2.1091) KDB 447498 D01	RF/Wi-Fi *
47 CFR FCC Partie 15, Sous-partie E (Section 15.407) ANSI C63.10:2013	RF/Wi-Fi *
AS/NZS 4268	RF/Wi-Fi *
JP ARIB STD-T66 (V3.7), avis MIC 88 Annexe 43 JP ARIB STD-T71 (V6.1), avis MIC 88 Annexe 45	RF/Wi-Fi *

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

In This Section:

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

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

For more information about the Check Point 730/750 Appliance, see the *Check Point 730/750 Appliance Administration Guide.*

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

Before You Get Started

Review these documents before doing the procedures in this guide:

- Release Notes
- Known Limitations

Shipping Carton Contents

This section describes the contents of the shipping carton.

Contents of the Shipping Carton

Item	Description
Appliance	A single Check Point 730/750 Appliance
Power Supply and Accessories	• 1 power adapter • 1 power cord • 2 standard network cables • 1 serial console cable • 1 mini USB console cable • Wall mount kit (screws and plastic anchors)
Guides	• *Check Point 730/750 Appliance Quick Start Guide* • *Check Point 730/750 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

Appliance Diagrams and Specifications

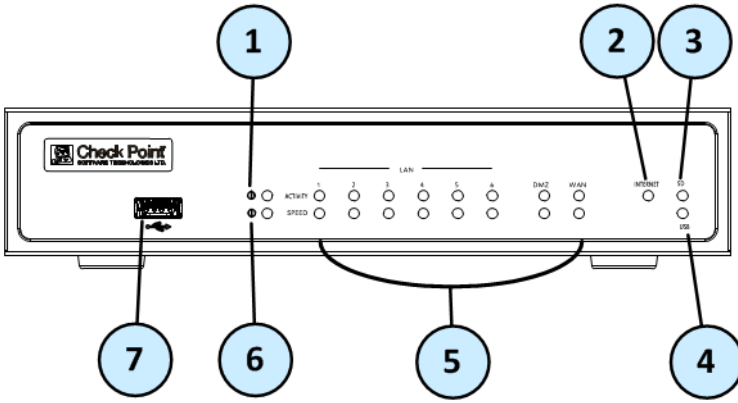
These are the Check Point 730/750 Appliance models:

- Wired
- Wireless (WiFi)

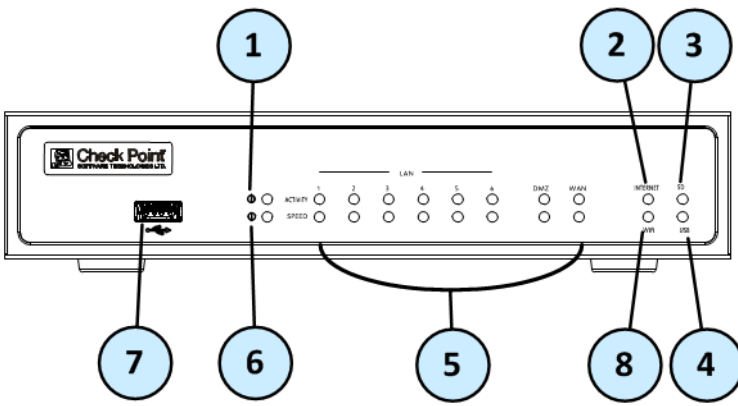
This section describes the differences in the front and back panels.

Front Panel

Wired Model



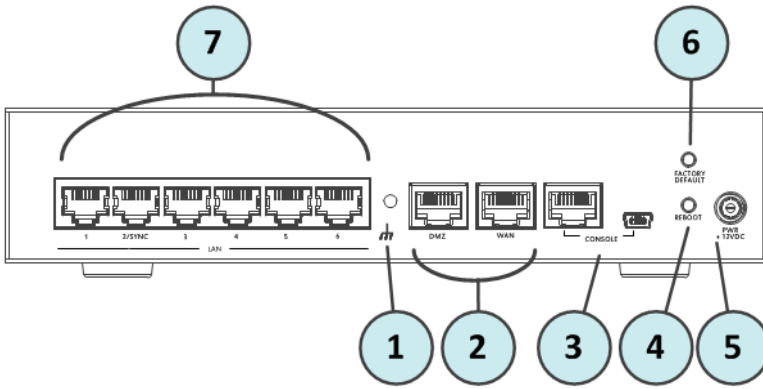
WiFi Model



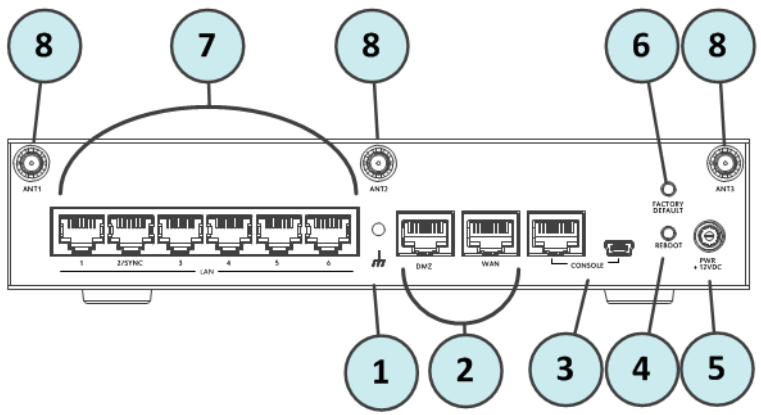
Key	Item	Description
1	Alert LED	• Blinking green during boot. • Red when the appliance has a resource problem such as memory shortage.
2	Internet LED	• Green when connected to the Internet. • Blinking red when the Internet connection is configured but fails to connect.
3	SD LED	Green when SD card is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

Back Panel

Wired Model



WiFi Model



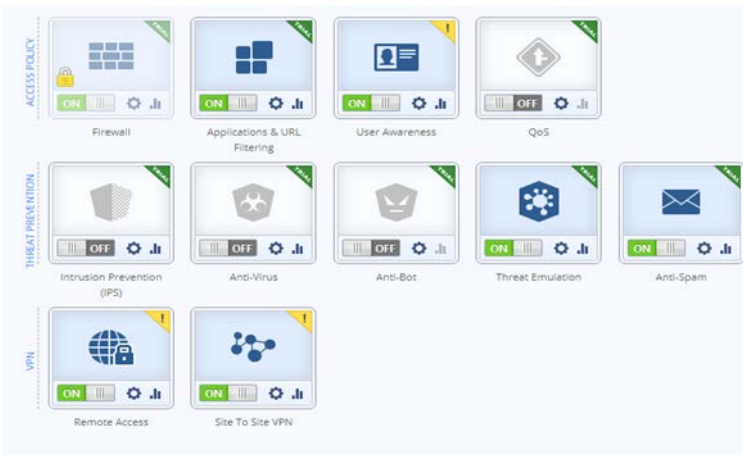
Key	Item	Description
1	Ground (Earth)	Functional grounding.
2	DMZ and WAN ports	Built in Ethernet ports.
3	Console port	RJ45 or Mini USB Serial connection configured to 115200 bps by default. **Note** - When both the RJ45 and Mini USB cables are connected, the Mini USB takes precedence.
4	Reboot button	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.

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 models).

Check Point Software Blades Overview

The available Check Point Software Blades can be divided into these major groups:

- Access Policy
- Threat Prevention
- VPN



Access Policy

The Access Policy has these features:

- **Firewall** - Makes sure that only allowed traffic enters the company's network. Other traffic is blocked before it enters.
- **Application Control and URL Filtering** - Makes sure that only authorized applications are used on the network and only allowed websites can be accessed.
- **User Awareness** - Lets you define policies for individual users.
- **Quality of Service (QoS)** - Enables bandwidth control and lets you give priority to your most important traffic.

