CC Evaluated Configuration
Installation Guide for Nokia IPSO 4.2

Part No. N450000685 Rev 001
February 2008
Nokia Contact Information
Corporate Headquarters

**Web Site**  
http://www.nokia.com

**Telephone**  
1-888-477-4566 or  
1-650-625-2000

**Fax**  
1-650-691-2170

**Mail Address**  
Nokia Inc.  
313 Fairchild Drive  
Mountain View, California  
94043-2215 USA

Regional Contact Information

**Americas**  
Tel: 1-877-997-9199  
Outside USA and Canada: +1 512-437-7089  
email: info.ipnetworking_americas@nokia.com

**Europe, Middle East, and Africa**  
Tel: UK: +44 161 601 8908  
Tel: France: +33 170 708 166  
email: info.ipnetworking_emea@nokia.com

**Asia-Pacific**  
Tel: +65 6588 3364  
email: info.ipnetworking_apac@nokia.com

Nokia Customer Support

**Web Site**  
https://support.nokia.com/

**Email**  
tac.support@nokia.com

**Americas Voice**  
1-888-361-5030 or  
1-613-271-6721

**Europe Voice**  
+44 (0) 125-286-8900

**Fax**  
1-613-271-8782  
+44 (0) 125-286-5666

**Asia-Pacific Voice**  
+65-67232999

**Fax**  
+65-67232897
# Contents

1 **Overview** ........................................................................................................................................... 7
   About the Installation Guide .................................................................................................................. 7
   Reference Material ................................................................................................................................. 8

2 **Evaluated Configuration** .................................................................................................................. 9
   Physical Components of the Evaluated Configuration ......................................................................... 9
   Functionality Excluded from the Evaluation .......................................................................................... 11
   Security Environment Considerations ................................................................................................. 14

3 **Secure Delivery Procedures** .......................................................................................................... 16
   Overview ................................................................................................................................................. 16
   Hardware Delivery ................................................................................................................................. 17
     Hardware Platforms ............................................................................................................................... 17
     Hardware Acquisition and Delivery ..................................................................................................... 18
     Nokia Security Appliance Acquisition Guidelines ............................................................................... 18
     Management Platform Acquisition Guidelines ............................................................................... 19
     Hardware Verification Procedure ....................................................................................................... 19
     Environmental Conditions .................................................................................................................. 20
   Software Delivery ................................................................................................................................. 21
     CD Distribution .................................................................................................................................... 21
     Software Delivery Verification ........................................................................................................... 22
     Product Documentation ....................................................................................................................... 23
     Check Point HFA Downloads ............................................................................................................... 23
   License Confirmation and Verification .................................................................................................. 24

4 **Deployment** ....................................................................................................................................... 25
   SmartCenter Server (Management Module) ........................................................................................... 25
   Enforcement Module ............................................................................................................................. 25
   SmartConsole (Management GUI) .......................................................................................................... 26
5 Pre-installation .................................................................................................................. 29

6 Fresh Installation .............................................................................................................. 30
   Overview ............................................................................................................................. 30
   Installing the SmartCenter Server ..................................................................................... 34
     Installing the SecurePlatform Operating System .......................................................... 34
       Operating System Installation ....................................................................................... 34
       Console Login ................................................................................................................ 42
       Sysconfig Wizard ......................................................................................................... 43
     cpconfig .......................................................................................................................... 49
     Installing HFAs (if available) .......................................................................................... 59
   Installation Settings .......................................................................................................... 59
   FIPS Mode Configuration .................................................................................................. 60
   Installing SmartConsole .................................................................................................... 61
     SmartConsole Software Installation .................................................................................. 61
     Installing HFAs (if available) .......................................................................................... 68
   First Time Login and Configuration .................................................................................. 68
     Installation Settings ......................................................................................................... 68
   Security Policy .................................................................................................................... 68
   Initialize SIC trust and Policy Installation ....................................................................... 69
   Installing the Enforcement Module .................................................................................... 70
     IPSO and NGX R65 software installation ....................................................................... 70
       Initial Appliance Configuration ....................................................................................... 70
       Installing IPSO and NGX R65 Software ......................................................................... 71
     cpconfig .......................................................................................................................... 75
     Installing HFAs (if available) .......................................................................................... 76
   Installation Settings .......................................................................................................... 76
   FIPS Mode Configuration .................................................................................................. 78

7 Installation Settings .......................................................................................................... 79
   Extending the Validity Period of a SIC Certificate ............................................................... 80
   Enabling Support for IP Options ....................................................................................... 80
   Scheduling Backups and Restoring from Backup ............................................................... 81
   Configuring OCSP .............................................................................................................. 82
   Configuring SecurID ........................................................................................................... 83
SecureClient Mobile Download .......................................................... 83
Enabling Offline SmartDefense Updates ............................................ 84
Configuring Support for Diffie-Hellman Groups 15-18 ....................... 86

8 First Time Login ................................................................................ 94
SmartCenter Server Fingerprint Verification ....................................... 95
Evaluated Configuration Permissions Profiles .................................... 97
Creating an Authorized Administrator Account ............................... 100
Deleting the cpconfig Administrator ................................................. 100

9 Check Point User Center ................................................................. 104
User Center Registration and Access ................................................. 105
Product Registration .......................................................................... 110
SecureKnowledge Solutions ............................................................... 115
1 Overview

In This Chapter

About the Installation Guide...
Reference Material...

About the Installation Guide

This document describes the delivery and operation procedures that must be implemented by Nokia customers and/or resellers to ensure the secure delivery, installation, generation, and start-up of the product in accordance with the Common Criteria evaluated configuration, as defined in the Nokia Firewall/VPN Appliances Security Target.

The guidelines provided in this document explain how to use the existing installation process to set up Nokia Firewall/VPN Appliances in a manner that is consistent with the evaluated configuration. This guidance must be read in conjunction with the referenced installation and configuration guides, and is written to take account of the specific details and setting that are required to be conformant with the evaluated configuration.

These guidelines and requirements are most often exceptions to the instructions written in the referenced documentation. If a feature or service is listed below, you must configure the mentioned item as described here. If a feature or service is not listed below, configure it as written in the referenced documentation.

If you follow the requirements in this document when setting up and using the system, your configuration will match the evaluated configuration.
1 Overview

Note that legitimate reasons may exist to modify the system setup in ways not described here if that is necessary for the system to fulfill its intended purpose. However, the evaluation results may not apply to such a configuration.

Reference Material

The evaluated configuration is described in:
- Nokia Firewall/VPN Appliances Security Target

The following references provide additional installation on the installation and configuration of Nokia Firewall/VPN Appliances:
- CLI Reference Guide for Nokia IPSO 4.2
- Per-appliance (e.g. IP390) Security Platform Installation Guide

Guidance for post-installation administration is provided in:
- Check Point CC Evaluated Configuration Administration Guide

See the following Check Point documentation provided on the product CD-ROMs for more information on administrating Nokia Firewall/VPN Appliances:
- SmartCenter Administration Guide
- Firewall and SmartDefense Administration Guide
- Virtual Private Networks Administration Guide

Instructions for configuring Diffie Hellman groups 15 through 18 are available in SecureKnowledge solution ID: sk27054 - Defining advanced Diffie-Hellman groups 14-18 for use with IKE.

