Check Point

SOFTWARE TECHNOLOGIES LTD.

Check Point 1100 Appliance

Centrally Managed

Getting Started Guide

25 February 2013

SG-80A Models:L-50W;L-50WD;L-50xxxxx(x= 0~9, A~Z, Blank or any Character)

Classification: [Protected] P/N 705188

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=22711

For additional technical information, 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 1100 Appliance Centrally Managed Getting Started Guide).

Health and Safety Information

Read the following warnings before setting up or using the appliance.

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

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

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

- When handling the board, use a grounded wrist strap designed for static discharge elimination.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the board by its edges only. Do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling processor chips or memory modules, avoid touching their pins or gold edge fingers.
- Restore the communications appliance system board and peripherals back into the antistatic bag when they are not in use or not installed in the chassis. Some circuitry on the system board can continue operating even though the power is switched off.
- Under no circumstances should the lithium battery cell used to power the real-time clock be allowed to short. The battery cell may heat up under these conditions and present a burn hazard.

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

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

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.

Federal Communications Commission (FCC) Statement:

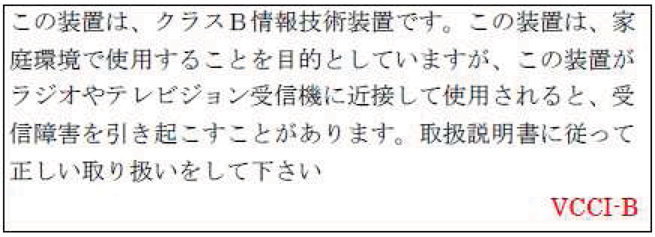
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

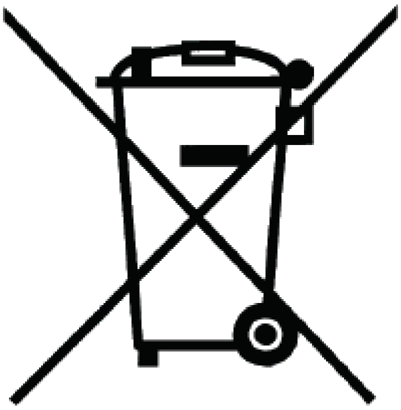
VCCI-B

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 (2004/108/EC).

This product is in conformity with Low Voltage Directive 2006/95/EC, and complies with the requirements in the Council Directive 2006/95/EC 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.

Contents

Chapter 1

Introduction

In This Chapter

Important - Before reading this Getting Started Guide, make sure that you have read and understood the information in the version’s release notes (http://supportcenter.checkpoint.com) and the *Check Point 1100 Appliance Known Limitations SecureKnowledge article* (http://supportcontent.checkpoint.com/solutions?id=sk90342).

Welcome

Thank you for choosing Check Point's Internet Security Product Suite. We hope that you will be satisfied with this solution and our support services. Check Point products provide your business with the most up to date and secure solutions available today.

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

For additional information on the Check Point Internet Security Product Suite and other security solutions, refer to: http://www.checkpoint.com (http://www.checkpoint.com). For technical assistance, contact Check Point 24 hours a day, seven days a week at:+1 972-444-6600 (Americas) +972 3-611-5100 (International). For additional technical information, refer to: http://support.checkpoint.com (http://supportcenter.checkpoint.com).

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

Shipping Carton Contents

This section describes the contents of the shipping carton.

Contents of the Shipping Carton

Item	Description
Appliance	A single Check Point 1100 Appliance
Power Supply and Cables	• 1 power supply unit • 1 standard network cable • 1 serial console cable • 1 telephone cable (only in ADSL models)
Guides	• Check Point 1100 Appliance Quick Start Guide • Check Point 1100 Appliance Getting Started Guide
Wireless Network Antennas	• A pair of wireless network antennas (only in wireless network models)
Sticker	• LEDs behavior
License Agreement	• End User License Agreement

Glossary

The following Check Point 1100 Appliance terms are used throughout this guide:

- **Security Gateway -** The security engine that enforces the organization's security policy and acts as a security enforcement point. The Security Gateway is managed by the Security Management server and sits on the network as an entry point to the LAN.
- **Security Policy -** The policy created by the system administrator that regulates the flow of incoming and outgoing communication.

- **Security Management server** - The server used by the system administrator to manage the security policy. The organization's databases and security policies are stored on the Security Management server and downloaded to the Security Gateway.
- **SmartConsole -** GUI applications that are used to manage various aspects of security policy enforcement. For example, SmartView Tracker is a SmartConsole application that manages logs.
- **SmartDashboard -** A SmartConsole GUI application that is used by the system administrator to create and manage the security policy.

Check Point 1100 Appliance Overview

Check Point's Check Point 1100 Appliance delivers integrated unified threat management to protect your organization from today's emerging threats. Based on proven Check Point security technologies such as Stateful Inspection, Application Intelligence, and SMART (Security Management Architecture), Check Point 1100 Appliance provides simplified deployment while delivering uncompromising levels of security.

Check Point 1100 Appliance supports the Check Point Software Blade architecture, providing independent, modular and centrally managed security building blocks. Software Blades can be quickly enabled and configured into a solution based on specific security needs.

Check Point 1100 Appliance can be centrally managed by a remote Security Management Server or locally managed by a Web user interface (WebUI).

Security Gateway Software Blades

These Software Blades are included in Check Point 1100 Appliance:

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

- **IPSec VPN -** 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 1100 Appliance provides cut-through performance, as URL categorization queries are done asynchronously.
- **Identity Awareness -** Gives user and machine visibility across network blades. Enables the creation of identity-based access policies for application and resource control.
- **IPS (More than 2000 protections**) **-** Best in class integrated IPS with leading performance and unlimited scaling. IPS protections are updated with IPS updates.
- **Anti-spam & Email Security (based on IP Reputation and content) -** Comprehensive and multidimensional protection for organizations' email infrastructure. This includes updates.
- **Traditional Anti-Virus -** Leading Anti-virus protection using state-of-the-art Anti-virus engine by Kaspersky. The Anti-virus engine runs in stream (network) mode, supporting high performance and concurrency.
- **Advanced Networking and Clustering -** For dynamic routing and Multicast support. Wire speed packet inspection with SecureXL and high availability or load sharing with ClusterXL.
- **QoS -** Quality of Service 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.

This Getting Started Guide Includes:

- A brief overview of essential Check Point 1100 Appliance concepts and features.
- A step by step guide to getting Check Point 1100 Appliance up and running.

Chapter 2

Configuring Check Point 1100 Appliance

In This Chapter

Management Options

Check Point 1100 Appliance can be managed centrally or locally.

- **Central Management -** The appliance is only 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.
- **Local Management -** 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. Using the WebUI, you can configure the software blades you activated in the First Time Configuration Wizard and fine tune the Security Policy.

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

Recommended Workflow

There are two types of centrally managed deployments:

- **Small-scale deployment** - Where you configure between 1 and 25 Check Point 1100 Appliance gateways.
- **Large-scale deployment** - Where you configure over 25 Check Point 1100 Appliance gateways using a SmartLSM profile and SmartProvisioning.

The recommended workflow for defining a small-scale deployment (on page 17) includes:

1. Installing a Security Management Server and SmartConsole clients that operate with Check Point 1100 Appliance.
2. Defining the Check Point 1100 Appliance object in SmartDashboard and preparing a policy for it.
3. Setting up the Check Point 1100 Appliance and connecting the cables.
4. Doing initial configuration of Check Point 1100 Appliance using the First Time Configuration Wizard.
5. Optional: You can manage settings such as DNS, host names, and routing through SmartProvisioning. For more information see the *SmartProvisioning Administration Guide*.

The recommended workflow for defining a large-scale deployment (on page 46) includes:

1. Installing a Security Management Server and SmartConsole clients that operate with Check Point 1100 Appliance.
2. Defining a SmartLSM profile in SmartDashboard.
3. Deploying with SmartProvisioning.

Small-scale Deployment

Predefining a Centrally Managed Deployment

To manage the Check Point 1100 Appliance in a centrally managed deployment, you must install a Security Management Server and SmartConsole clients that operate with Check Point 1100 Appliance.

The Security Management Server versions that operate with Check Point 1100 Appliance are versions R75.46, R76 and higher.

For installation instructions, see the version’s release notes (http://supportcenter.checkpoint.com).

After installing the SmartConsole clients you can define the Check Point 1100 Appliance object in SmartDashboard and prepare the security policy (in small-scale deployments) or create a SmartLSM profile (in large-scale deployments).

Defining the Object in SmartDashboard

You can define the Check Point 1100 Appliance in SmartDashboard before or after configuration of the appliance on site. The options are:

Management First - Where you define the gateway object in SmartDashboard before you configure and set up the actual appliance on site. This is commonly used for remotely deployed appliances or appliances that connect to the Security Management Server with a dynamic IP (e.g. assigned by a DHCP server or an ISP), 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.