Threat Prevention

The Threat Prevention policy has these features:

- **Intrusion Prevention System (IPS)** - Blocks attempts to exploit known vulnerabilities in files and network protocols.
- **Anti-Virus** - Blocks malware, such as viruses and worms, before it can get into the network.
- **Anti-Spam** - Blocks spam.
- **Anti-Bot** - Detects bot-infected machines and blocks 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.

VPN

The VPN protects your business data in these ways:

- **Remote Access** - Encrypts traffic from authorized PCs and user devices that access your network, both in the office and from a remote location.
- **Site-to-Site VPN** - Encrypts all communications between multiple sites in your network.

Cloud Services

Cloud Services lets you connect your Check Point 730/750 Appliance to a Cloud Services Provider that uses a Web-based application to manage, configure, and monitor the appliance. See Setting up Cloud Services (on page 95).

Configuring Check Point 730/750 Appliance

In This Section:

The appliance is a Security Gateway and uses a web application to manage a Security Policy. After you configure the appliance with the First Time Configuration Wizard, the default Security Policy is enforced automatically. Use the WebUI to configure the software blades you activated in the First Time Configuration Wizard and fine tune the Security Policy.

Workflow

This is the recommended workflow for configuring Check Point 730/750 Appliance:

1. Setting up the Check Point 730/750 Appliance (on page 46).
2. Connecting the cables (on page 46).
3. Configuring the appliance with the First Time Configuration Wizard.
4. Defining a security policy with the Web User Interface (WebUI).

Setting up the Check Point 730/750 Appliance

1. Remove the Check Point 730/750 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 730/750 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 730/750 Appliance model and the options you select.

Starting the First Time Configuration Wizard

To configure the Check Point 730/750 Appliance for the first time after you complete the hardware setup, use the First Time Configuration Wizard.

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

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

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

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

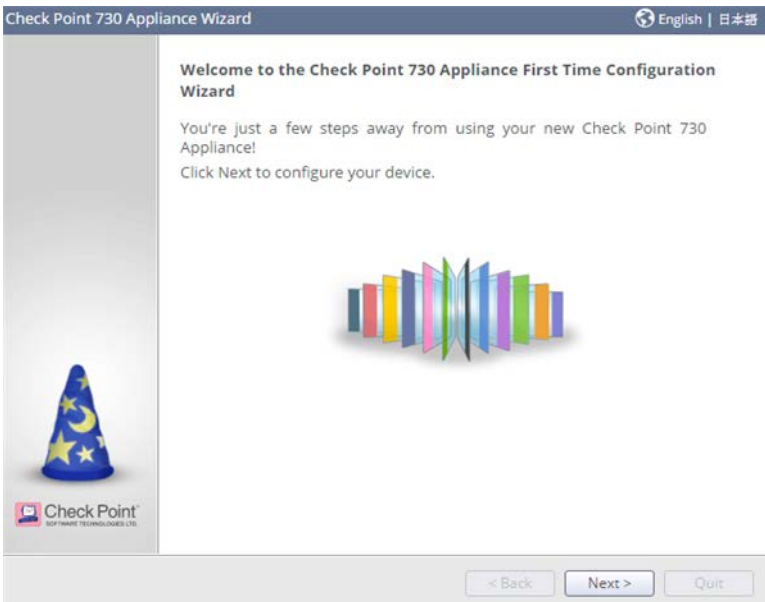
- http://my.firewall
- http://192.168.1.1:4434

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

The **First Time Configuration Wizard** runs.

Welcome

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



To change the language of the WebUI application:

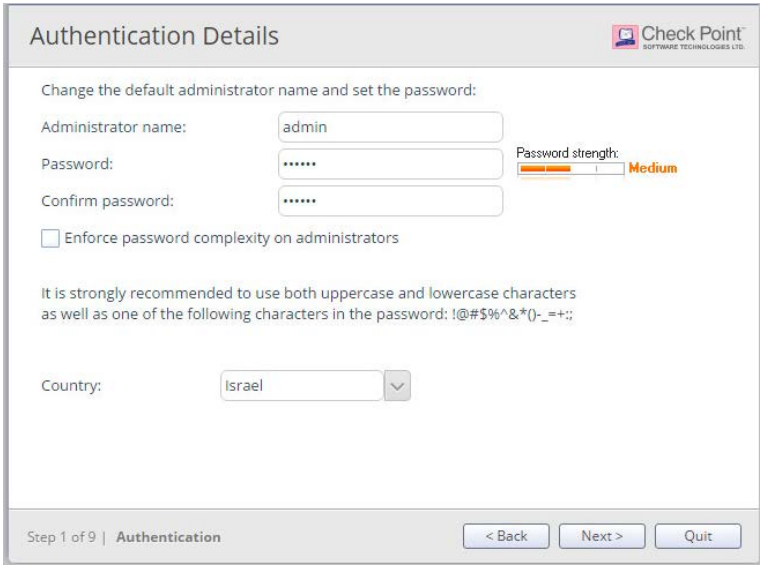
Select the language link at the top of the page.

Note that only English is allowed as the input language.

Authentication Details

In the **Authentication Details** page, enter the required details to log in to the Check Point 730/750 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** - 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).

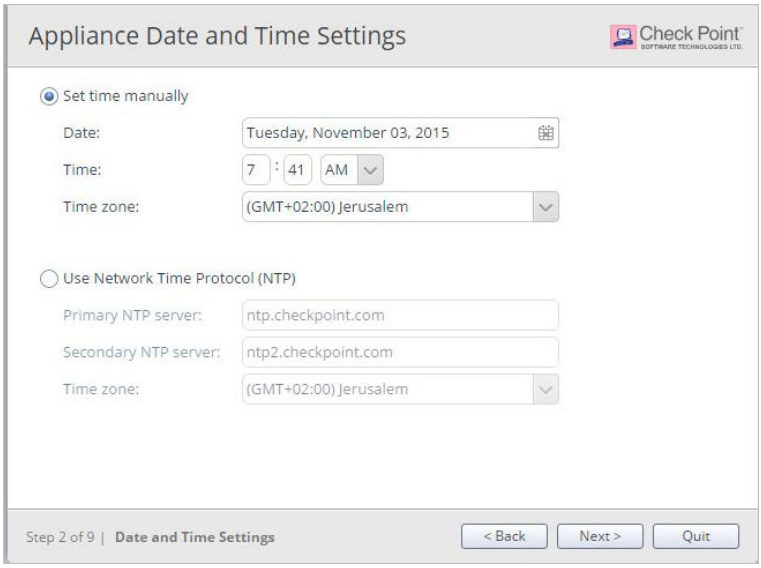


Appliance Date and Time Settings

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 show your correct location. Daylight Savings Time is automatically enabled by default. You can change this in the WebUI application on the **Device** > **Date and Time** page.

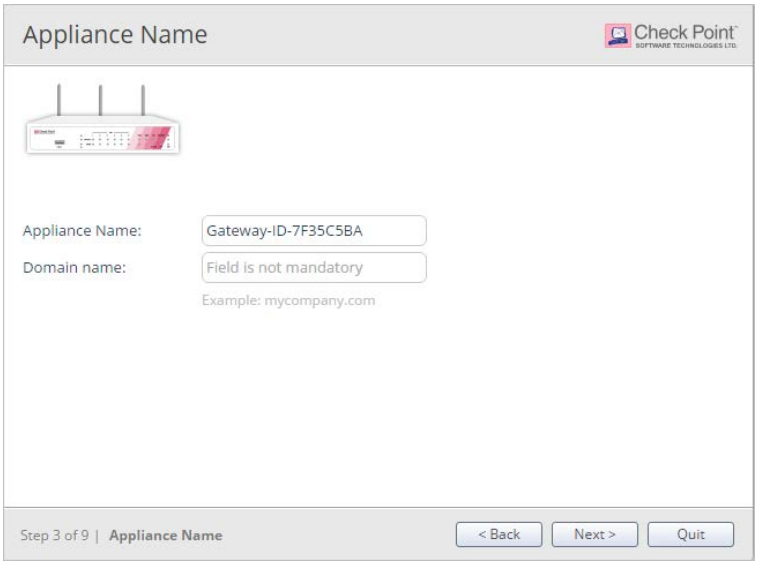
When you use the NTP option, there are two default servers you can use. These are ntp.checkpoint.com and ntp2.checkpoint.com.