Note: See 9 - SecureKnowledge Solutions for instructions on how to access Check Point SecureKnowledge solutions.
2 Evaluated Configuration

In This Chapter

Physical Components of the Evaluated Configuration  page 7
Functionality Excluded from the  page 11
Security Environment Considerations  page 14

Physical Components of the Evaluated Configuration

The evaluated configuration includes the following components:

- **Enforcement Module** – Check Point VPN-1 Power/UTM software running on Nokia Firewall/VPN Appliances
- **SmartCenter Server** - management server software installed on a host running the SecurePlatform operating system
- **SmartConsole** – management GUI software installed on a host running a Microsoft Windows operating system. The SmartConsole hardware and operating system are not considered part of the evaluated system – they are installed and configured by the administrator as needed to support the Check Point application.
- **SSL Network Extender** and **SecureClient Mobile** – SSL VPN clients that can be downloaded from the Enforcement Module to the user's workstation.
An evaluated configuration includes one SmartCenter Server, one or more Enforcement Modules, and one or more SmartConsoles.

The evaluated configuration can be configured to interact with the following external entities:

- An authentication server for authenticating single-use passwords:
  - Using the RADIUS protocol; or
  - Using the RSA SecurID protocol
- Certificate Authority and OCSP responders
- CRL Distribution Points for certificate revocation checking:
  - Using the HTTP protocol; or
  - Using the LDAP protocol
- Peer VPN gateways and SecuRemote/SecureClient remote access users authenticating using IKE/IPsec with certificate-based or preshared-secret authentication
- CVP and UFP servers used to provide additional third-party content protection functionality
Functionality Excluded from the Evaluation

Nokia Firewall/VPN Appliances can provide a broad range of services (product types), features and capabilities. Some of these require additional products or licenses to be installed on the appliance and/or on the SmartCenter Server.

This section describes additional features and capabilities that are excluded from the evaluated configuration:

- **Load Sharing (Nokia IPSO Clustering) and High Availability (VRRP)** – Nokia Firewall/VPN Appliances support state synchronization between multiple appliances for automatic failover and load balancing between cluster members. This functionality was not included in the evaluated configuration.

- **SmartUpdate** – SmartUpdate provides a method for software updates as well as license management, allowing the system administrator to track, manage and maintain:
  - Remote upgrades of existing Check Point products
  - New installations of Check Point products on existing Nokia Firewall/VPN Appliances
  - The attachment of product licenses to Nokia Firewall/VPN Appliances

  SmartUpdate is implemented via a Remote Installation daemon that is disabled in the TOE evaluated configuration.

- **OPSEC client APIs** – the SmartCenter Server provides a set of APIs (and corresponding network protocols) for Check Point OPSEC partners that support integration of third-party management products. The OPSEC client APIs are not available in the TOE evaluated configuration.

- **SNMP** – Nokia Firewall/VPN Appliances provide SNMP support for remote management by third-party monitoring systems. This includes an SNMP agent for SNMP v1, v2c, and v3 (USM) protocol versions, as well as a variety of MIBs allowing intuitive and standards-based
support for monitoring device utilization, High Availability, interoperation of devices and Check Point VPN-1 utilization as well as traffic load monitoring. SNMP support is disabled in the TOE evaluated configuration.

- **Nokia Network Voyager** – a comprehensive and secure “Application Operating Environment” for software management on Nokia Firewall/VPN Appliances. This includes Nokia IPSO version inventory management, configuration display and backup, and real-time and historical of system statistics. This interface is not available in the TOE evaluated configuration.

- **CLIs and SSH** - Nokia Firewall/VPN Appliances include CLI interfaces that are used for initial installation and configuration of the appliance, the OS and the software. A CLI is also provided on the SmartCenter Server. The CLI can be accessed from a directly connected console or remotely using the SSH protocol.

  In the evaluated configuration, these CLIs should not be used after this installation stage. All management of the TOE should be performed via the SmartCenter Server and Management GUIs. If the appliance must be reconfigured (e.g. a NIC is added to the appliance), it should be reinstalled to ensure that it remains in a secure configuration.

- **Extended Remote Access VPN Modes** - Nokia Firewall/VPN Appliances support extended VPN modes that solve connectivity issues with remote access clients. The following remote access VPN modes are outside the TOE evaluated configuration:
  
  o **Hybrid mode** - IKE Phase I supports either certificate-based or shared secret-based authentication. Nokia Firewall/VPN Appliances support a hybrid mode for remote access clients where the gateway authenticates using a certificate, and the client authenticates using a single-use or reusable password. Hybrid mode is outside the TOE evaluated configuration.
  
  o **Microsoft IPSec/L2TP clients** – support for Microsoft IPSec/L2TP clients is outside the TOE evaluated configuration.
• **LDAP User Management** – Nokia Firewall/VPN Appliances support the LDAP protocol for managing users on an external LDAP directory server. LDAP User Management requires an additional SmartDirectory license to be installed. User authentication and authorization information is retrieved from the directory over a secure channel. This configuration is not being evaluated and is outside the TOE evaluated configuration.

• **Routing Protocols** – the Nokia IPSO operating system provides robust support for a wide range of dynamic routing protocols. The evaluated configuration requires static routes to be used, and does not include dynamic routing protocols.

• **Transparent Mode** - Nokia Firewall/VPN Appliances allow the administrator to configure pairs of network interfaces in Transparent Mode, such that layer 2 traffic picked up on one interface is transparently forwarded to the paired interface if it is allowed to flow by the Security Policy. Transparent Mode is not being evaluated and is outside the evaluated configuration.

• **DShield Storm Center** - Nokia Firewall/VPN Appliances can be configured to submit rejected traffic logs to a SANS-operated center that collects malicious activity reports from a large number of contributing organizations on the Internet, and correlates these reports to produce block lists for address ranges from which such activity has been identified. The appliances can also be configured to download and apply these block lists. This functionality is excluded from the evaluated configuration and should be disabled by the administrator.

• **Content Inspection** – in addition to providing support for external content inspection servers using the CVP and UFP interfaces, Nokia Firewall/VPN Appliances support an optional IPSO UTM Base Package installation that allows the administrator to enable anti-virus, URL filtering, and anti-spam components on the appliance itself. This add-on functionality is not included in the evaluated configuration.
Security Environment Considerations

The following issues should be taken into account when preparing the security environment for the evaluated configuration:

- **Physical Access Control**: Physical access must be controlled. The SmartCenter Server, SmartConsole workstations, and firewall appliances must be located in secure locations, protected from physical access by unauthorized persons.