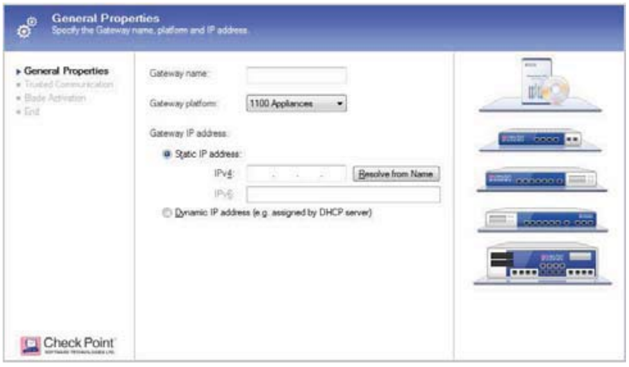
Gateway First – Where you configure and set up the Check Point 1100 Appliance first. It will then try to communicate with the Security Management Server (if this is configured) at 1 hour intervals. If the gateway is connected when you create the object in SmartDashboard, the wizard retrieves data from the gateway (such as topology), and helps in configuration.

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

To define the Check Point 1100 Appliance object:

1. Log in to SmartDashboard using your Security Management credentials.

2. From the Network Objects tree, right click **Check Point** and select **Security Gateway**. The Check Point Security Gateway Creation window opens.
3. Select **Wizard Mode**. The wizard opens to General Properties.
4. Type a name for the Check Point 1100 Appliance object and make sure that the gateway platform is set to **1100 Appliances**.
5. Select one of the following options for getting the gateway's IP address:
   - **Static IP address** - enter the IPv4 address of the appliance. Note that if the Check Point 1100 Appliance has not yet been set up and defined, the **Resolve from Name** option does not work at this point.
   - **Dynamic IP address** (e.g. assigned by DHCP server)



General Properties

Specify the Gateway name, platform and IP address.

Gateway name:

Gateway platform: 1100 Appliances

Gateway IP address:

● Static IP address:

IPv4: . . .

IPv6:

○ Dynamic IP address (e.g. assigned by DHCP server)

Click **Next**.

6. If you specified a static IP address, the Authentication and Trusted Communication sections show (if you specified a dynamic IP address, go to step 7).

   a) In the Authentication section, select one of the options:

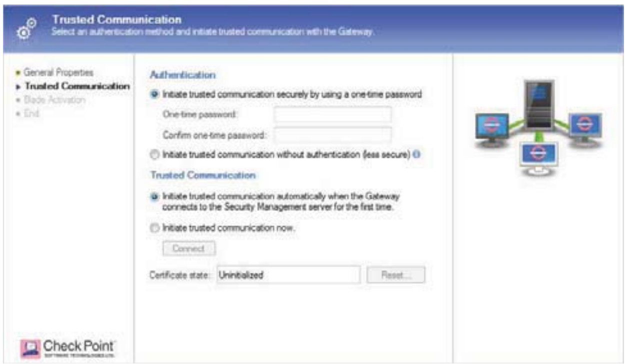
      - **Initiate trusted communication securely by using a one-time password** - the one-time password is used to authenticate communication between the Security Gateway and the Security Management server in a secure manner.
        Enter a **one-time password** and confirm it. This password is only used 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

- **Initiate trusted communication without authentication (less secure)** - select this option only if you are sure that there is no risk of imposture (for example, when in a lab setting).

b) In the Trusted Communication section, select one of the initialization options:

- **Initiate trusted communication automatically when the Gateway connects to the Security Management server for the first time** - trust will be established when the Gateway will connect for the first time.
- **Initiate trusted communication now** and click **Connect**. A status window appears. Use this option only if you have already set up the appliance.



Trusted Communication
Select an authentication method and initiate trusted communication with the Gateway.

- General Properties
- **Trusted Communication**
- Blade Activation
- End

Authentication

● Initiate trusted communication securely by using a one-time password

One-time password:

Confirm one-time password:

○ Initiate trusted communication without authentication (less secure)

Trusted Communication

● Initiate trusted communication automatically when the Gateway connects to the Security Management server for the first time.

○ Initiate trusted communication now.

Connect

Certificate state: Uninitialized

Reset...

The Certificate state field displays the current certificate status.

Click **Next** and go to step 8.

7. If you specified a dynamic IP address, the Gateway Identifier and Authentication sections show.

a) Select one of the identifiers:

- **Gateway name** – enter the same name that you will give the appliance during its initial configuration.
- **MAC address** – enter the MAC address that is on the sticker on the appliance or on the box.
- **First to connect** – means that this Gateway will be the next appliance to connect.

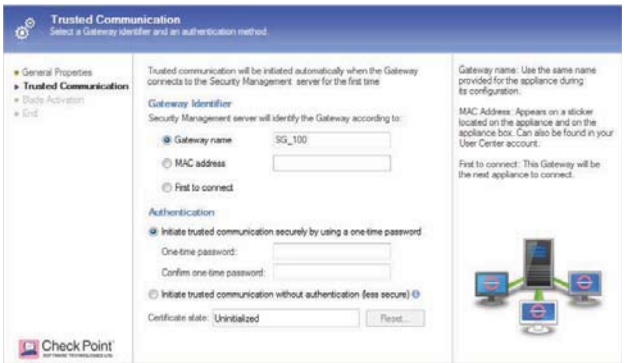
Note - For your convenience, if the gateway name matches, the Security Management Server will identify the gateway regardless of its MAC address.

b) In the Authentication section, select one of the options:

- **Initiate trusted communication securely by using a one-time password** - the one-time password is used to authenticate communication between the Security Gateway and the Security Management server in a secure manner.
  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

- **Initiate trusted communication without authentication (less secure)** - select this option only if you are sure there is no risk of malicious behavior (for example, when in a lab setting).



Trusted Communication

Select a Gateway identifier and an authentication method

Trusted communication will be initiated automatically when the Gateway connects to the Security Management server for the first time

Gateway Identifier

Security Management server will identify the Gateway according to:

● Gateway name: SG_100

○ MAC address:

○ First to connect

Authentication

● Initiate trusted communication securely by using a one-time password

One-time password:

Confirm one-time password:

○ Initiate trusted communication without authentication (less secure)

Certificate state: Uninitialized

Gateway name: Use the same name provided for the appliance during its configuration.

MAC Address: Appears on a sticker located on the appliance and on the appliance box. Can also be found in your User Center account.

First to connect: This Gateway will be the next appliance to connect.

Click **Next**.

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

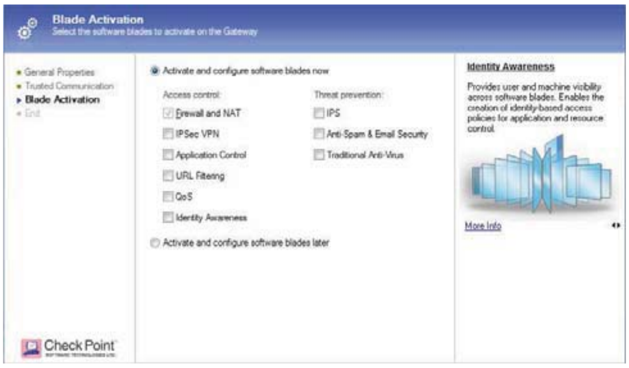
   To configure blades now:

   a) Make sure that the **Activate and configure software blades now** option is selected.

   b) Select the check boxes next to the blades you want to activate and configure.

   To configure blades later:

- Select the **Activate and configure software blades later option**. Do this later by editing the object from the Network Objects tree.



Blade Activation
Select the software blades to activate on the Gateway

- General Properties
- Trusted Communication
- Blade Activation
- End

● Activate and configure software blades now

Access control:
☑ Firewall and NAT
□ IPSec VPN
□ Application Control
□ URL Filtering
□ QoS
□ Identity Awareness

Threat prevention:
□ IPS
□ Anti-Spam & Email Security
□ Traditional Anti-Virus

○ Activate and configure software blades later

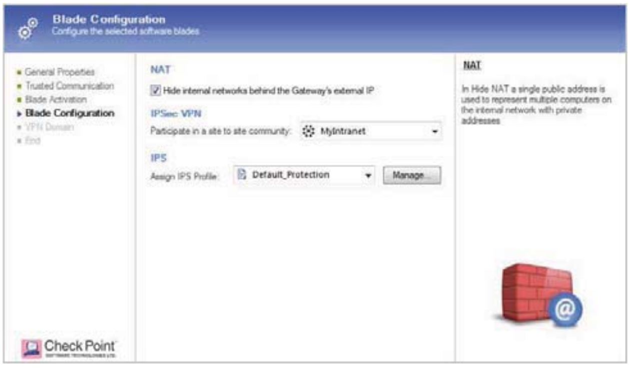
Identity Awareness
Provides user and machine visibility across software blades. Enables the creation of identity-based access policies for application and resource control.

Click **Next**.

9. If you selected to activate and configure software blades now, configure the required options:

   - **For NAT,** the **Hide internal networks behind the Gateway's external IP** checkbox is selected by default. Clear it, if you do not want to use this feature.
   - **For IPSec VPN**: Make sure that the VPN community has been predefined. If it is a star community, Check Point 1100 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.
   - **For IPS**:
     - Select a profile from the **Assign IPS Profile** list or click **Manage** to create/edit an IPS profile.
   - **For Identity Awareness**:
     - Complete the wizard that opens to define the Identity Awareness acquisition sources.
       To configure acquisition sources at a later time, click **Cancel** in the wizard. After you define the Check Point 1100 Appliance object, you can configure Identity Awareness acquisition sources by editing the Check Point 1100 Appliance object.