Appliance Name

In the **Appliance Name** page, enter a name to identify the Check Point 730/750 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.



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 to connect 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.
    - **Analog Modem** - Connect to the Internet using an analog modem through a USB port. In the WebUI application, you can configure to use an analog modem through the serial port.
    - **Bridge** - Connects multiple network segments at the data link layer (Layer 2).

- **Wireless** - Connects to a wireless network. Connection through the wireless interface in the First Time Configuration Wizard is always DHCP.
- **DNS Server** (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 **Device** > **DNS**.

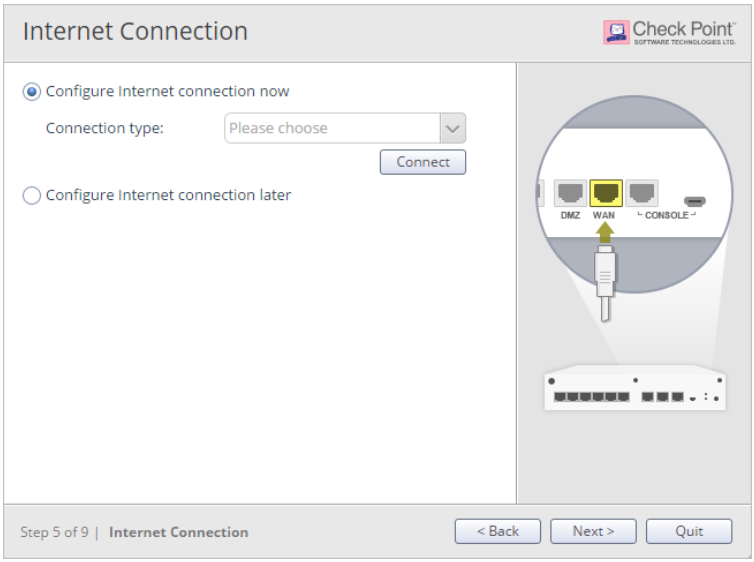
We recommend that you configure the DNS since Check Point 730/750 Appliance needs to perform DNS resolving for different functions. For example, to connect to Check Point User Center during license activation or when Application Control, Web Filtering, Anti-Virus, or Anti-Spam services are enabled.

4. 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.



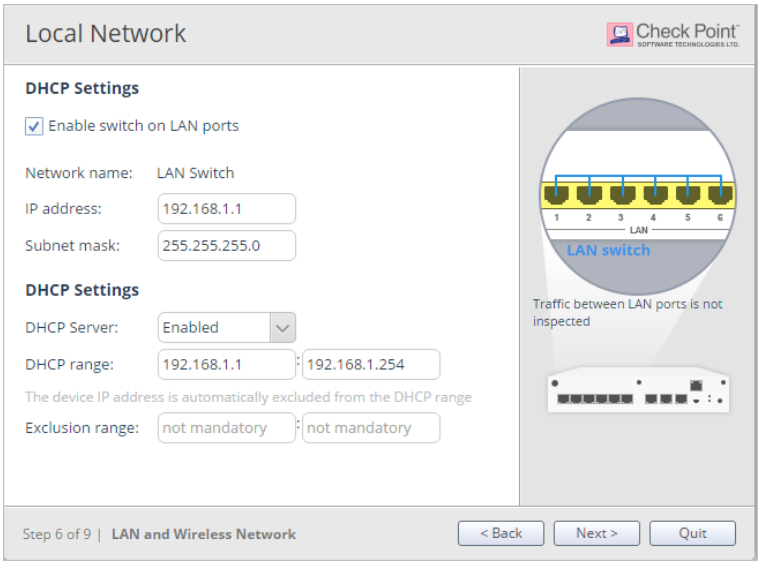
Local Network

In the **Local Network** page, select 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

This applies to Wireless Network models only.

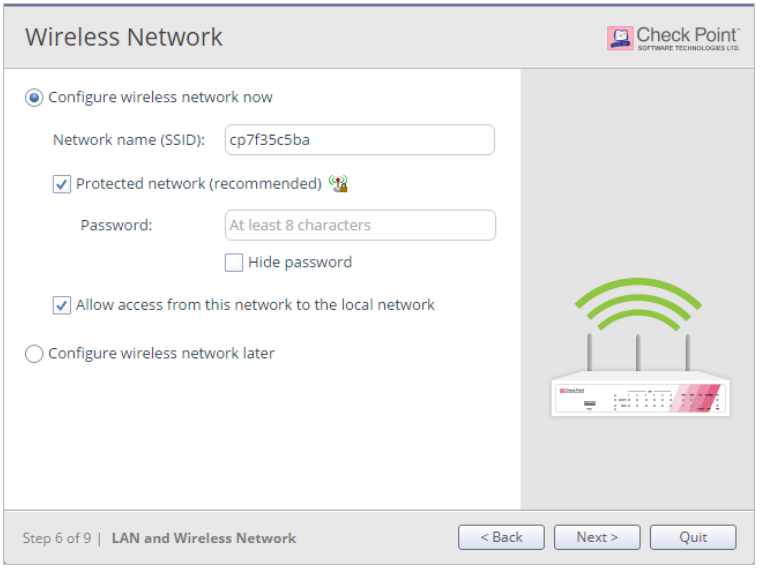
In the **Wireless Network** page, configure wireless connectivity details.

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

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

To configure the wireless network now:

1. Select **Configure wireless network now.**
2. Enter a name in the **Network name (SSID)** field. This is the name shown to clients that look for access points in the transmission area.
3. Select **Protected network (recommended)** if the wireless network is protected by password.
4. Enter a **Password**.
5. Click **Hide** to conceal the password.
6. **Allow access from this network to the local network** is selected by default. Clear if it is not necessary. If this option is selected, the wireless network is considered trusted and access by default is allowed from it to the local network.



Administrator Access

In the **Administrator Access** page, configure if administrators can use Check Point 730/750 Appliance from a specified IP address or any IP address.

To configure administrator access:

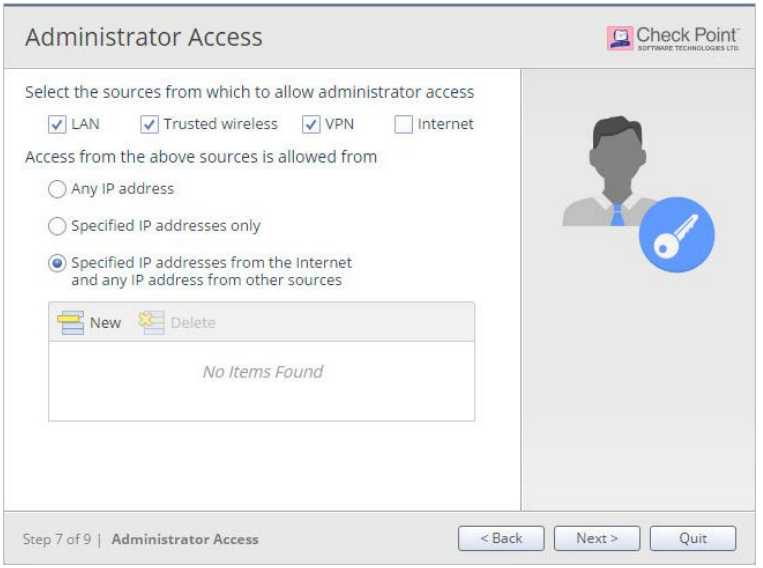
1. Select the sources from where administrators are allowed access:
   - **LAN -** All internal physical ports.
   - **Trusted wireless -** Wireless networks that are allowed access to the LAN by default. This field is only shown in wireless network modes.