- **Attack Resistance**: Nokia Firewall/VPN Appliances have been evaluated as resistant to attacks performed by attackers possessing a moderate (greater than low) attack potential. This is considered appropriate security to process unclassified, or sensitive but unclassified information in the Mission-Critical Categories. Nokia Firewall/VPN Appliances should not be used to provide security in an environment where the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered high.

- **Permitted Applications**: You may not install any general-purpose applications, public data or other capabilities that are outside the evaluated configuration on any firewall or SmartCenter Server host. In particular, you must not install services (e.g. an FTP server) that can be accessed remotely by non-administrative users.

- **Trustworthy Administrators**: Only trustworthy Administrators should receive authorization to manage the evaluated configuration.

- **Traffic Mediation**: A configured firewall shall mediate traffic for at least two networks. You must ensure that all information paths between mediated networks pass through a firewall in the evaluated configuration.

- **Administrative Workstation**: Nokia Firewall/VPN Appliances shall be managed from an administrative workstation, running SmartConsole. Use of CLI or Web interfaces is restricted to product installation. Once the product is operational, the only administrator interfaces used by authorized administrators are the SmartConsole applications.

- **Preventing Access by Untrusted Users**: The following components must be installed on subnets connected to a firewall interface that is
protected by the Security Policy such that they cannot be accessed by untrusted users:

- SmartCenter Server host
- SmartConsole hosts
- An external authentication server that is used to support SecurID single-use authentication, if any.

- **RADIUS servers:** The communication with a RADIUS server if any is protected using a MD5 shared secret. Secrets should be chosen out of a sufficiently large range (at least 16 randomly selected octets) in order to provide protection against exhaustive search attacks. It is also recommended to periodically change these shared secrets, in order to improve resistance to replay attacks.

- **Single-Use Password Authentication:** The evaluated configuration supports authentication of Telnet and FTP users and of SSL VPN users by sending the user-entered username and password using the RADIUS or SecurID protocols to an external authentication server. In the evaluated configuration, this should only be used in conjunction with single-use password mechanisms, e.g. the RSA SecurID hardware or software tokens. Multiple-use passwords are inherently insecure if used over an unencrypted or physically insecure network.

- **Secure Installation Environment:** Nokia Firewall/VPN Appliances are shipped with all software pre-installed. However, if you reinstall the software on the appliance (from the backup CD delivered with the appliance), you must load the software onto a secure FTP server that is connected to the appliance over a physically secure network in order to perform the installation procedure securely.
3 Secure Delivery Procedures

In This Chapter

Overview ........................................ page 16
Hardware Delivery ............................ page 17
Software Delivery .............................. page 21
License Confirmation and Verification .... page 24

Overview

This section provides information on verifying the secure delivery of the Nokia Firewall/VPN Appliances. Product delivery consists of hardware and software components.

Customers order Nokia Firewall/VPN Appliances from Nokia. The appliances are delivered to the customer with all software pre-installed, and a backup copy of the installed software is provided on a CD for backup and reference purposes.

The CD package provided with the appliance also contains the Check Point management software used to manage the appliances and administrator guidance. The management software is installed by the customer on separate commodity hardware platform purchased by the customer directly from the hardware manufacturer.

The customer is then responsible for completing the installation and configuration of the evaluated configuration, as described in this guidance document.
Hardware Delivery

Hardware Platforms

The evaluated configuration includes three types of hardware platforms: appliance platforms, SmartCenter Server platforms, and SmartConsole (Management GUI) platforms. Corresponding VPN-1 Power/UTM NGX R65 software must be installed on each platform.

The customer purchases one or more of the appliance hardware platforms identified in the *Nokia Firewall/VPN Appliances Security Target*. Appliances are delivered to the customer with all software pre-installed.

A separate hardware platform from the list of Check Point SecurePlatform appliances identified in the Security Target should be used for the SmartCenter Server. The customer installs the operating system and software.

One or more SmartConsole hosts should be installed. SmartConsole is installed on a standard PC workstation running a Microsoft Windows operating system. The workstation is not considered part of the Target of Evaluation, and is not specified in the Security Target.

The product supports the following Microsoft Windows operating systems (or later versions thereof):

- Windows 2000 Professional or Server or Advanced Server with Service Pack 3 (SP3) with Q326886 Hotfix
- Windows XP Professional SP2
- Windows Server 2003 (Standard, Enterprise, or Datacenter Edition) SP1

The SmartConsole machine hardware must meet the following minimum requirements:

- Intel Pentium II 300 MHz or equivalent processor
Secure Delivery Procedures

- 100 MB free disk space
- 256 Mbytes RAM
- One network adapter card
- CD-ROM Drive
- 800 x 600 video adapter card

Hardware Acquisition and Delivery

The software depends on the correct operation of the underlying hardware and firmware in order to meet the security requirements of the evaluated configuration. The hardware platforms identified in the Security Target have been vetted for compatibility with these requirements. It is important that the customer ensure that valid hardware has been received.

Nokia Security Appliance Acquisition Guidelines

Nokia Firewall/VPN Appliances are shipped directly from Nokia to the customer. Nokia uses the following authorized carriers:
- Fedex (www.fedex.com)
- UPS (www.ups.com)

These carriers are trusted by Nokia to deliver the products according to Nokia’s specifications and without allowing the integrity of the products to be compromised in transit.

Each of these carriers provides a tracking number that can be used by the customer to track the product from its source to its destination. The customer is notified via a Purchase Order (PO) of the delivery/shipment information, including the specific FedEx or UPS tracking number.
Management Platform Acquisition Guidelines

SecurePlatform and Windows operating systems used for the Check Point management software run on commodity hardware. This is hardware that is used by many organizations, for many purposes. Because of the diversity of the supported hardware platforms, an adversary will not be able to install a Trojan Horse in hardware that is targeted for Check Point software in general, or for a specific customer's organizational border protection devices in particular.

The following are recommendations that can be used to further mitigate the risks of hardware substitution:

- Buy hardware from people you trust. In particular, purchase the hardware directly from the hardware vendor, according to the procedures provided on the hardware vendor’s Web site.
- Prefer new hardware to used or refurbished equipment.
- Attempt to make hardware purchases seem random. If possible, do not identify upfront the purpose for which these platforms are going to be used. Use platform types that have been purchased by your organization for other purposes as well.
- Use reputable commercial carriers to deliver hardware to your organization. Where possible, pick it up yourself.
- Apply physical access controls throughout the hardware platform's lifetime, including any periods of time when the hardware is in storage, before product installation.

Hardware Verification Procedure

Use the following steps to verify that valid hardware has been received:

1. Examine the outside packaging and markings of the delivery container containing the hardware to ensure that it arrived via the contracted commercial carrier from the hardware vendor.
2. Examine the shipping and tracking information available with the package to look for any unexpected information related to the timing and route for the shipment. If there is any doubt about the veracity of
Secure Delivery Procedures

3. Visually examine the hardware platform to determine that it is labeled in accordance with the hardware vendor's standard markings, and that it matches the platform model that was ordered.