- **For Application Control, URL Filtering, Anti-Spam and Email Security, and Traditional Anti-Virus**, there are no other settings to configure.



Blade Configuration
Configure the selected software blades

NAT

☑ Hide internal networks behind the Gateway's external IP

IPSec VPN

Participate in a site to site community: MyIntranet

IPS

Assign IPS Profile: Default_Protection

NAT

In Hide NAT a single public address is used to represent multiple computers on the internal network with private addresses

Click **Next**.

10. If you selected IPSEC VPN, configure VPN Encryption Domain settings.

    - To hide the VPN domain, select **Hide VPN domain behind this gateway's external IP**.

      The VPN domain contains network objects behind this gateway. Instead of defining the network topology behind this gateway, it is possible to use this option, which sets the VPN domain to be this gateway's external IP address. This option is only applicable if you chose to hide all internal networks behind this gateway's external IP (see gateway's NAT settings). All outgoing traffic from networks behind this gateway to other sites that participate in VPN community will be encrypted (including replies, of course).

      Note - If you choose this option, connections that are initiated from other sites that are directed to hosts behind this gateway will **not be encrypted**. If you require access to hosts behind this gateway, either choose other options (define VPN topology) or, if possible, 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, go to step 11.
    - To select a predefined VPN domain, go to step 12.

11. To create a new VPN domain group:

a) Make sure that the **Create a new VPN domain** option is selected.

b) In the **Name** field, enter a name for the group.

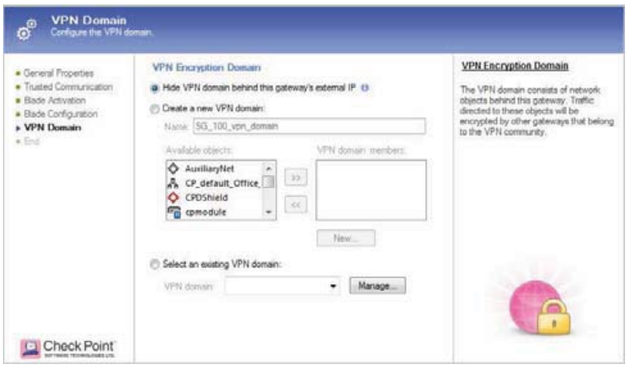
c) From the **Available objects** list, select the applicable object(s) and click >>. The objects are added to the VPN domain members list.

d) If necessary, create a new object by pressing **New**.

12. To select a predefined VPN domain:

a) Choose the **Select an existing VPN domain** option.

b) From the **VPN Domain** list, select the domain.



VPN Encryption Domain

● Hide VPN domain behind this gateway's external IP

○ Create a new VPN domain:

Name: SG_100_vpn_domain

Available objects: AuxiliaryNet, CP_default_Office_, CPDShield, cpmodule

VPN domain members:

○ Select an existing VPN domain:

VPN domain:

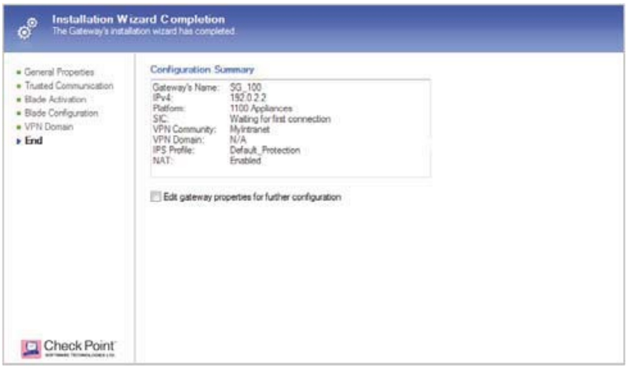
VPN Encryption Domain

The VPN domain consists of network objects behind this gateway. Traffic directed to these objects will be encrypted by other gateways that belong to the VPN community.

Click **Next**.

13. In the Installation Wizard Completion page, you see a summary of the configuration parameters you set and can do further actions.

- Select **Edit Gateway properties for further configuration** to configure the Security Gateway. When you click **Finish**, the General Properties window of the newly defined object opens.



Installation Wizard Completion

The Gateway's installation wizard has completed.

Configuration Summary

Gateway's Name:	SG_100
IPv4:	192.0.2.2
Platform:	1100 Appliances
SIC:	Waiting for first connection
VPN Community:	MyIntranet
VPN Domain:	N/A
IPS Profile:	Default_Protection
NAT:	Enabled

□ Edit gateway properties for further configuration

Click **Finish**.

Preparing to Install the Security Policy

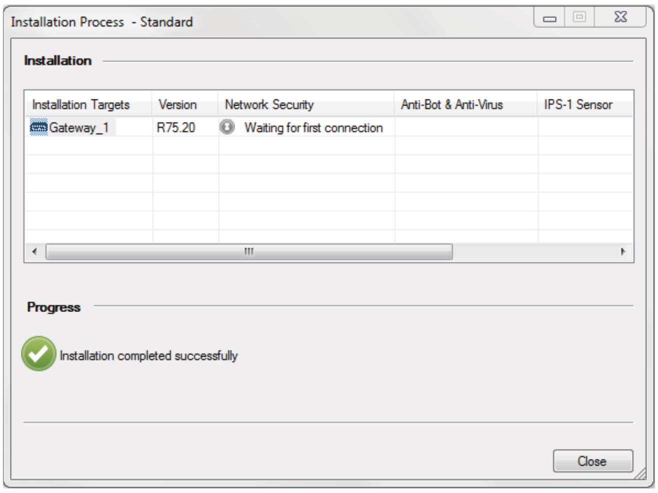
Use this procedure to prepare the policy for automatic installation when the gateway connects.

1. Click **Policy** > **Install** from the menu.
2. In the Install Policy window, choose:
   - The installation targets - the Check Point 1100 Appliance Security Gateways on which the policy should be installed
   - The policy components (Network Security, QoS, etc.).

   By default, all gateways that are managed by the Security Management server are available for selection.
3. In the Installation Mode section, 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
4. Click **OK**. The Installation Process window shows the status of the Network Security policy for the selected target.

Important - If you used the Management First configuration option:

- The Check Point 1100 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". This means that the policy is successfully *prepared* for installation. 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.



Installation Process - Standard

Installation

Installation Targets	Version	Network Security	Anti-Bot & Anti-Virus	IPS-1 Sensor
Gateway_1	R75.20	Waiting for first connection		

Progress

✓ Installation completed successfully

Note - If you used the Gateway First configuration option:

- Upon successful completion of this step, the policy is pushed to the Check Point 1100 Appliance.
- For a list of possible statuses, see Viewing the Policy Installation Status (on page 61).

Continue tracking the status of the security policy installation with the Policy Installation Status window and the status bar ("Viewing the Policy Installation Status " on page 61).

Setting Up the Check Point 1100 Appliance

1. Remove the Check Point 1100 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

To connect the cables on Check Point 1100 Appliance models:

1. Connect the power supply unit to the appliance and to a power outlet. The appliance is turned on once the power supply unit is connected to an outlet. The Power LED on the front panel turns on. This indicates that the appliance is turned on. The Notice LED on the front panel starts blinking. This indicates that the appliance is booting up. When the Notice LED turns off, the appliance is ready for login.
2. Connect the standard network cable to the network interface port (LAN1) on the appliance and to the network adapter on your PC.
3. Connect another standard network cable to the WAN interface on the appliance and to the external modem, external router, or network point (in ADSL models, connect a telephone cable to the ADSL port).

Using the First Time Configuration Wizard

Configure Check Point 1100 Appliance with the First Time Configuration Wizard.

During the wizard, click **Quit** to save the settings that have been configured and close the wizard.

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 1100 Appliance model and the options you select.

Starting the First Time Configuration Wizard

To configure the Check Point 1100 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, the wizard will run again the next time you connect to the appliance. This can occur if one of these conditions applies:

- You have not completed the wizard.
- The browser window is closed.
- The appliance is restarted while you run the wizard.
- There is no activity for a predefined amount of time (the default is 10 minutes).

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

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

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

If a security warning message is shown, confirm it and continue. For more details, see Appendix A: Browser Security Warnings (on page 59).