- **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 730/750 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.

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

The appliance can connect to the Check Point User Center to pull the license information and activate the appliance. You must register the appliance in your Check Point User Center account. If you don't already have an account, you must create one.

To activate the appliance:

Click **Activate License**.

A 30 day trial license will be used if:

- License activation is not completed.
- The registration information for your MAC address can't be found in the Check Point User Center.

To activate your appliance later:

In the WebUI, go to **Home** > **License** > **Activate License**.

To configure a proxy server:

1. Click **Set Proxy**.

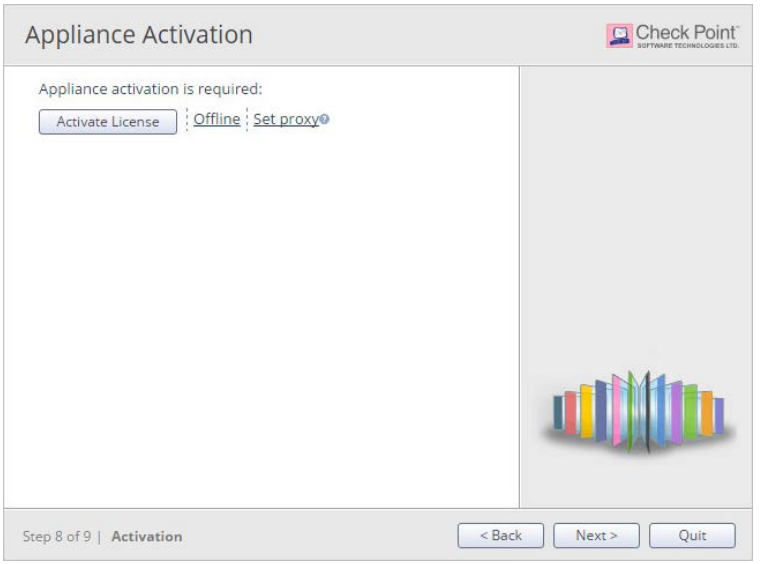
   The **Proxy Configuration** box opens.
2. Select the checkbox **Use proxy server**.
3. Enter the address and port.
4. Click **Apply**.

To configure the appliance offline:

1. Go to http://register.checkpoint.com/cpapp to register your appliance.
2. Enter the appliance's credentials, MAC address and registration key.
3. After you complete the registration wizard, download the activation file to a local location.
4. In the **Appliance Activation** page, click **Offline**.

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

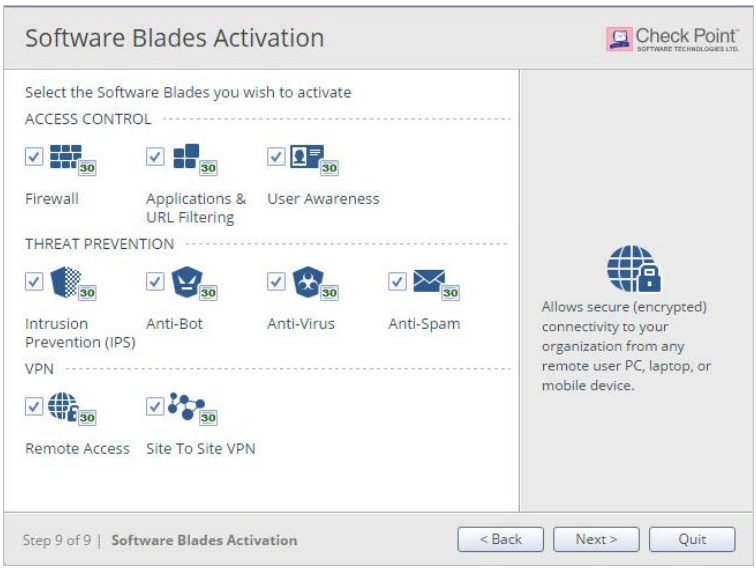
7. You will be notified that you successfully activated the appliance. The next page shows the license status for each blade.



Software Blade Activation

Select the software blades to activate on this Check Point 730/750 Appliance.

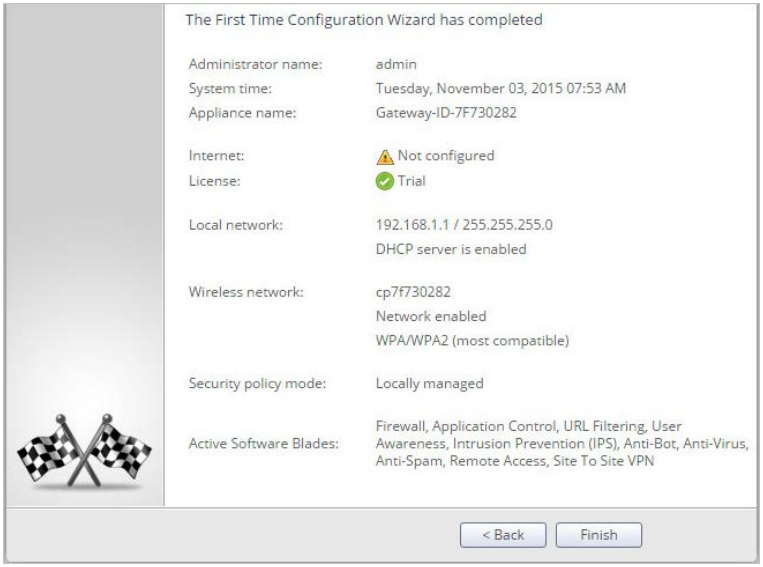
QoS (bandwidth control) can only be activated from the WebUI after completing the First Time Configuration Wizard.



Summary

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

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



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

To back up the system configuration in the WebUI:

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

Basic System Configuration

In This Section:

Do these configurations after you complete the First Time Configuration Wizard and log in to the appliance.

Threat Prevention Updates

Click the status bar at the bottom of the WebUI to see updates. To keep your protection up to date, configure automatic updates.

To schedule updates:

1. Click **Schedule** at the bottom of the page or move the cursor over the update status.
2. Select the blades you want to schedule for updates.

   Note - When a "Not up to date" message shows for other blades, you must manually update them.

3. Select Recurrence:
    - Daily
    - Weekly
    - Monthly
4. Click **Apply**.

Firmware Upgrades

To see notifications of available upgrades:

1. Click the status bar.

   We recommend you configure automatic upgrades.
2. Move the cursor over the notification to show the version number.
3. Click **Upgrade Now** or **More Information**.

To configure automatic upgrades:

1. Go to **Device** > **System Operations**.
2. Click **Configure automatic upgrades**.

   The **Automatic Firmware Upgrades** window opens.
3. Click **Perform firmware upgrades automatically**.
4. Click **Upgrade immediately** or **Upgrade according to this frequency**.
5. Click **Apply**.

   Note - If the gateway is configured by Cloud Services, automatic firmware upgrades are locked.

To make sure you have the latest version:

1. Go to **Device** > **System Operations**.
2. Click **Check now**.

Internet Connectivity

To see the Internet Connectivity status:

Click the status bar.

If you are not connected, go to **Devices** > **Internet**.

Licensing

You must first register the appliance in your Check Point User Center account. If you do not have a User Center account, you must create one to receive support and updates.

To see license information:

1. Go to **Home** > **License**.
2. If you did not do this during the First Time Configuration Wizard, click **Activate**.

If Internet connectivity is configured:

1. Click **Activate License**
2. Browse to http://register.checkpoint.com/cpapp
3. Complete these fields:
   - MAC address
   - Registration key
4. Select **Hardware Platform**.
5. In **Hardware Mode**l, select **Check Point 730/750 Appliance**.
6. Click **Activate License**.