4. Nokia appliances are shipped in a carton. Within the carton, the appliance is placed inside an ESD bag, and a foam end cap is placed on each side of the chassis to protect the appliance during shipping. You should examine the carton and the ESD bag for evidence of tampering. Tamper evidence includes tears, scratches, and other irregularities in the packaging. The CDs within the appliance carton should be received in a sealed envelope.

Follow the hardware vendor's guidance to disconnect or disable any wake on LAN (WoL) or other NIC-related remote management functionality.

Environmental Conditions

If the hardware is to be installed in extreme environmental conditions (heat, cold, humidity, power spikes, vibration, etc.), verify that these conditions are compatible with the hardware vendor's specifications.
Software Delivery

CD Distribution

A unique product reference is required to ensure that there is no ambiguity in terms of which instance (i.e. version of the product) is being evaluated, or purchased by the customer.

The software pre-installed on Nokia Firewall/VPN Appliances includes Nokia IPSO and Check Point VPN-1 Power/UTM software.

Nokia IPSO releases are identified by version and build numbers. Version numbers consist of a major version and minor version, e.g. 4.2. Build numbers take the form of a sequentially allocated number and an optional alphabetical qualifier for minor builds, e.g. 051c.

Each release of the VPN-1 Power/UTM product is identified by a unique reference that consists of a release number and (after the initial base release) a hot fix number following the convention: Product Name R## (Release Number) with HFA ## (Hot Fix Number). Each hot fix is assigned an identifier in the form of HFA ##, starting at HFA 01.

The product CD-ROMs, as well as accompanying product documentation, are labeled externally with the Nokia and/or Check Point unique references, as appropriate.

The unique reference for the evaluated configuration is Nokia IPSO 4.2 Build 051C with Check Point VPN-1 Power/UTM NGX R65 HFA 02.

Note: In general, guidance is not reissued for HFAs; therefore, guidance identified as NGX R65 can be used for any NGX R65 HFA.
3 Secure Delivery Procedures

Note: Various Check Point documentation and administrator interfaces refer to the product variously as 'Check Point VPN-1 Power' or 'UTM'. These are different marketing codes for the same product, differing if at all only in licensing restrictions (e.g. number of IP addresses on internal networks). Use the delivery verification procedures described in this chapter to determine that you have received the correct product and version.

Software Delivery Verification

The customer should verify that the software case does not show any signs of tampering.

The CD-ROMs should be labeled as depicted below:
Product Documentation
Product documentation is provided in soft copy on the product CD-ROMs.

Check Point HFA Downloads
As part of Check Point's Common Criteria-evaluated flaw remediation procedures, Check Point publishes updated Hot Fix Accumulators (HFAs) and provides them to customers with a Software Subscription license.


WARNING: HFA downloads are outside the evaluated configuration:

The Common Criteria evaluation was performed on Nokia Firewall/VPN Appliances running VPN-1 Power/UTM NGX R65 HFA 02. HFAs higher than 02 might include changes to the product that violate evaluated security requirements.

However, it should be noted that the Check Point process for implementing and distributing HFAs was included in the evaluation. Given the abovementioned caveat, Check Point does recommend that customers download and install the latest HFA available. This may only be performed during installation; therefore, when a new HFA is published, you must reinstall to apply the HFA.

Download the SecurePlatform HFA (you will be asked to log in to your Check Point User Center account and agree to the Software Subscription Download Agreement. See 9 - User Center Registration and Access for instructions on accessing the Check Point User Center); calculate the MD5 signature for the downloaded file and compare it to the MD5 signature posted on the Check Point Web site. You may also call Check Point to verify the HFA MD5 signature.
License Confirmation and Verification

As part of the configuration procedure of the VPN-1 Power/UTM software, it is necessary for a customer to enter his license details, which define the product purchased to the installation software.

*Chapter 9 - Check Point User Center* provides instructions on how to register to the Check Point User Center and perform license registration. The customer registers the product, using the provided unique certificate key printed on the back of the case containing the purchased product. The Certificate key is a complex combination of alphanumeric and special characters which are not be easily identified via a trial and error process. Once the certificate key has been entered, customers are advised of the product type they have purchased. This is an initial check that the customer is getting the product that he/she intended to purchase.

The permanent license required to install the product is then generated for the customer. Only those features bundled in the license are activated on the installation CD.

**Note:** The evaluated configuration does not cover use of evaluation licenses.
4 Deployment

In This Chapter

- SmartCenter Server (Management Module) page 25
- Enforcement Module page 25
- SmartConsole (Management GUI) page 26

In the context of this evaluation, a distributed deployment is implemented.

You will need to:

- Install a SmartCenter Server;
- Install one or more Nokia Firewall/VPN Appliances (Enforcement Modules);
- Install one or more SmartConsole workstations.

**SmartCenter Server (Management Module)**

The SmartCenter Server is the server used by the system administrator to manage the Security Policy. The databases and policies of the organization are stored on the SmartCenter Server, and are downloaded to the Nokia Firewall/VPN Appliances.

The SmartCenter Server must be installed on a protected subnet that is directly connected to one or more Nokia Firewall/VPN Appliances. The appliances protect the SmartCenter Server from any network access by untrusted users.

**Enforcement Module**

The product is installed in its operational environment in a configuration where IP packets (datagrams) flowing between controlled networks are routed so that they pass through the Enforcement Module. This allows the
Deployment

Enforcement Module to inspect and optionally modify these information flows.

**SmartConsole (Management GUI)**

The evaluated configuration includes three SmartConsole applications that are included on the product CD-ROMs:

- SmartDashboard
- SmartView Tracker
- SmartView Monitor

These applications are installed on standard PC administrator workstations running **Microsoft Windows**, and are used as the only management interface for the operational evaluated configuration. The SmartConsole applications interact with the SmartCenter server.

**Note:** CLI and the CLI and database editing tool are not to be used after installation and generation of the evaluated configuration.
The evaluated configuration includes both local and remote administration:

- **Local administration:** a SmartConsole Management GUI host is directly connected to the SmartCenter Server Local Area Network (LAN);
• **Remote administration**: a SmartConsole host is installed on a protected subnet that is directly connected to a remote evaluated configuration appliance, and an IPSec VPN tunnel with Triple DES encryption is set up between the two evaluated configuration Nokia Firewall/VPN Appliances protecting the management GUI and SmartCenter Server, respectively.

*Note:* The Remote Administration Rule (See *CC Evaluated Configuration Administration Guide*) prevents remote SmartConsole hosts that are not protected as described above from connecting to the SmartCenter Server.

*Note:* Configuration of the VPN community should not be performed via remote administration, since a VPN tunnel is being used to access the SmartCenter Server, and any modification of VPN community settings may cause a break in this connectivity.
Pre-installation

1. Verify IP address allocations, routes, and host names. (Make sure you know what the network looks like.)

2. Confirm that static DNS resolution is working properly. (Make sure you know what DNS names need to be resolved by the firewall and what their addresses are.)