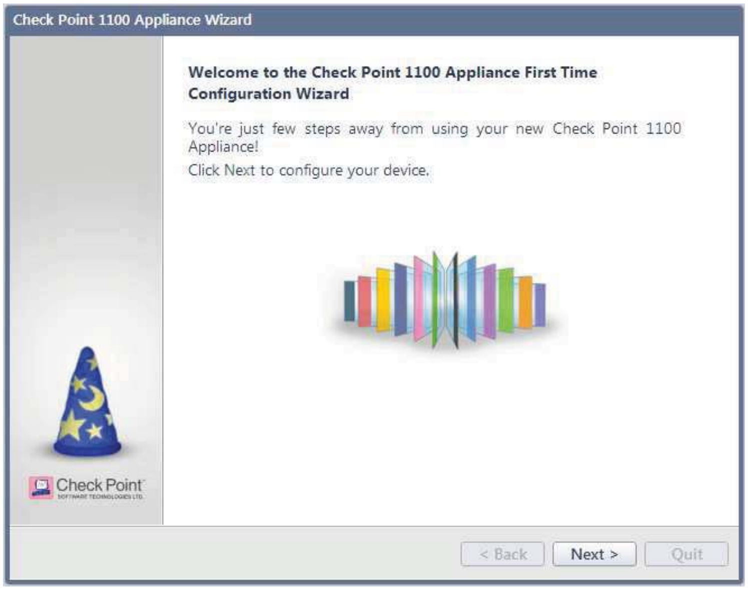
To start the First Time Configuration Wizard:

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

The **First Time Configuration Wizard** runs.

Welcome

The **Welcome** page introduces the product.



Welcome to the Check Point 1100 Appliance First Time Configuration Wizard

You're just few steps away from using your new Check Point 1100 Appliance!

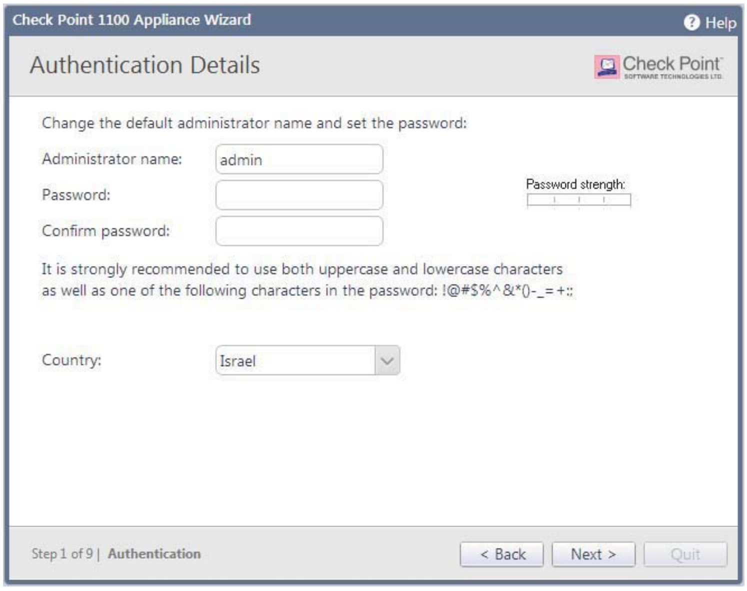
Click Next to configure your device.

Authentication Details

In the **Authentication Details** page, enter these details necessary for logging in to the Check Point 1100 Appliance WebUI application or if the wizard terminates abnormally:

- **Administrator Name -** We recommend that you change the default "admin" login name of the administrator. The name is case sensitive.
- **Password -** You can use the **Password strength** meter to measure the strength of your password. This meter is only used as an indicator and does not enforce creation of a password with a specified number of characters or character combination.

  The minimum length for a strong password is 6 characters that contain at least one capital letter, one lower case letter and a special character. If you specify such a password, a green bar in the last section of the meter will appear. It is strongly recommended to create a password using both uppercase and lowercase letters.
- **Confirm Password -** Retype the password.
- **Country** - Select a country from the list (for wireless network models).



Authentication Details

Change the default administrator name and set the password:

Administrator name: admin

Password:

Confirm password:

It is strongly recommended to use both uppercase and lowercase characters as well as one of the following characters in the password: !@#$%^&*()-_=+:;

Country: Israel

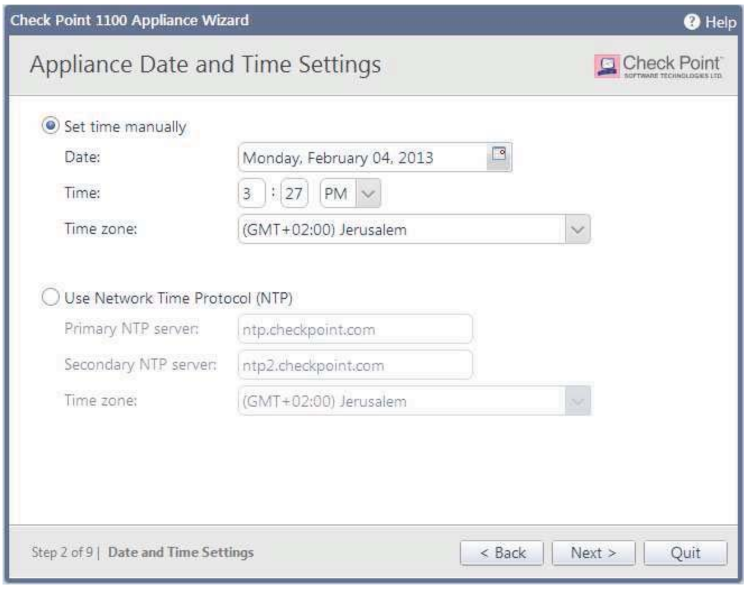
Step 1 of 9 | Authentication

Appliance Date and Time Settings

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

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

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


Check Point 1100 Appliance Wizard
Help
Check Point SOFTWARE TECHNOLOGIES LTD.
< Back
Next >
Quit

Appliance Date and Time Settings

● Set time manually

Date: Monday, February 04, 2013

Time: 3 : 27 PM

Time zone: (GMT+02:00) Jerusalem

○ Use Network Time Protocol (NTP)

Primary NTP server: ntp.checkpoint.com

Secondary NTP server: ntp2.checkpoint.com

Time zone: (GMT+02:00) Jerusalem

Step 2 of 9 | Date and Time Settings

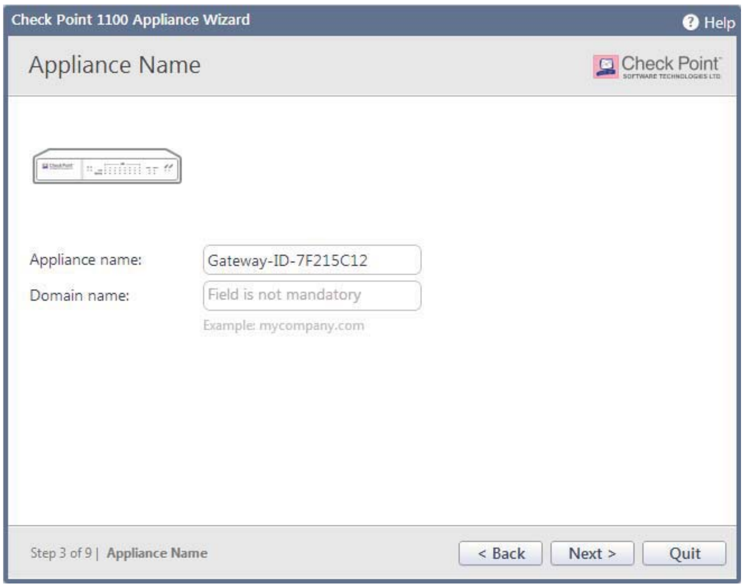
Appliance Name

In the **Appliance Name** page, enter a name for the appliance that is used to identify the Check Point 1100 Appliance and a domain name.

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

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

- When Check Point 1100 Appliance does not use a static IP and the unique identifier for the gateway in SmartDashboard is set to use the Gateway name.
- When Check Point 1100 Appliance is managed through SmartProvisioning.



Check Point 1100 Appliance Wizard

Appliance Name

Appliance name: Gateway-ID-7F215C12

Domain name: Field is not mandatory

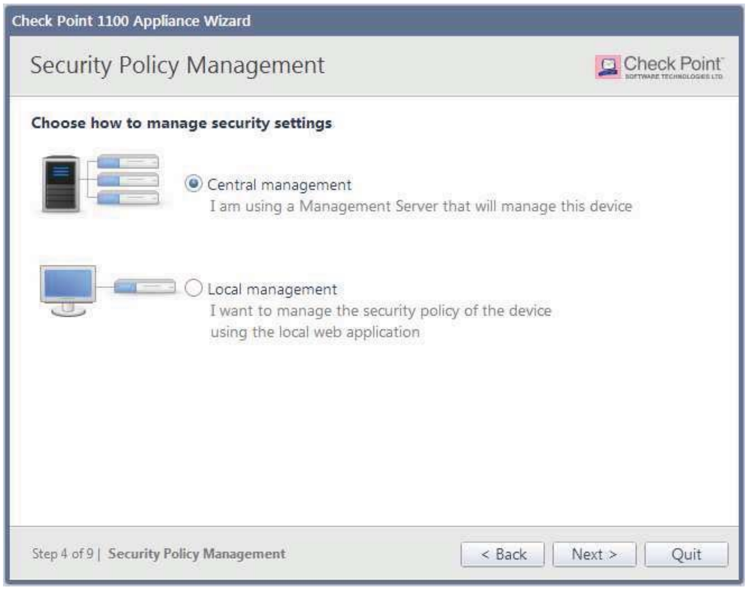
Example: mycompany.com

Step 3 of 9 | Appliance Name

Security Policy Management

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

- **Central management** - The Check Point 1100 Appliance is only a Security Gateway. It is managed by a remote Security Management Server that defines the gateway object and the security policy. The WebUI is used only for configuring the appliance.
- **Local management** - The Check Point 1100 Appliance is a Security Gateway and uses the appliance's WebUI for local management. The WebUI manages the security policy that Check Point 1100 Appliance enforces and activated software blades.