You are notified when you successfully activate the appliance. If changes are made to your license, click **Reactivate** to get the updated license information.

If your license is expired:

Contact your local Check Point representative or visit http://www.checkpoint.com.

To pull a new license:

Go to **User Center** > **License** > **Reactivate.**

Backup and Restore

See *Check Point 600/700 Appliance Administration Guide* for backup and restore instructions.

Configuring Access Policy

In This Section:

Configuring Firewall Policy

Your Check Point 730/750 Appliance is assigned a Firewall policy.

To manually change the policy:

1. Go to **Access Policy** > **Firewall Blade Control**.
2. Select an action:
   - Set the default Access Policy control level.
   - Set the default applications.
   - Set URLs to block.
   - Allow secure browsing.
   - Configure User Awareness.

These are the security levels:

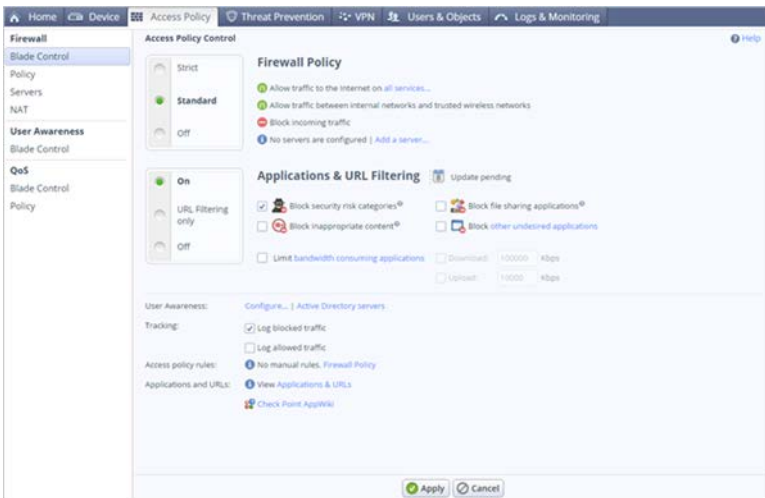
- **Standard (Default) -** Allows outgoing traffic on configured services, and traffic between internal and trusted wireless networks. Blocks incoming unencrypted traffic.
- **Strict -** Blocks all traffic in all directions.
- **Off -** Allows all traffic. Manually defined rules are not applied.

  Note - When the firewall is deactivated, your network is not secured.

To add access policy rules:

Go to **Access Policy** > **Firewall Policy**.

You can also define access to specified servers.



Setting Outgoing Services

To set outgoing services in a Standard policy:

Click **all services**.

To allow specified services only:

1. Click **Block all outgoing services except the following**.
2. Select the services to allow.

To allow all services

1. Click **Allow all outgoing services**.
2. Click **Apply**.

Configuring Applications and URL Filtering

The **Applications & URL Filtering** lets you define the access policy for Internet applications and websites. Select if you want Applications & URL Filtering to be **On, Off**, or **URL Filtering only**.

You can select which categories and applications to block. Security risk categories and applications are blocked by default.

Configure one or more of these options:

- **Block security risk categories -** Lets you block applications and URLs that may be security risks:
  - Spyware
  - Phishing
  - Botnet
  - Spam
  - Anonymizer
  - Hacking

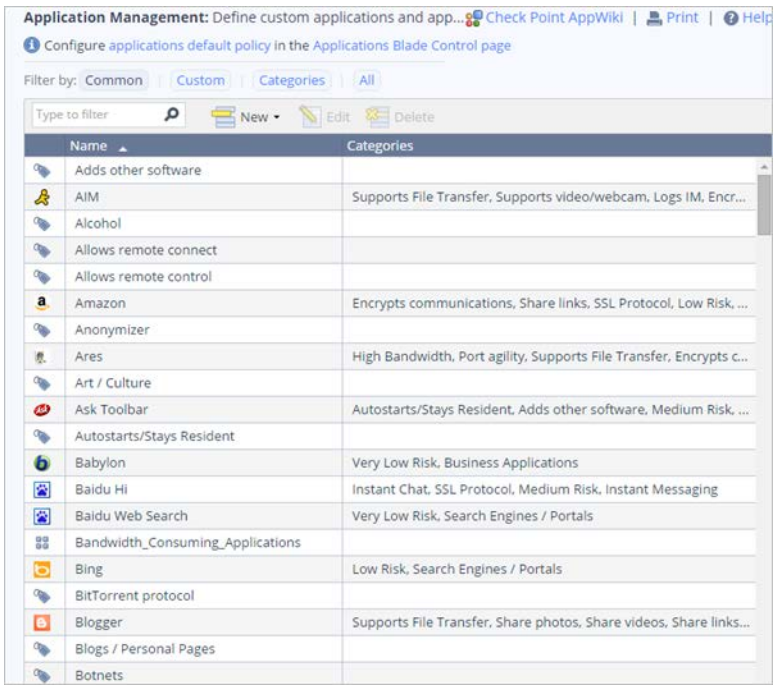
  This option is selected by default.
- **Block inappropriate content -** Lets you block access to websites with inappropriate content like pornography, violence, gambling and alcohol.
- **Block file sharing applications -** Lets you block file-sharing from sources that use torrents and peer-to-peer (P2P) applications.
- **Block other undesired applications -** Lets you block specified applications or URLs. Click this option to manage your basic Application and URL Filtering policy.
- **Limit bandwidth-consuming applications -** Lets you limit or block applications that take up a lot of bandwidth. P2P file sharing, media sharing and media streams are selected by default. You can edit the group to add other applications or categories.

  Note - Your maximum bandwidth limit must be lower than the actual bandwidth provided by your ISP.

Configuring Access Policy

To configure your access policy using standard categories:

1. Go to **Users & Objects** > **Applications & URLs**.
2. Click **applications Default Policy** or **Applications Blade Control page**.
3. Select the applications and URLs to block.
4. Click **Apply**.



Blocking Specific Applications or URLs

To customize your access policy:

1. Go to **Users & Objects** > **Applications & URLs**.
2. Click **Applications Default Policy** or **Applications Blade Control** page.
3. Select **Custom** or **New** to enter a specified application or URL to block.
4. Click **Apply**.

For more information on application and URL control, see the *Check Point 600/700 Appliance Administration Guide* or the online help from the top right corner of your WebUI.

Creating a Permanent Access Rule

A Permanent Access Rule is used to make exceptions to the default category definitions for specified users or groups. You can set stand-alone access rules and block one group of users from an area that others can access, or override the policy and give access to certain applications for only specified users. For example, HR can access Facebook during work hours as part of their job but other users are blocked. Another example of an exception is the payroll records of a company can only be accessed by the finance group.

To create a permanent access rule:

1. Go to **Access Policy** > **Firewall** > **Policy**.
2. In **Outgoing access to the Internet**, click **New**.

   The **Add Rule** window opens.
3. In the **Add Rule** window, click **Any** in the **Source** column and then click **Users** in the new window (Filter: Users).

   This lets you create a rule for the selected user only. See Configuring Local Users (on page 90) for steps to create local users. You can also click **New** > **Local user** to create a new local user from the rule wizard.
4. Select a user from the list.
5. In the **Add Rule** window, click **Any** in the **Application** column.
6. From the **Common** or **Custom** filter, select a URL or application to apply to the rule.

   Or

   Click **New** at the bottom of this window, and then select **URL** or **Application** to enter a customized URL or application.
7. Select **Apply**.
8. Click **Block** or **Accept** in the **Action** column
   - **Block** - Prevent the selected users from accessing the URLs or Applications included in the rule.
   - **Accept** - Override a generic block rule to let the selected users access URLs or Applications.
9. Select when this rule applies.