3. If you intend to reinstall the software on Nokia Firewall/VPN Appliances, prepare a FTP server as discussed above in Security Environment Considerations. Load the IPSO image file (ipso.tgz) and the NGX R65 wrapper (.tgz file) on the FTP server.
6 Fresh Installation

In This Chapter

Overview  page 30
Installing the SecurePlatform Operating System  page 34
Installing the SmartCenter Server  page 34
Installing SmartConsole  page 61
Installing the Enforcement Module  page 70

Overview

You must install each separate component on the relevant machine. Install the SmartCenter Server and one or more SmartConsoles. Install one or more enforcement modules.

After you complete installing a SmartCenter Server host or appliance and make it operational in your network, administrators must not log in directly into these hosts, nor use the CLI interfaces.

Some tasks require access to the CLI; in particular, installing patches and hot fixes, adding network interfaces, reconfiguring the network, etc. These tasks are to be performed in the context of a reinstallation, in order to ensure that the evaluated configuration remains in a secure state. It is possible to reinstall each host and appliance separately, without requiring reinstallation of the other hosts.
The installation workflow is described in Figure 1 and detailed below.

**Figure 1 - Installation Flow**

1. Install SmartCenter Server OS
2. Install SmartConsole
3. Initial Appliance Configuration
4. sysconfig
5. cpconfig
6. Installing HFAs (if available)
7. Installation Settings (see Chapter 7)
8. FIPS Mode configuration (see Chapter 8)
9. First Time Login (see Chapter 9)
10. Security Policy (see Administration Guide)
11. Initialize SIC trust Policy > Install...
12. FIPS Mode configuration (see Chapter 8)
13. Evaluated Configuration
The two steps depicted in Figure 1 in green are described in the *CC Evaluated Configuration Administration Guide*. All other steps are described in this document.

Installation on each of these components can be carried out mostly independently, except for the following dependencies (identified in Figure 1 as arrows):

- First Time Login can only be performed in SmartConsole after the SmartCenter Server is installed.

  **Note:** First Time Login must be performed **before** the evaluated configuration is operational, because it involves logging in to the SmartCenter Server console (for deleting the cpconfig administrator account). FIPS Mode on the SmartCenter Server does not prevent the administrator from performing this step.

- Enforcement module (appliance) installation requires an Activation Key for SIC trust establishment. This Activation Key is generated by the SmartCenter Server when the enforcement module object is created via SmartDashboard.

- The evaluated configuration requires a Security Policy to be installed on the enforcement module; policy installation requires that all three components be installed.

The default security policy is restrictive – it does not allow any information flows through the enforcement module. A Security Policy must be installed in order to enable any information flow. The instructions in the *Security Policy* section of the *CC Evaluated Configuration Administration Guide* **must** be followed when defining and installing a Security Policy; a partial or divergent Security Policy might contain exploitable vulnerabilities, or might cause communication failures between the SmartCenter Server and enforcement modules, requiring reinstalliation.
Note: Because FIPS Mode configuration on the enforcement module
disables some cpshell commands, make sure to complete all
installation settings prior to performing FIPS Mode configuration.

The HFA installation steps involve installation of any HFAs higher than
HFA 02 that might be available at the time of installation. Check Point
recommends that such HFAs be installed; however, such HFAs are not
part of the evaluated configuration. See Check Point HFA Downloads for
more details.

The minimal evaluated configuration consists of one of each component.
Once the evaluated configuration is operational, additional SmartConsole
hosts and enforcement modules may be installed and configured:

- Additional SmartConsole hosts are installed as described above,
  except that there is no need to perform First Time Login.

Note: If you intend to install additional SmartConsole hosts,
make sure that they are compatible with the list of GUI
Clients defined in cpconfig on the SmartCenter Server;
once the SmartCenter Server is operational, it is not
possible to add additional GUI Clients.

- Additional enforcement modules may be installed as described
above, after the evaluated configuration is made operational. There
is no need to access the SmartCenter Server console for this
purpose.
Installing the SmartCenter Server

Installing the SecurePlatform Operating System

The installation of the SecurePlatform operating system is the first installation step for the SmartCenter Server.

The SecurePlatform installation process includes an initial installation phase in which the disk is formatted and the operating system is installed, and an initial configuration phase that begins with a reboot of the operating system and a console login, followed by an invocation of the sysconfig command.

Operating System Installation

Follow the steps below to install the SecurePlatform operating system:

1. Insert the VPN-1 Power/UTM with HFA 02 CD1 into the CD drive and reboot. After rebooting, the Welcome to Check Point screen is displayed:

![Welcome to Check Point Screen](image)
2. Select **Enter** to confirm the installation. If you do not press **Enter** within a pre-designated interval, the computer will reboot from the hard disk. Wait while the installation program is loaded. The installation program checks the hardware platform to verify that it is compatible with SecurePlatform hardware requirements. If the hardware is suitable, the **Welcome** menu is displayed:

![Welcome Menu](image)

**Note**: Do **not** continue with the installation if the hardware is found to be unsuitable.

3. The **Welcome** menu allows the administrator to request additional information on identified hardware devices (**Device List**), to install additional hardware drivers from a diskette (**Add Driver**), to abort installation (**Cancel**) or to proceed with normal installation (**OK**).

Driver installation may be required for some hardware platforms, as indicated in the hardware configuration guidance. Only install drivers whose origin and integrity can be verified. This can be determined where the drivers are received directly from the hardware vendor using
verifiable delivery procedures, or by calculating the driver MD5 or SHA-1 hash and verifying it against valid hashes provided by Check Point or by the hardware vendor.

**Note:** In any case, do not install network interface card (NIC) drivers. NIC drivers are critical to the correct operation of the evaluated security functionality; installing unevaluated NIC driver code will take the product outside of its evaluated configuration.

4. When the administrator selects **OK**, the **System Type** window screen appears:

![System Type Window](image.png)

Under the question **What type of system would you like to install?** select the **SecurePlatform** option, then press **OK** for the next step.
5. The **Keyboard Selection** menu is displayed:

![Keyboard Selection Menu]

Select keyboard type by using the up and down arrow keys, then use tab to navigate to the **OK** button and press Enter.
6. On the **Networking Device** menu select the network interface (link) by using the up and down arrow keys, then use tab to navigate to the **OK** button and press Enter. Select the interface of which you will connect to for later management and configuration of your machine. At this step you must be familiar with your network configuration so you will configure the correct network device as your management interface.
7. Once the correct link was selected you will be prompted to enter additional data for the network interface configuration. In the Network Interface Configuration menu, specify the Management Interface IP address, netmask and default gateway of the network interface, and select **OK**.

- **IP address** - The IP address assigned to the network interface.
- **Netmask** – The network mask for the IP address.
- **Default gateway IP** - The IP address of the default Gateway assigned to your machine's IP address.
8. In the **HTTPS Server Configuration** screen de-select **Enable web based configuration** option by pressing the space key, then use tab to navigate to the **OK** button and press Enter:

![](image1.png)

9. The **Confirmation** screen is displayed. Select **OK** to proceed:

![](image2.png)
10. The following installation operations are performed:
   - Hard drive formatting
   - Software package installation
   - Post installation procedures
   This step can take several minutes, after which the **Installation Complete** screen is displayed. Select **OK** to complete the installation:

![Check Point SecurePlatform Installation](image)

11. The system will now reboot. Make sure to remove the CD, or diskette that you used during the installation process. On most systems the CD will be ejected automatically after selecting **OK** in the Installation Complete menu.