Check Point 1100 Appliance Wizard

Security Policy Management

Choose how to manage security settings

● Central management
I am using a Management Server that will manage this device

○ Local management
I want to manage the security policy of the device using the local web application

Step 4 of 9 | **Security Policy Management**

Internet Connection

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

To configure Internet connection now:

1. Select **Configure Internet connection now**.
2. From the **Connection Protocol** drop down list, select the protocol used for connecting to the Internet.
3. Fill in the fields for the selected connection protocol. The information you must enter is different for each protocol. You can get it from your Internet Service Provider (ISP).
   - **Static IP** - A fixed (non-dynamic) IP address.
   - **DHCP** - Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses within a specified range to devices on a network. This is a common option when you connect through a cable modem.
   - **PPPoE (PPP over Ethernet)** - A network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks.
   - **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
   - **L2TP** - Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself. It relies on an encryption protocol that it passes within the tunnel to provide privacy.
   - **Cellular Modem** - Connect to the Internet using a wireless modem to a cellular ISP.
   - **Analog Modem** - Connect to the Internet using an analog modem.
   - **ADSL** - Connect to the Internet using ADSL.
   - **Bridge** - Connects multiple network segments at the data link layer (Layer 2).
4. In the **DNS Server** field (shown for Static IP and Bridge connections), enter the DNS server address information in the relevant fields. For DHCP, PPPoE, PPTP, L2TP, ADSL, Analog Modem, and Cellular Modem, the DNS settings are supplied by your service provider. You can override these settings later in the WebUI application under the Device > DNS page.

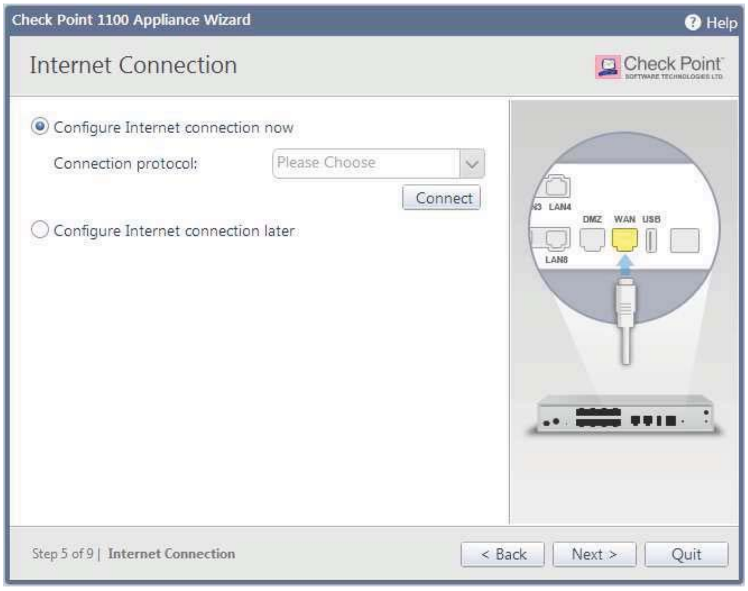
   It is recommended to configure the DNS since Check Point 1100 Appliance needs to perform DNS resolving for different functions. For example, for connecting to Check Point User Center during license activation or when Application Control, Web Filtering, Anti-Virus or Anti-Spam services are enabled.

5. Select **Monitor connection status** to let the appliance probe for Internet connectivity. It is possible to get an IP address from your ISP without the capability to connect to the Internet. This option verifies that you have connectivity. You can change this setting later in the WebUI.
6. Click **Connect** to connect to your ISP now and test you connection's status. If you selected **Monitor connection status**, the gateway starts probing the Internet once the connection is up. The probing status is available in the WebUI.

Indication regarding success or failure of the connection appears at the bottom of the page.

To configure the Internet connection at a later time:

Select **Configure Internet connection later**.



Check Point 1100 Appliance Wizard

Internet Connection

● Configure Internet connection now

Connection protocol: Please Choose

○ Configure Internet connection later

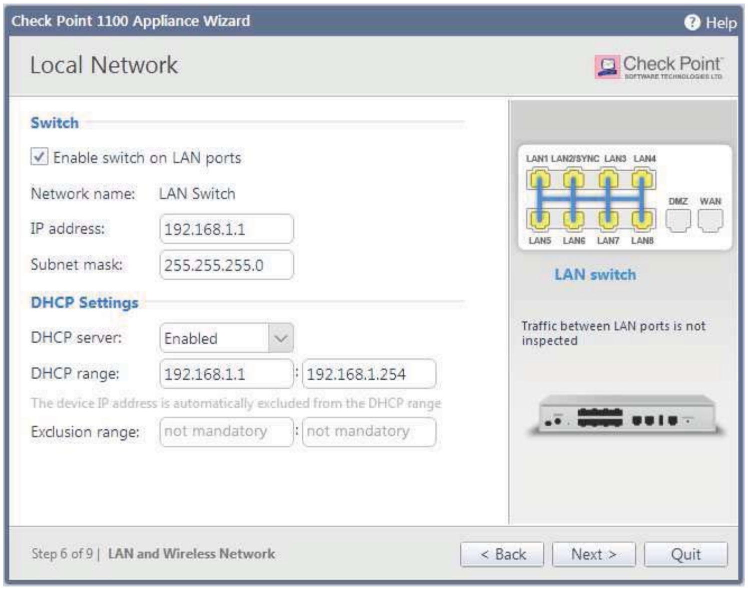
Step 5 of 9 | Internet Connection

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.

Note - 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.



Local Network

Switch

☑ Enable switch on LAN ports

Network name: LAN Switch

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

DHCP Settings

DHCP server: Enabled

DHCP range: 192.168.1.1 : 192.168.1.254

The device IP address is automatically excluded from the DHCP range

Exclusion range: not mandatory : not mandatory

Traffic between LAN ports is not inspected

Step 6 of 9 | LAN and Wireless Network

Wireless Network (for Wireless Network Models)

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

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

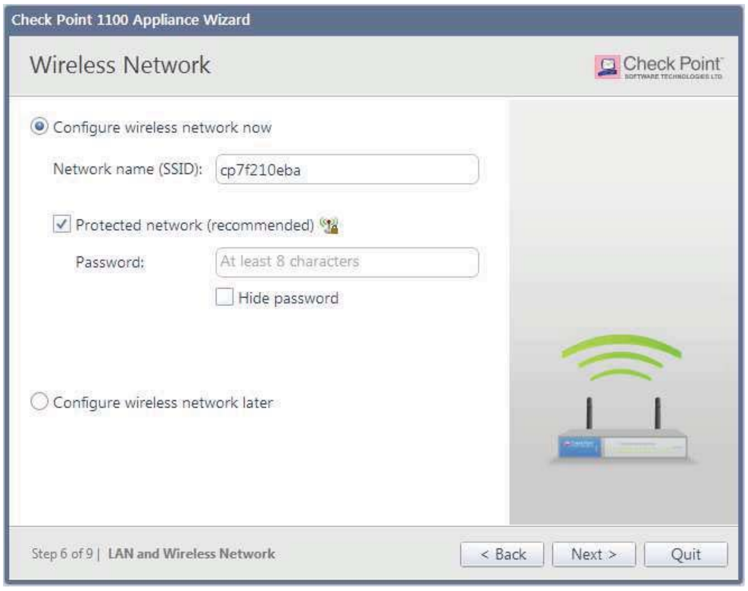
It is recommended to protect the wireless network with a password. Otherwise, a wireless client can connect to the network without authentication.

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.

To configure the wireless network at a different time:

Select **Configure wireless network later**.