   Note - This type of access rule will affect all users and groups, unless you set up an overriding rule for individual users or groups.

Blocking Access for Users or Groups

To block internet access for users or groups:

1. Complete steps 1 to 4 in Creating a Permanent Access Rule (on page 74).
2. Make sure **Any** is selected in the **Application** column and **Block** is selected in the **Action** column.
3. Use the time of day feature to apply this rule.

   For example, you can block the network to staff after hours, or block children's Internet access at bedtime at home.

Configuring Threat Prevention

In This Section:

Cyber Threats

Malware is a major threat to network operations that is increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and Trojans.

To challenge today's malware landscape, Check Point's comprehensive Threat Prevention solution offers a multi-layered, pre- and post-infection defense approach and a consolidated platform that enables enterprise security to deal with modern malware.

The Intrusion Prevention System (IPS) blocks potentially malicious attempts to exploit known vulnerabilities in files and network protocols.

The Anti-Virus engine blocks viruses that pass through web and mail traffic (HTTP and SMTP) as well as through the File Transfer Protocol (FTP).

The Anti-Bot engine detects bot-infected machines and blocks bot Command and Control communications.

The Anti-Spam engine blocks or flags emails that contain or are suspected to contain spam.

The Threat Emulation protects networks against unknown threats in files that are downloaded from the internet or attached to emails.

Enabling/Disabling Threat Prevention Control

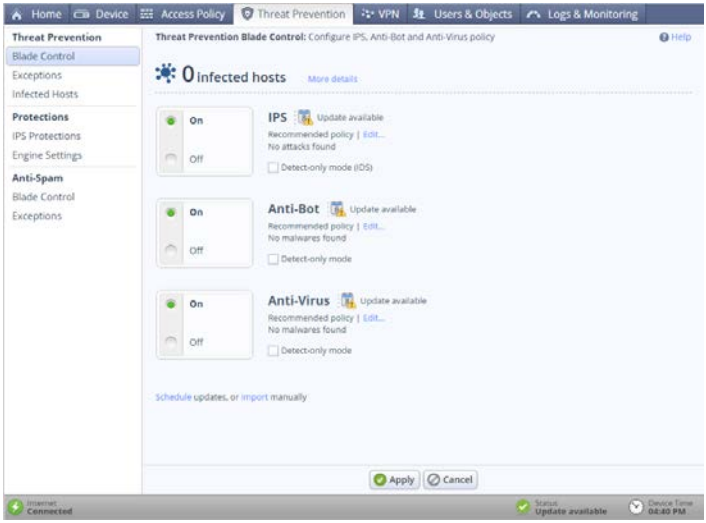
In **Threat Prevention** > **Blade Control**, you can enable or disable the IPS, Anti-Bot, and Anti-Virus blades.

To enable/disable the blade:

1. Go to **Threat Prevention** > **Blade Control**.
2. For the blades you want to enable, select **On**.
3. For the blades you want to disable, select **Off**.
4. Click **Apply**.

   When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in

the next synchronization between the gateway and Cloud Services.



IPS Security Levels

Select the level of IPS protection you want:

- **Typical** - Most suitable for small or medium sized businesses and provides the best mixture of security and performance.
- **Strict** - Focuses on security.
- **Custom** - You can manually define your protection level. After you select this option, click **Apply**.

You can also set IPS to detect-only mode and use the logs to see any attack attempts.

To see the logs:

Go to **Logs & Monitoring** > **Security Logs** page.

Changing the Anti-Virus, Anti-Bot and Threat Emulation Policy

Anti-Virus, Anti-Bot, and Threat Emulation share the same policy. Your Check Point 730/750 Appliance is configured to manage a standard policy.

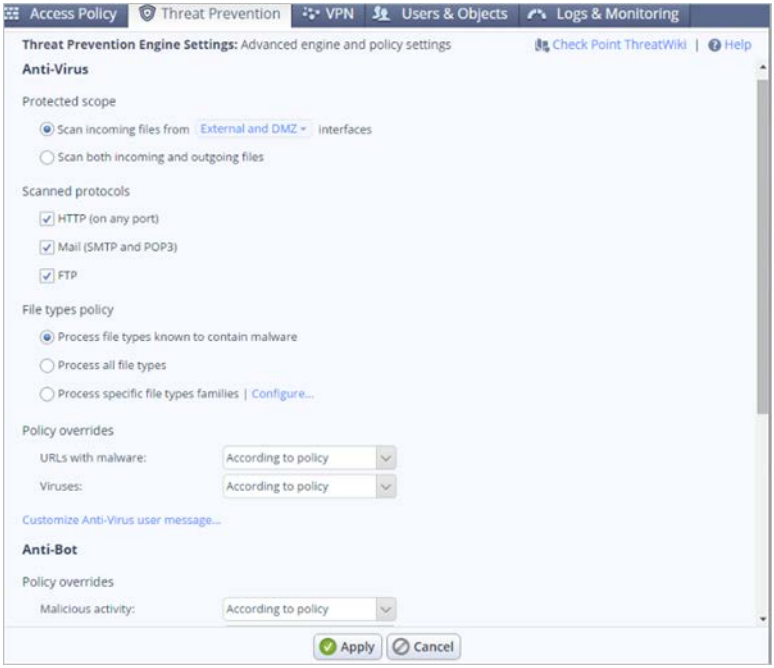
To manually change the policy:

Go to **Threat Prevention** > **Engine Settings**.

You can:

- Configure when files will be inspected.

  By default, only incoming files are inspected.
- Select policy overrides.
- Select file types policy.
- Block viruses from web and mail traffic (HTTP, SMTP, and POP3) and from the File Transfer Protocol (FTP).
- Prevent virus and bot attacks. You can also set **detect only mode** and use the logs to see if there are any attacks.
- Protect against malicious files.



Scheduling Blade Updates

The **Blade Control** page also shows the update status:

- **Up to date**
- **Updated service unreachable -** Usually caused by a loss in Internet connectivity. Check your Internet connection in the **Device** > **Internet** page and contact your ISP if the problem continues.
- **Update available / Not up to date -** A new package is ready to download but it is not time for the scheduled update.

To schedule updates:

1. Go to **Threat Prevention** > **Blade Control**.
2. Click **Schedule Updates**.
3. Select the blades you want to update.
4. Select the recurrence.
5. Click **Apply**.

For more information on Anti-Virus Blade control options, see the *Check Point 600/700 Appliance Administration Guide* or the online help from the top right-hand corner of your WebUI.

Configuring the Anti-Spam Blade

The Anti-Spam blade lets you block or flag emails that contain spam. If you flag emails, you prevent the loss of any emails as suspected spam. You can handle suspected spam differently. You can also set to detect-only mode and use the logs to see if there are spam attacks.

To configure the Anti-Spam blade:

1. Go to **Threat Prevention** > **Anti-Spam Blade Control**.
2. Select **On** or **Off**.
3. Click **Apply**.

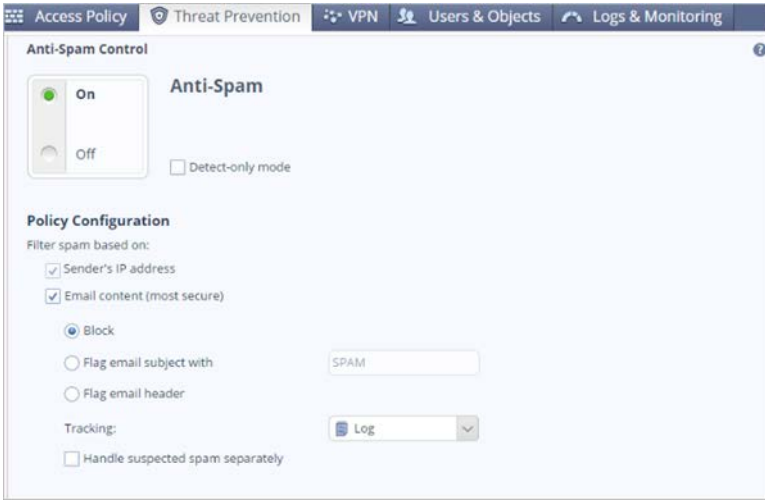
Configuring the Anti-Spam Policy

Your Check Point 730/750 Appliance is configured to manage a typical Anti-Spam Policy. To change this policy, see Configuring Anti-Spam Exceptions (on page 84).