12. During the boot process, an option is presented to display a boot menu. There is no need to select this option. If the boot menu is displayed, select the **Start in normal mode** option.
Console Login

13. Login to the SecurePlatform console interface:

- **First Time Login** - If you are logging on for the first time, use admin as both username and password. You will then be prompted to change your password by entering a new password (twice):

![Login Screen](image)

The password must conform to the following operating system-enforced complexity requirements:

- at least 6 characters, in length
- a mixture of alphabetic and numeric characters
- at least four different characters
- does not use simple dictionary words, or common strings such as “qwerty”

**Note**: the password for the admin account is only used for the installation process. Do not perform a console login once the evaluated configuration is operational.
• **Change user name** – the administrator is prompted to select an alternative user name in place of 'admin'. This is optional. Press Enter to skip this step. If entering a new user name, only user names consisting entirely of alphanumeric characters are accepted.

![Login as admin](image)

You must change the default password.

Enter new password:
Enter new password (again):

You may choose a different user name.

Enter new user name: admin123
Your user name has been changed from admin to admin123.

? for list of commands
sysconfig for system and products configuration

[cpmodule]#

**Sysconfig Wizard**

Sysconfig and cpconfig are Check Point utilities used to configure the SecurePlatform operating system and the VPN-1 software, respectively. The first time sysconfig is run after installation, it runs in a wizard mode that guides the administrator through the various menus. It automatically invokes a corresponding cpconfig wizard to configure relevant Check Point products on the machine. Sysconfig and cpconfig can thereafter be run from the cpshell prompt, allowing the administrator to modify the configuration.
14. Run the `sysconfig` command from the console to configure SecurePlatform.:

![](image1.png)

**Note:** Perform first-time configuration in one session. If the configuration session terminates prematurely (e.g. because of session timeout causing forced administrator logout), you may have to reinstall the operating system.

**Note:** The sysconfig command line wizard is further described in the “First Time Setup Using the Command Line” section in the SecurePlatform&SecurePlatformPro document.

As a general rule for Check Point sysconfig and cpconfig utilities, in order to select an option or an action, one has to press the specified letter key which is indicated in parenthesis or quotation marks, and press Enter:
15. Select “n” to proceed to the next menu and press Enter.

16. The **Network Configuration** menu is displayed. You **must** configure Host Name, Network Connections, and Routing. You **may** configure a Domain Name. You **must not** configure Domain Name Servers:

- **Host Name** – press “1” and press Enter:

  ![Host Name Configuration]

  Enter the Host name (Computer’s name) and press Enter:

  ![Enter Host Name]

  [Figure: Putty window showing Host Name configuration with option to enter host name.]

  [Figure: Putty window showing prompt to enter host name.]
You are then requested to enter the IP address associated with that Host name. Enter the IP address in a dotted format and press the Enter key:

Press “e” and press Enter to return to the **Network Configuration Screen** menu.

- **Domain Name** (optional) – press “2” and press Enter:

Select **Set domain name** by pressing “1” and then Enter. You are now prompted to enter the Domain Name of your host. See example below. Press Enter to continue.

Press “e” and press Enter. You will return to the **Network Configuration Screen** menu.
- **Network Connections** – press “4” in the **Network Configuration Screen** menu and press Enter. The following menu is displayed:

![Network Connections Configuration Menu](image)

Use the **Network Connections Configuration** menu to configure your network connections. Operation of this menu is equivalent to other sysconfig menus. For each connection, configure its IP address, broadcast address, and netmask. Specify the connection that will be used as the management connection.

Select the **Add new connection** option to define a secondary IP address (alias) on an interface, to assign VLAN definitions, or to define PPPoE, PPTP, or ISDN properties for an interface. For more details on the configuration of these non security-relevant options, see the *SecurePlatform/SecurePlatform Pro* guide. Do not modify the loopback address.

Exit this menu by pressing “e” and Enter. You will return to the **Network Configuration Screen** menu.

- **Routing** – press “5” in the **Network Configuration Screen** menu and press Enter. The following menu is displayed:

![Routing Configuration Menu](image)
To change the default gateway for the SmartCenter Server, select **Set default gateway** by pressing “1” and Enter.

**Note:** Your default gateway was already configured while installing the SecurePlatform operating system as depicted in the first line of the figure above. If it is correct you need not perform any configuration in this step.

Exit this menu by pressing “e” and Enter. You will return to the **Network Configuration Screen** menu.

17. Press “n” and Enter to continue to the **Time and Date Configuration** menu:

![Time and Date Configuration Menu](image)

Use this menu to define the local time zone, date and time for the enforcement module. Operation of this menu is equivalent to other sysconfig menus.

18. The time and date configuration marks the end of the sysconfig wizard. Pressing “n” and Enter progresses the administrator to the cpconfig wizard, used to install and configure appropriate Check Point products.
cpconfig

19. The cpconfig wizard displays the **Import Check Point Products configuration** menu:

   Press “n” and Enter to skip this option.

20. The following screen is displayed:

   Press “n” to start the cpconfig wizard.
21. **Licence Agreement** – Read the License Agreement, scroll down using the Enter key. Once you have reached the end of the agreement, press “y” to accept this agreement:

![Image of Licence Agreement screen]

22. **Product Selection Screen** - Select either Check Point Power or Check Point UTM, according to your license type by pressing the option number key (“1” or “2”, respectively):

![Image of Product Selection screen]
Press “n” to proceed to the next screen. Select **New Installation** by pressing “1”, then press “n”. A list of products appears:

23. Select the **SmartCenter** option by pressing “3”. Then press Enter. Press “n” to continue.
24. Select **Primary SmartCenter** by pressing “1”:

Press “n” to continue.

25. In the Connectra Plug-In screen de-select **Install Connectra NGX R62CM Plug-In** option by pressing “1”, then press “n” to continue.
A validation window will be displayed, press “n” to continue to license installation.
26. **License installation** – a valid license must be installed for the SmartCenter Server. When prompted *Do you want to add licenses*, press “y” and Enter.

Press “f” and Enter to fetch the license from a file. When prompted for the file name, provide a path to the removable media containing the license file. See Chapter 9 section *Product Registration* for instructions on how to create this license file.

Alternatively to the **Fetch from file** method, you may press “m” and Enter for manual license installation (see figure below):

- Enter the IP address (in a dotted notation). It **must** be the exact IP as it appears in the license you have obtained. Press Enter to continue
- Enter the Signature key – It may also be called “License String” in the license you have obtained. Press Enter to continue
- SKU/features – Enter the string of the SKU/features which came with the license you have obtained. Press Enter and your license is installed:

![License Installation Example](image)
27. **Configuring Administrator** - You will be prompted to add a cpconfig administrator. The cpconfig administrator account is used for the installation process, and is deleted at the end of the installation process. It is granted Read/Write permissions, and is authenticated using a password (whereas administrators must always use certificate-based authentication once the evaluated configuration is operational). There are no cpconfig administrator user name or password composition rules.