Check Point 1100 Appliance Wizard

Wireless Network

● Configure wireless network now

Network name (SSID): cp7f210eba

☑ Protected network (recommended)

Password: At least 8 characters

□ Hide password

○ Configure wireless network later

Step 6 of 9 | LAN and Wireless Network

Administrator Access

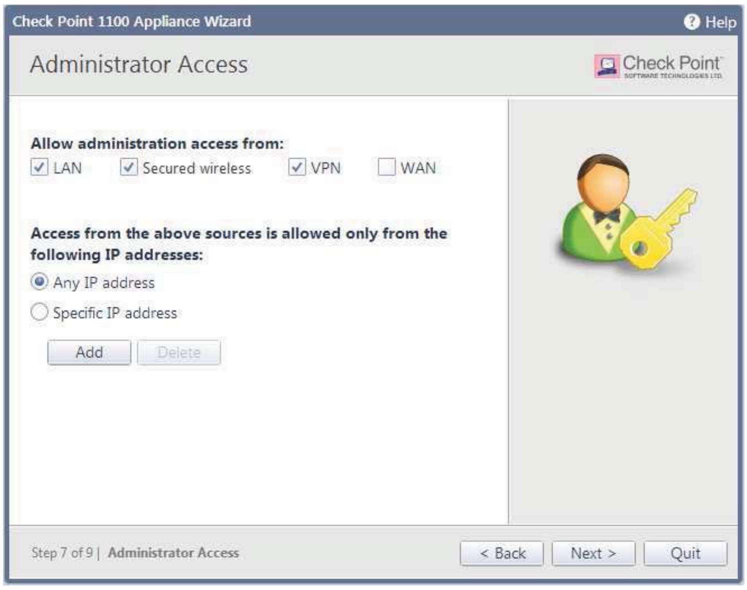
In the **Administrator Access** page, configure if administrators can use Check Point 1100 Appliance from a specified IP address or any IP address.

To configure administrator access:

1. Select from where administrators are allowed access:
   - **LAN -** All internal physical ports
   - **Secured wireless -** Wireless networks with a secure password
   - **VPN -** Using encrypted traffic through VPN tunnels from a remote site or using a remote access client
   - **WAN -** Clear traffic from the Internet (not recommended)
2. Select the IP address that the administrator can access Check Point 1100 Appliance from:
   - **Any IP address**
   - **Specific IP address** - Click **Add** to configure the IP address information.

   a) In the IP Address Configuration window, select an option:
      - **Specific IP address** - Enter the IP address or click **Get IP from my computer**.
      - **Specific network** - Enter the network address and subnet mask.

b) Click **Apply**.



Check Point 1100 Appliance Wizard

Administrator Access

Allow administration access from:

☑ LAN ☑ Secured wireless ☑ VPN □ WAN

Access from the above sources is allowed only from the following IP addresses:

● Any IP address

○ Specific IP address

Step 7 of 9 | Administrator Access

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 are working offline while configuring the appliance:

1. From a computer with authorized access to the Check Point User Center (http://supportcenter.checkpoint.com) do procedure a or b:

   a) Use your User Center account:

   - Log into your User Center account.
   - Select the specified container of your Check Point 1100 Appliance.
   - From the **Product Information** tab, click **License** > **Activate**. This message is shown: "Licenses were generated successfully."
   - Click **Get Activation File** and save the file locally.

   b) Register your appliance:

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

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

   The Import from File window opens.

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

   You 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:

1. Click **Set proxy**.

2. Select **Use proxy server** and enter the proxy server **Address** and **Port**.
3. Click **Apply.**
4. Click **Activate License.**

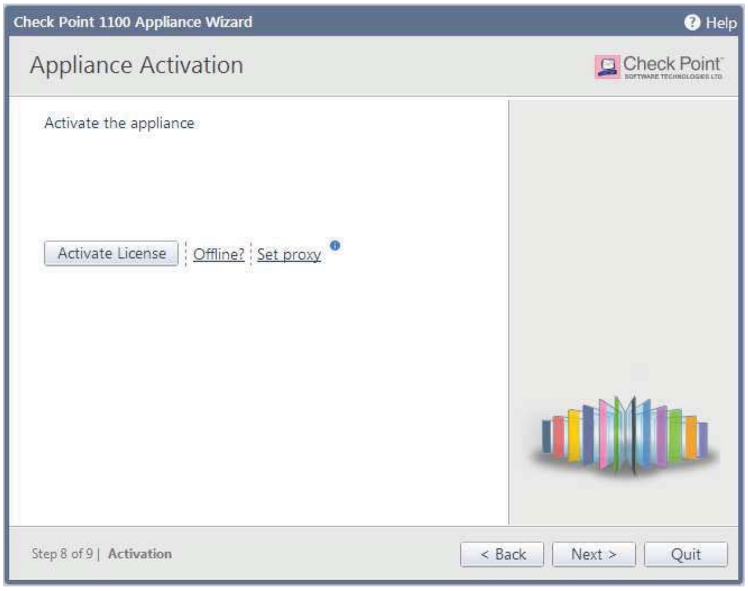
   You will be notified that you successfully activated the appliance and you will be shown the status of your license for each blade.

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

1. Click **Next**.

   The License activation was not complete notification message is shown.
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.


Check Point 1100 Appliance Wizard

Appliance Activation

Activate the appliance

Step 8 of 9 | Activation

Centrally Managed - Security Management Server Authentication

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

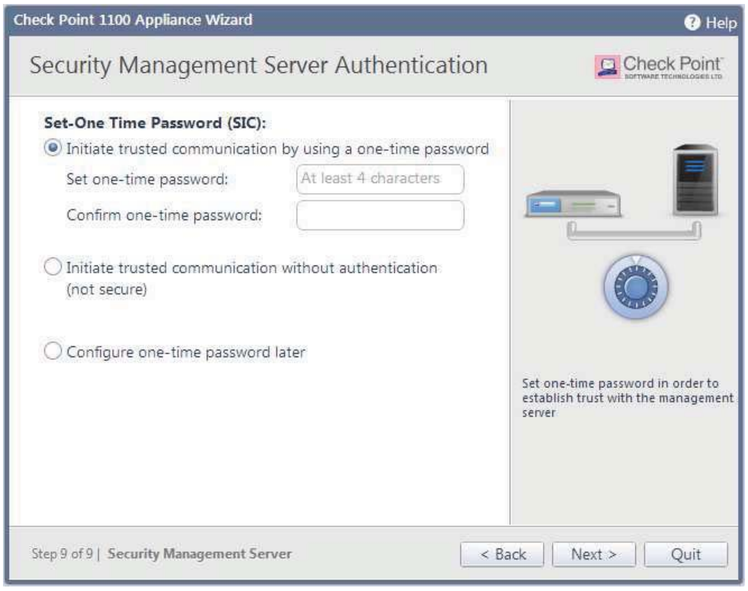
Use this page to select an option to authenticate trusted communication with the Security Management Server:

- **Initiate trusted communication securely by using a one-time password** - The one-time password is used to authenticate communication between Check Point 1100 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 1100 Appliance object in the SmartDashboard of the Security Management server (see step 6 ("Defining the Object in SmartDashboard " on page 17)).

- **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.



Check Point 1100 Appliance Wizard

Security Management Server Authentication

Set-One Time Password (SIC):

● Initiate trusted communication by using a one-time password

Set one-time password: At least 4 characters

Confirm one-time password:

○ Initiate trusted communication without authentication (not secure)

○ Configure one-time password later

Set one-time password in order to establish trust with the management server

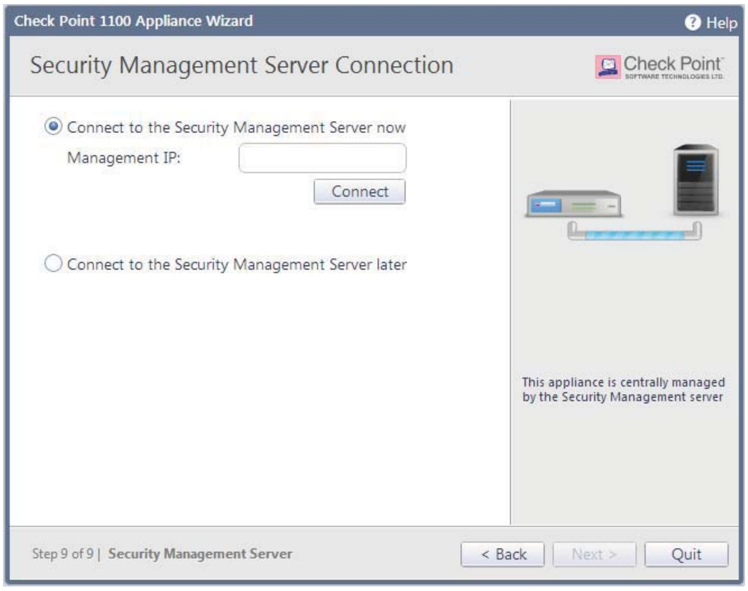
Step 9 of 9 | Security Management Server

Centrally Managed - Security Management Server Connection

After setting a one-time password for the Security Management Server and the Check Point 1100 Appliance, you can connect to the Security Management Server to establish trust with between the Security Management Server and Check Point 1100 Appliance.

Use this page to setup the connection:

- **Connect to the Security Management Server now** - Select this option to connect to the Security Management Server now.
  - **Management IP** - Enter the IP address of the Security Management Server.
  - **Connect** - Upon successful connection to the Security Management Server, the security policy will automatically be fetched and installed.
- **Connect to the Security Management Server later** - Select this option to connect to the Security Management Server later.