The spam filter can identify spam emails by their source address (default), or by email content.

To configure your appliance to inspect email content:

1. Go to **Threat Prevention** > **Anti-Spam Blade Control**.
2. Click **Email content**.
3. Select one or more of these actions:
   - **Block spam emails**.
   - **Flag spam email subject with X -** Replace X with manually defined text to add to the subject line for spam emails.
   - **Flag spam email header -** Identify email as spam in the email message header.
   - **Handle suspected spam separately**



Configuring Anti-Spam Exceptions

You can configure which senders, domains, or IP addresses are not considered spam. Emails from these senders are not inspected.

You can also identify specified senders, domains or IP addresses for the Anti-Spam engine to automatically block.

To configure Anti-Spam exceptions:

1. Go to **Threat Prevention** > **Anti-Spam**.
2. Click **Exceptions**.

   Note - Filter Spam based on: Email content must be activated on the **Anti-Spam Blade control** page to apply Anti-Spam policies.

For more information on Anti-Spam Blade control options, see the *Check Point 600/700 Appliance Administration Guide* or the online help from the top right-hand corner of your WebUI.

Configuring Anti-Spam to Detect-Only Mode

To configure the Anti-Spam to work in detect only mode:

1. Click **Detect-only mode**.
2. Click **Apply**.

   Note - In detect-only mode, only logs will show. The blade will not block emails.

Setting up Users and Administrators

In This Section:

These sections explain how to set up the initial configuration of your network:

- **Administrators** - Have permission to configure policies and settings
- **Users** - Individuals who have permission to use the appliance but not make any changes to policies
- **Groups** - Users with the same rules are grouped together

Important - You must complete the First Time Configuration Wizard before you do these procedures.

Configuring Local System Administrators

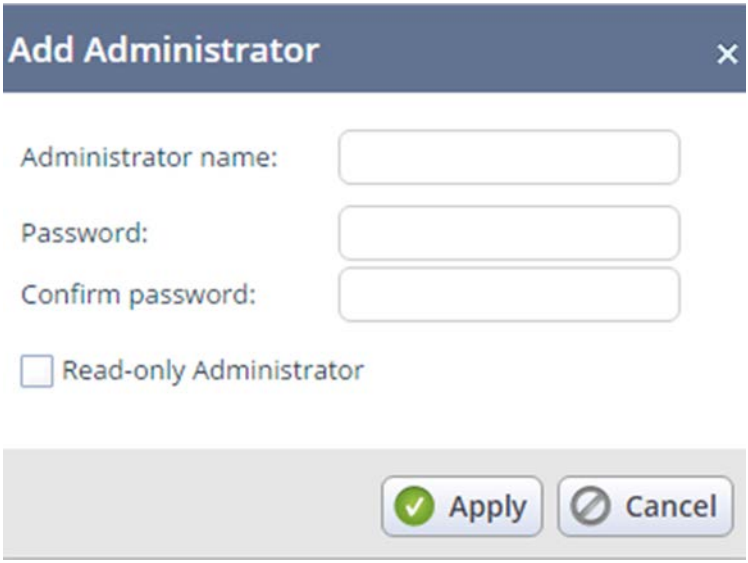
We recommend you configure your system so an administrator can log in from a specific network only.

To configure local system Administrators:

1. Go to **Device** > **Administrators**.
2. Click **New**.

   The Add Administrator window opens.
3. Enter Administrator Name and Password.

   Note - You cannot use these characters in your password: { } [ ] ` ~ | ' "
4. Optional: To set the administrator with read-only privileges, click **Read-only Administrator**.
5. Click **Apply**.



Editing Information of Locally Defined Administrators

To edit information of locally defined administrators:

1. Go to **Device** > **Administrators**.
2. Select the administrator and click **Edit**.
3. Edit the information.
4. Click **Apply**.

   Note - Only administrators with full access privileges can edit administrators.

Deleting a Locally Defined Administrator

To delete a locally defined administrator:

1. Go to **Device** > **Administrators**.
2. Select the administrator and click **Delete**.
3. Click **Yes** in the confirmation window.

   Note - You cannot delete an administrator who is logged in.

Configuring Local Users

User profiles define how users can operate within the network:

- The time frame that users can access the network
- If users can work remotely

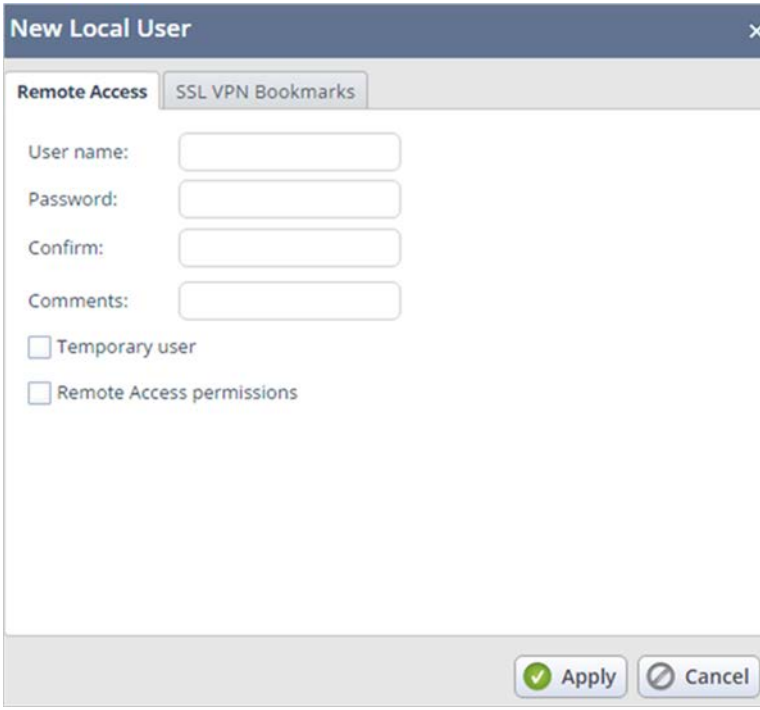
To add a new local user:

1. Go to **Users & Objects** > **User Awareness.**
2. Click **On**.
3. Click **Users**.
4. Click **New**.
5. Enter **User name**, **Password** and **Comments** (optional).

   Note - You cannot use these characters in your password { } [ ] ` ~ | ' "
6. For temporary or guest users, click **Temporary User**. Enter the expiration date and time.
7. To give remote access permissions, select **Remote Access permissions**.

8. Click **Apply**.

   The user is added to the table in the Users window.



Granting Remote Access Permissions

To add a new local users group and grant remote access permissions:

1. Go to **Users & Objects** > **Users**.
2. Click the arrow on the **New** button and select **Users Group**.
3. Enter a group name.
4. Click **Apply**.

To give remote access permissions:

Click **Remote Access permissions**.

To add users to the group:

1. Select from the user list or click **New** to create new users.

   You can see a summary of the group members above the user list. Click the X next to the table to remove members.
2. Click **Apply**.

   The group is added.

Editing a Specific User or Group

To edit a specific user or group:

1. Go to **Users & Objects** > **Users**.
2. Select the user or group from the list.
3. Click **Edit**.
4. Edit the information.
5. Click **Apply**.