Answer the question “Do you want to add an administrator” by pressing the “y” key. Then, press Enter. You are now prompted to enter a password. Enter your administrator password and press Enter. You will be asked to verify the password, re-Enter the password and press Enter.
28. **GUI Clients** – define the set of SmartConsole hosts that may connect to the SmartCenter Server. Answer the question “Do you want to add a GUI Client” by pressing the “y” key. Then, press Enter. You are now prompted to enter the list of hosts, each on a separate line. When done, press CTRL-D to end the list. GUI Clients can be defined in various formats, as described in the screen capture below.

![Screen capture of GUI Client configuration](image)

**Note**: When defining the set of permitted GUI clients, take into account that once the evaluated configuration is operational, the administrator is not allowed to log in to the SmartCenter Server console in order to expand the defined set.

**Note**: It is important to realize that the specification of the set of authorized GUI Clients uses a different interface than other menu interfaces described in this Installation Guide. For example, you must enter Any rather than “3” to allow SmartConsole access from any IP address without restriction (subject to Security Policy rules allowing such communication and to administrator authentication).

29. You will be asked to confirm the list of GUI clients by pressing “y”. The installation process proceeds to configure the Random Pool (this phase completes automatically).
30. **Certificate Authority** - The definitions on this window are used to initiate the Internal Certificate Authority, which is used in turn to enable secure communication between the SmartCenter Server and its modules. The certificate is automatically generated at this stage. At the end of it you will be asked to save the Certificate’s Fingerprint to a file. Press the letter “y” and then Enter.
31. **Fingerprint** - The Fingerprint is used the first time you login to a SmartConsole in order to verify the identity of the SmartCenter Server. When you login, you will be asked to compare and contrast the displayed fingerprint with the SmartCenter Server fingerprint in order to verify the identity of the SmartCenter being accessed using SmartConsole. Export the fingerprint to a file (on removable media), so that you have it available for comparison. Specify the fingerprint file name and press Enter. Confirm the action by pressing Enter:

![Configuring Certificate's Fingerprint](image)

32. Press Enter to start the SmartCenter Server services and to complete the sysconfig session. You will be prompted to reboot. On the cpshell prompt, type the `reboot` command and confirm by pressing “y” and Enter. The computer will restart.

33. Log in to cpshell using your operating system account. Log in to Expert Mode by typing `expert` on the cpshell prompt and provide the same password as for the admin account (or if it has been renamed, the corresponding account). Since this is the first use of Expert Mode, you will be prompted to set a new Expert Mode password. Type the new password and press Enter. Re-type the new password and press Enter.
To learn more about Expert Mode, see Chapter 5 Administration, User Management of the SecurePlatform&SecurePlatformPro guide.

The Expert Mode password must conform to the same password complexity rules as the administration account:

- at least 6 characters, in length
- a mixture of alphabetic and numeric characters
- at least four different characters
- does not use simple dictionary words, or common strings such as “qwerty”

### Installing HFAs (if available)

34. Download and install the latest HFA available (if higher than HFA 02) on the Check Point Web site. Detailed instructions for installing the HFA are provided in the HFA release notes.

**Note:** HFAs higher than HFA 02 are outside the evaluated configuration. See Check Point HFA Downloads for more details.

### Installation Settings

35. Enter the following commands to disable functionality that is not available in the evaluated configuration:

```bash
cpd_config -d avsu
cpd_config -d RemoteLic
cpd_config -d SicUpgrade
cpd_config -d RoamingAdmin
```

36. You may now perform any or all of the configuration steps described in Chapter 7 - Installation Settings that require SmartCenter Server console access before you move on to the next step. These steps describe installation settings that have been documented and evaluated as being compatible with the evaluated security policy.
**FIPS Mode Configuration**

37. Copy the sic_policy.conf file provided on the Nokia installation CD to the $CPDIR/conf directory, overwriting the existing file.

38. Enable SmartCenter Server in FIPS Mode by entering the following cpshell commands:

```bash
cpstop
ckp_regedit -a "Software\CheckPoint\SIC" FIPS_140 -n 1
cpstart
```

**Note:** A SmartCenter Server must be in FIPS mode to manage enforcement modules that have been configured in FIPS mode; all enforcement modules managed by a SmartCenter Server that has been configured in FIPS mode must be in FIPS mode in order to be managed by that SmartCenter Server.
Installing SmartConsole

SmartConsole Software Installation

1. In the evaluated configuration, SmartConsole Application has to be installed on a different machine than the SmartCenter Server. The machine has to be a Microsoft Windows Platform Machine, as described above in Hardware Platforms.

Note: SmartConsole hosts should be defined as GUI Clients via the Check Point Configuration tool on the SmartCenter Server (cpconfig).

Log on as a Windows Administrator and insert the CD: VPN-1 Power/UTM with HFA 02 CD2.

The Wrapper should be launched automatically and a Welcome window displayed:
If this window is not displayed, run the **Setup.exe** application from the CD-ROM.

2. Click **Forward** to continue. The License Agreement is displayed. Click **I accept the terms of the License agreement**. Click **Forward** to continue:
3. Select **Check Point Power** or **Check Point UTM**, according to your license, and click **Forward** to continue:

![Check Point Power and UTM selection](image)

4. Select **New Installation** and click **Forward** to continue.

![New Installation selection](image)
5. A list of products appears. Select **SmartConsole** and click **Forward** to continue:
6. The selected product verification window appears, with the selected product being SmartConsole. Click **Forward** to continue:

![SmartConsole verification window](image)

7. Approve the default installation directory, or click **Browse…** to select a new location. Click **Next** to continue:

![Choose destination location](image)
8. In the **Select Clients** screen select the following: **SmartDashboard**, **SmartView Tracker** and **SmartView Monitor**. Click **Next** to continue.

9. A prompt window is opened: **Do you want to create SmartConsole Shortcuts on Desktop?** Select either answer.

Following the installation process, click **OK** on the successful installation window:
Click **Finish** when the InstallShield Wizard completes installation:

![InstallShield Wizard Complete](image1)

Click **Finish** again on the following screen:

![Thank you for installing Check Point Software.](image2)
Installing HFAs (if available)

10. Download and install the latest SmartConsole HFA available (if higher than HFA 02) on the Check Point Web site. Detailed instructions for installing the HFA are provided in the HFA release notes.

Note: HFAs higher than HFA 02 are outside the evaluated configuration. See Check Point HFA Downloads for more details.

First Time Login and Configuration

11. Once both the SmartCenter Server and at least one SmartConsole have been installed, you may proceed to configuring the initial administrator account that is then used for configuring the Security Policy: perform the configuration steps detailed in Chapter 8 - First Time Login.