Check Point 1100 Appliance Wizard

Security Management Server Connection

● Connect to the Security Management Server now

Management IP:

○ Connect to the Security Management Server later

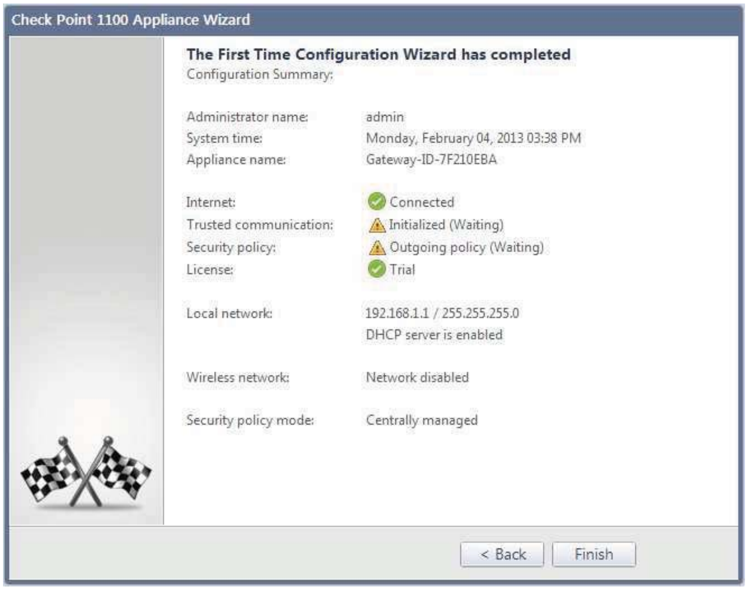
This appliance is centrally managed by the Security Management server

Step 9 of 9 | Security Management Server

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.



Check Point 1100 Appliance Wizard

The First Time Configuration Wizard has completed

Configuration Summary:

Administrator name:	admin
System time:	Monday, February 04, 2013 03:38 PM
Appliance name:	Gateway-ID-7F210EBA
Internet:	✓ Connected
Trusted communication:	⚠ Initialized (Waiting)
Security policy:	⚠ Outgoing policy (Waiting)
License:	✓ Trial
Local network:	192.168.1.1 / 255.255.255.0 DHCP server is enabled
Wireless network:	Network disabled
Security policy mode:	Centrally managed

Note - You should back up the system configuration in the WebUI. Go to the **Device** > **Backup** page.

Large-scale Deployment

Predefining a Centrally Managed Deployment

To manage the Check Point 1100 Appliance in a centrally managed deployment, you must install a Security Management Server and SmartConsole clients that operate with Check Point 1100 Appliance.

The Security Management Server versions that operate with Check Point 1100 Appliance are versions R75.46, R76 and higher.

For installation instructions, see the version’s release notes (http://supportcenter.checkpoint.com).

After installing the SmartConsole clients you can define the Check Point 1100 Appliance object in SmartDashboard and prepare the security policy (in small-scale deployments) or create a SmartLSM profile (in large-scale deployments).

Defining a SmartLSM Profile

SmartLSM lets you manage a large number of Check Point 1100 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.

Use SmartDashboard to define a single SmartLSM profile for Check Point 1100 Appliance.

To define a single SmartLSM profile Check Point 1100 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 1100 Appliance SmartLSM Security Gateways.
3. From the Network Objects tree, right-click **Check Point** and select **SmartLSM Profile > 80 Series 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.

Deploying with SmartProvisioning

You can use SmartProvisioning to manage many Check Point 1100 Appliance gateway objects with deployed SmartLSM security profiles. Configure these appliances using the First Time Configuration Wizard (on page 27) or a USB drive configuration file . For more information about the USB drive configuration file, see the *Check Point 1100 Appliance Administration Guide*.

For more information about large-scale deployment using SmartProvisioning, see the *SmartProvisioning Administration Guide*.

Chapter 3

Check Point 1100 Appliance Hardware

In This Chapter

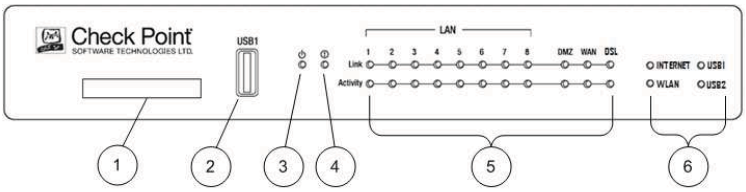
There are four Check Point 1100 Appliance models:

- Wired
- Wireless Network
- ADSL
- Wireless Network + ADSL

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

Front Panel

Wireless Network + ADSL Model

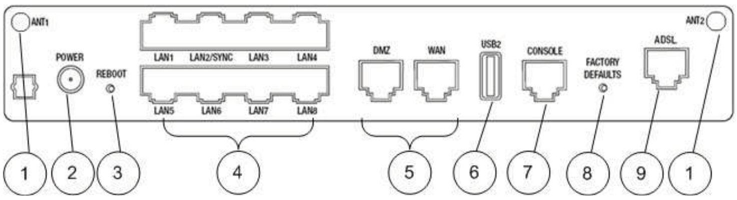


Key	Item	Description
1	Express Card	Express card slot that is used for cellular modems in Express Card form factor.
2	USB1 port	USB1 port that is used for: • Cellular and analog modems. • External storage devices (for example to save traffic logs). • Reinstalling the appliance with new firmware. • Running a first-time configuration script.
3	Power LED	Green when the appliance is turned on.
4	Notice LED	• Blinking green during boot. • Red when the appliance has a resource problem such as memory shortage.
5	LAN1 - LAN8, DMZ, WAN LEDs	Link Indicator • Orange when the port speed is 1000 Mbps. • Green when the port speed is 100 Mbps. • Not lit when the port speed is 10 Mbps. Activity Indicator • Blinking green when encountering traffic.

Key	Item	Description
	DSL LED	Link Indicator • Green when DSL connection is established. • Blinking green when establishing a DSL connection. • Not lit when DSL connection is not established. Activity Indicator • Blinking green when encountering traffic. • Not lit when the DSL line is idle. (Only in ADSL and Wireless Network + ADSL models)
6	Internet LED	• Green when connected to the Internet. • Blinking red when the Internet connection is configured but fails to connect.
	WLAN LED	Blinking green when encountering traffic. (Only in Wireless Network and Wireless Network + ADSL models)
	USB1, USB2 LEDs	Orange when a USB device is connected.

Back Panel

Wireless Network + ADSL Model



Key	Item	Description
1	ANT1 and ANT2	Ports for attaching wireless network antennas. (Only in Wireless Network and Wireless Network + ADSL models)
2	Power outlet	Connects to the power supply unit's cable.
3	Reboot button	Lets you forcibly reboot the appliance. The button is recessed into the appliance chassis to prevent accidental reboot. The appliance reboots immediately after you press the button.
4	LAN1 - LAN8 ports	Built in Ethernet ports.
	LAN2/SYNC port	In a cluster configuration, you must connect a cable between this port on both appliances that take part in the cluster. You can configure the cluster sync port to a port other than LAN2.
5	DMZ and WAN ports	Built in Ethernet ports.
6	USB2 port	Second USB port. Same functionality as the USB1 port on the Front Panel.
7	Console port	Serial connection configured in 115200 bps. You can also use this port to connect an analog modem.

Key	Item	Description
8	Factory Defaults 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 54).
9	ADSL port	Port for attaching ADSL cable. (Only in ADSL and Wireless Network + ADSL models)

Restoring Factory Defaults

The Check Point 1100 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 1100 Appliance to its factory default settings if necessary.

You can restore a Check Point 1100 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 as explained in the *Check Point 1100 Appliance Quick Start Guide*.

To restore factory defaults with the WebUI:

1. In the Check Point 1100 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 defaults button with a pin and hold it for at least 3 seconds.
2. When the Power and Notice LEDs are lit red, release the button. The appliance reboots itself and starts to restore factory defaults immediately.
3. While factory defaults are being restored, all LAN Link and Activity LEDs blink orange and green alternately to show progress.

   This takes some few minutes. When this completes, the appliance reboots automatically.

To restore the Check Point 1100 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 Secure Platform Embedded Boot Menu is shown.

   ```
   Welcome to SecurePlatform Embedded Boot Menu:
   1. Start in normal Mode
   2. Start in debug Mode
   3. Start in maintenance Mode
   4. Restore to Factory Defaults (local)
   5. Install/Update Image/Boot-Loader from Network
   6. Install/Update Image from USB
   7. Install/Update Boot-Loader from USB
   8. Restart Boot-Loader
   Please enter your selection :
   ```
3. Enter **4** to select **Restore to Factory Defaults (local)**.
4. When you are prompted: "Are you sure? (y/n)" choose **y** to continue and restore the appliance to its factory defaults settings.

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

Chapter 4

Support and Further Information

In This Chapter

Support

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

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

Where To From Here?

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

For more information about the Check Point Check Point 1100 Appliance and links to the administration guides, see the Check Point site (http://www.checkpoint.com/CP1100).

Be sure to also use our Online Help when you operate the Check Point 1100 Appliance WebUI and with Check Point SmartConsole clients.