Deleting a User or Group

To delete a user or group:

1. Go to **Users & Objects** > **Users**.
2. Select the user or group from the list.
3. Click **Delete**.
4. Click **OK** to confirm.

Setting up Cloud Services

In This Section:

Cloud Services lets you connect your Check Point 730/750 Appliance to a Cloud Services that uses a Web-based application to manage, configure, and monitor the appliance. This lets your appliance be remotely serviced by your managed services provider.

Before you can connect to Cloud Services, make sure you have:

- Received an email from your Cloud Services Provider that contains an activation link.

  Or

- The Service Center IP address, the Check Point 730/750 Appliance gateway ID, and the registration key. Use these details to manually connect your Check Point 730/750 Appliance to Cloud Services.

Connecting to Cloud Services

To automatically connect to Cloud Services:

1. In the email that the Security Gateway owner gets from the Cloud Services Provider, click the **activation link**.

   After you log in, a window opens and shows the activation details sent in the email.
2. Make sure the details are correct and click **Connect**.

This is a sample email:

Dear John Doe,

You are invited to activate your security services using the Security Appliance.
Once connected, you will be fully protected by a comprehensive security solution that will secure your assets and minimize the risks of a data breach.

Click http://myfirewall:443476382020.

If the First Time Configuration Wizard for the Security Appliance appears, follow the initial setup instructions in your Getting Started Guide.

If the above activation link doesn't work, do the following:

1. *On a computer connected to the Security Appliance, browse to the Security Appliance management interface: http://myfirewall:4434.*
2. *Go to the Home tab and select Cloud Services.*
3. *Click on the Configure button.*
4. *Copy your activation key smbmgmt.provisioning.local&Sample-Gateway.domain.Prime&6382020 to the Activation Key field.*

5. *Click Apply to connect.*

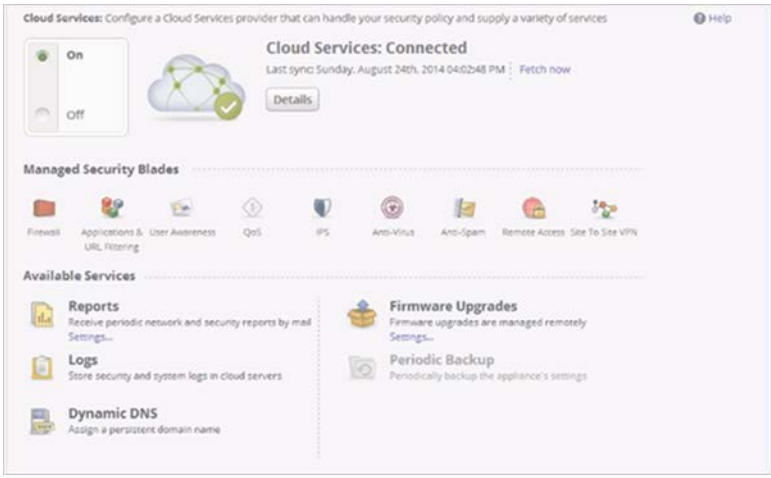
Your appliance will connect to smbmgmt.provisioning.local&Sample-Gateway.domain.Prime (Gateway ID) using the key 6382020 (registration key).

Thank you,
Service Center security team

When connectivity is established, the Cloud Services section at the top of the page shows:

- The date of the synchronization
- The On/Off lever shows that Cloud Services is turned on.

A **Cloud Services Server** widget shows **Connected** on the status bar. Click this widget to open the Cloud Services page.



Guest Network

In This Section:

Your Check Point security appliance lets you provide guest Internet access without giving access to your local network. When you configure a guest network with a Hotspot, you can monitor users that connect through your guest network.

To establish a Guest Network:

- Enable a WiFi network on your appliance. The guest network is actually a Virtual Access Point (VAP).
- Define the network interfaces that will redirect users to the Hotspot portal when they browse from those defined interfaces.

Configuring a Guest Network

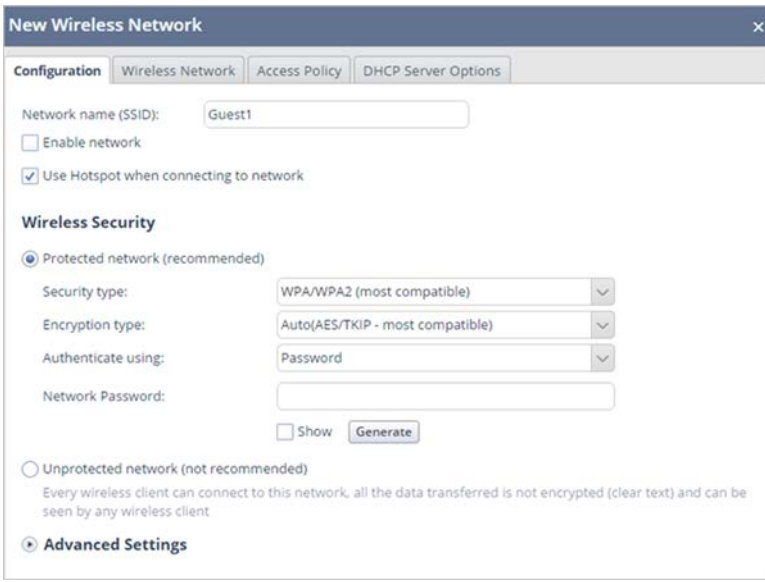
To configure a guest network:

1. Go to **Device** > **Wireless**.
2. Click **Guest**.
3. Select **Use Hotspot**.
4. Set Wireless Security to Unprotected or Protected.

5. In the **Access Policy** tab, set the access and log policy options.

   Note - Do not select the boxes in the **Access Policy** tab if you do not want guests to access your local network.

6. Enter a **password**.
7. Click **Apply**.



Monitoring and Reports

In This Section:

Viewing Monitoring Reports

The **Monitoring** page shows statistics for security events and network analysis. When you enter this page, the latest data shows.

To see monitoring reports:

1. Go to **Home** or **Logs and Monitoring** > **Monitoring**.
2. Select to show statistics from the last hour or last day.
3. Click **Demo** to see sample reports.
4. Click **Refresh** to update information.

Viewing Security Reports

The **Reports** page shows security reports for the time frame you specify. Security events include:

- **High Risk Applications** - The number of potentially risky applications accessed.
- **Infected Hosts** - The number of infected hosts or servers detected.
- **Malwares** - The number of malwares detected by Anti-Bot and Anti-Virus.

To see security reports in the reports dashboard:

1. Go to **Home** or **Logs and Monitoring** > **Reports**.
2. The different security reports show for the specified time frame:
   - Hourly
   - Daily
   - Weekly
   - Monthly

To generate a report:

1. Go to **Reports** > **Generate** to create a new report or **Regenerate** if a report already exists.
2. Click the link to see the report.

   The date and time link shows the date and time of the latest report generation.

   Note - The last generated report for each type is saved. When you generate a new report, you overwrite the last saved report.

Viewing System Logs

The **Security Logs** page shows the last 100 log records. To load more records, scroll down the page. The log table is automatically refreshed.

To see the system logs:

1. Go to **Logs and Monitoring** > **Security Logs**.

   The Security Logs page shows up to 500 system logs generated by the appliance at all levels.
2. Click **View Details** to get more information on the highlighted log.

For more information on Reports, Logs, and Monitoring, see the *Check Point 600/700 Appliance Administration Guide* or the online help from the top right-hand corner of your WebUI.

Getting Support

In This Section:

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.

Where to From Here

You have now learned the basics that are necessary to begin using your Check Point 730/750 Appliance.

For more information about the Check Point 730/750 Appliance and links to the *Check Point 600/700 Appliance Administration Guide*, go to the Check Point Support Center (http://www.checkpoint.com/cp600) where you can find all related sks, downloads, and documentation.