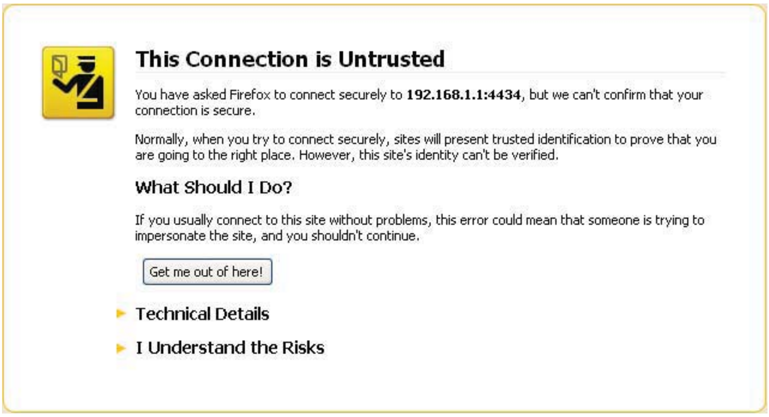
Chapter 5

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



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.1.1:4434**, but we can't confirm that your connection is secure.

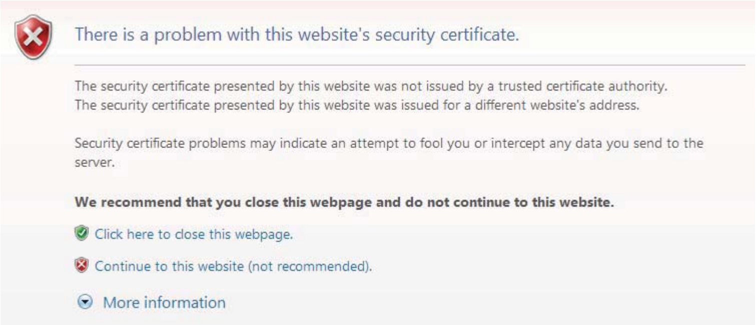
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

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

Internet Explorer



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

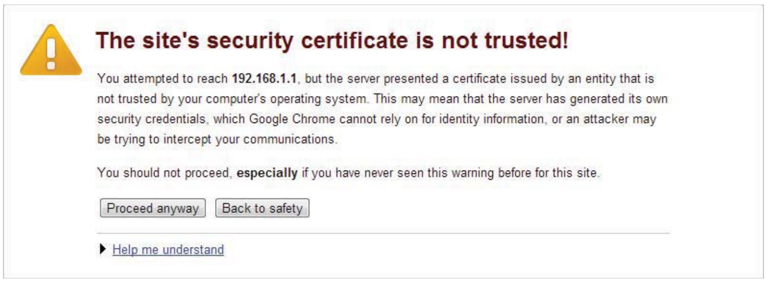
Click here to close this webpage.

Continue to this website (not recommended).

More information

Click **Continue to this website (not recommended)**.

Google Chrome



The site's security certificate is not trusted!

You attempted to reach **192.168.1.1**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Click **Proceed anyway**.

Chapter 6

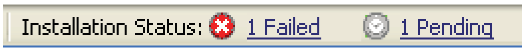
Appendix B: Security Management Issues

In This Chapter

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.



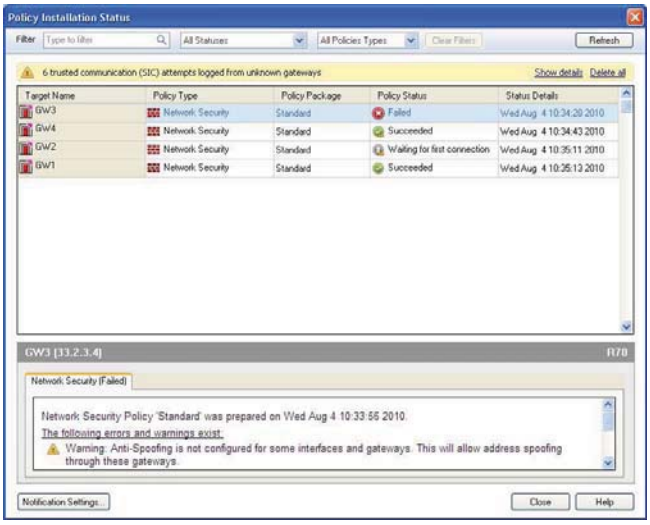
Installation Status: 1 Failed 1 Pending

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 65).

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, clicking **Show details** shows the details of unknown gateways trying to connect to the Security Management Server.



6 trusted communication (SIC) attempts logged from unknown gateways

Target Name	Policy Type	Policy Package	Policy Status	Status Details
GW3	Network Security	Standard	Failed	Wed Aug 4 10:34:20 2010
GW4	Network Security	Standard	Succeeded	Wed Aug 4 10:34:43 2010
GW2	Network Security	Standard	Waiting for first connection	Wed Aug 4 10:35:11 2010
GW1	Network Security	Standard	Succeeded	Wed Aug 4 10:35:13 2010

GW3 [33.2.3.4] R70

Network Security (Failed)

Network Security Policy 'Standard' was prepared on Wed Aug 4 10:33:56 2010.

The following errors and warnings exist:

Warning: Anti-Spoofing is not configured for some interfaces and gateways. This will allow address spoofing through these gateways.

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.

Icon	Policy status	Description
●	Waiting for first connection	When a Check Point 1100 Appliance object has been configured, but initial trust has not been established (the gateway has not yet connected to the Security Management Server). • If a policy has been prepared, upon successful connection, the policy will be pulled. • If a policy *was not prepared*, the Policy Type column shows "No Policy Prepared" and upon first connection only trust is established.
●⚠	Waiting for first connection	Same as above but there are warnings that show attempts to establish trust that failed or there are verification warnings.
🕒	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. 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.
ℹ	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 ℹ
- From the status bar - click on the **Failed** or **Pending** link. The contents of the Policy Installation Status window are shown filtered according to the link clicked.
- From notification balloons - click the **See Details** link in the balloon.

Configuring Notification Settings

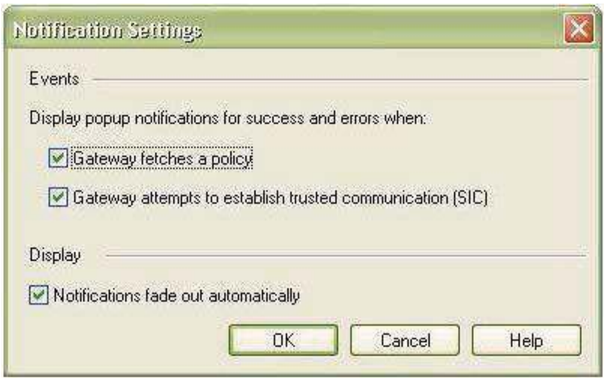
The status bar is updated each time a gateway tries to install a policy or tries to connect to the Security Management Server. You can also configure a popup notification balloon to open in SmartDashboard. You can configure the types of events shown and how notification balloons are shown. By default,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

   Notification Settings

   Events

   Display popup notifications for success and errors when:

   ☑ Gateway fetches a policy

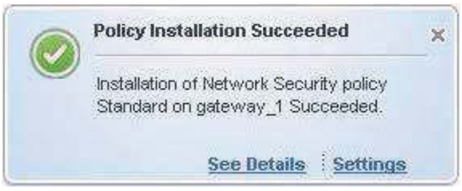
   ☑ Gateway attempts to establish trusted communication (SIC)

   Display

   ☑ Notifications fade out automatically

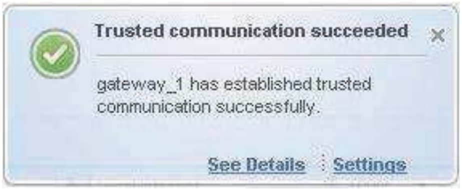
2. To show trials of installing a policy, select **Gateway fetches a policy**.
3. To show trials of connecting to the Security Management Server, select **Gateway attempts to establish trusted communication (SIC)**.
4. To set the notifications to pop-up momentarily in SmartDashboard and then fade out, select **Notifications fade out automatically**.

Note - If you do not select the **Notifications fade out automatically** check box, notifications will stay open until you manually close them.



Policy Installation Succeeded

Installation of Network Security policy Standard on gateway_1 Succeeded.



Trusted communication succeeded

gateway_1 has established trusted communication successfully.

Index

FCC Warning statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more 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.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

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

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. 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.

RF exposure related statements

RF exposure warning: The equipment complies with RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Déclarations d'exposition aux RF liées Avertissement d'exposition RF: L'équipement est conforme aux limites d'exposition aux RF établies pour un environnement non contrôlé. L'antenne (s) utilisée pour ce transmetteur ne doit pas être co-localisés ou fonctionnant en conjonction avec une autre antenne ou transmetteur.

This device complies with Industry Canada licence-exempt RSS standard(s). 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 of the device.

Ce dispositif est conforme à la norme de l'industrie Canada exempts de licence RSS (s). L'opération est soumise aux deux conditions suivantes: (1) Cet appareil ne peut causer d'interférences nuisibles, et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences qui peuvent causer un mauvais fonctionnement de l'appareil.

This equipment complies with Canada 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.

Cet équipement est conforme aux limites Canada exposition aux radiations établies pour un incontrôlés environnement. Cet équipement doit être installé et utilisé avec une distance minimale de 20 centimètres entre le radiateur et votre corps.