Installation Settings

12. Perform the SmartConsole host configuration steps described in Chapter 7 - Installation Settings. These steps describe installation settings that enable evaluated configuration functionality:
   • Enabling Offline SmartDefense Updates
   • Configuring Support for Diffie-Hellman Groups 15-18

Security Policy

13. Using the certificate-based administrator defined in the previous step, create an initial default configuration by following the configuration steps detailed in the Administration Guide chapter Creating the Security Policy.
Initialize SIC trust and Policy Installation

14. After installation of the enforcement modules and establishment of SIC trust between the SmartCenter Server and the enforcement modules, Perform Policy > Install… in SmartDashboard to install the defined Security Policy.
Installing the Enforcement Module

IPSO and NGX R65 software installation

Initial Appliance Configuration

1. Establish a physical console connection to the appliance. The console can be any standard VT100-compatible terminal or terminal emulator with the following properties:
   - RS-232 data terminal equipment (DTE)
   - 9600 bps
   - 8 data bits
   - No parity
   - 1 stop bit
   You can also use data communications equipment (DCE) device.

   To establish the physical console connection, follow these steps:
   a. Connect the appropriate cable to the local console port on the front panel of the appliance. If the console is DTE, use the supplied null-modem cable (console cable). If the console is DCE, use a straight-through cable.
   b. Connect the other end of the cable to the console system.

2. Turn the appliance on.
   When the system enters autoboot mode and displays the following message, press any key to display the boot manager prompt:
   Type any character to enter command mode

3. At the boot manager prompt, enter:
   Passwd

4. At the prompt, enter a new password, and re-enter the new password for verification.
Installing IPSO and NGX R65 Software

This section explains how install Nokia IPSO 4.2 and Check Point NGX R65 software on a Nokia appliance.

**Note:** This step is optional as the software is delivered to the customer pre-installed on the appliance. For example, you might want to re-install the software if the appliance has an older version installed. You may skip this section and perform `cpconfig` unless you need to perform a fresh re-installation.

**Note:** When you perform the software re-installation, be sure to follow the instructions carefully. You will overwrite the contents of the hard disk, including the existing IPSO image.

5. At the boot manager prompt, enter `install`

6. Enter the boot manager password when prompted.

7. The installation script runs.
   Answer “n” when asked if this node will be using IGRP or BGP.

8. Provide appropriate answers to the installation script prompts to install the new IPSO image from an FTP server, including FTP server user name and password (if needed), IP address and net mask (e.g. 192.168.2.111/24), network interface information, and path and file name of ipso image on FTP server.

9. To install NGX R65, type “2” when you see the following message:
   1. Retrieve all valid packages, with no further prompting.
   2. Retrieve packages one-by-one, prompting for each.
   3. Retrieve no packages.
   Enter choice [1-3] [1]: 2
10. The installation procedure continues and prompts you to choose which packages to download. Retrieve the R65 wrapper (.tgz) file.

   **Note:** You must **not** install the IPSO UTM Base package. This package is not included in the evaluated configuration.

11. Type “y” and Enter when you see the following:
   - Checking if bootmgr upgrade is needed...
   - No need to upgrade bootmgr.
   - Do you want to upgrade bootmgr anyway? [n]

   **Note:** You must type so that the boot manager is upgraded. You will be unable to place your appliance in FIPS operating mode if you do not allow the original boot manager to be replaced.

12. At the end of the installation procedure, press Enter to reboot.

13. After some miscellaneous output appears on the console connection, the following prompt appears:

   Hostname?

   **Note:** If the Hostname? prompt does not appear on the console, see the appliance Installation Guide for troubleshooting suggestions.

14. Respond to the Hostname? prompt within 30 seconds to prevent the IPSO DHCP client from starting.

   **Note:** If you wait more than approximately 30 seconds before you type a response to the Hostname? prompt, the DHCP client program starts automatically, and the system might be provided a host name and IP address that is unknown to you. (This could happen if a DHCP server on your network is configured to supply configuration information to any system that requests
If this happens, enter the following commands after logging in to the console, and reboot:

```
rm /config/active
or
mv /config/active /config/active.old
```

15. You will be prompted for a password for user admin. Enter a password for the admin account.

16. When you see the following message, type “1”:

   You can configure your system in two ways:
   1) configure an interface and use our Web-based Voyager via a remote browser
   2) configure an interface by using the CLI
   Please enter a choice [1-2, q]:

17. You are prompted to select a network interface to configure, e.g.:

   Select an interface from the following for configuration:
   1) ser-s2p1
   2) eth-s3p1
   3) eth-s4p1
   4) eth-s5p1
   5) quit this menu

   Enter choice [1-5]:

   The list of interfaces that you see depends on the network interface cards (NICs) that are installed, and the port and slot numbering depends on the platform. In the example above ser-s2p1 is a serial interface in chassis slot 2, port 1, and eth-s3p1 is an ethernet interface in chassis slot 3, port 1. Type the number for the interface to configure. Remember that this is the interface you will connect to with Voyager or the CLI to continue with the configuration.
18. When prompted, enter the IP address and subnetwork mask length, e.g.: 192.168.2.111/24.

19. You are now prompted to install the R65 wrapper package. Type “1” and Enter to install the package.

Would you like to:

1. Install this as a new package
2. Upgrade from an old package
3. Skip this package
4. Exit new package installation

Choose (1-4):

20. The package is installed and the appliance reboots. When prompted, log into the system using the admin account and password set in step 15 above.
cpconfig

21. At the system console, enter: `cpconfig` to run the cpconfig wizard. Press Enter to read the license agreement. Scroll down using the Enter or Space keys. Once you have reached the end of the agreement, press “y” to accept this agreement.

22. Select either Check Point Power or Check Point UTM, according to your license type by pressing the option number key (‘1’ or ‘2’, respectively and the Enter key).

23. Press “2” and Enter to select the **Distributed** installation type.

24. Press “1” and Enter to select **VPN-1 Power Gateway**.

25. Respond to both the **Dynamically Assigned IP Address gateway installation** and **Check Point clustering product** prompts by pressing “n” and the Enter key.

26. A valid license must be installed for the SmartCenter Server. When prompted **Do you want to add licenses**, press “y” and Enter. Install the license as for the SmartCenter Server.

27. **Configuring Groups Permissions** – Press Enter for the default value, and confirm by pressing “y” and Enter.

28. **Configuring Random Pool** – you are now asked to perform a short random keystroke session. Keep typing until you hear the beep and the displayed bar is full.

29. **Secure Internal Communication** - allows you to establish an Activation Key that will be used for initializing Secure Internal Communication (SIC) between this enforcement module and the SmartCenter Server.
The Activation Key is generated on the SmartCenter Server when defining the enforcement module object. See the *CC Evaluated Configuration Administration Guide* section *SIC Trust Establishment* for the procedure needed to obtain the Activation Key.

Type in the Activation key in the prompt and press Enter. Re-type the activation key and press Enter.

30. Press “y” and Enter to reboot.

**Installing HFAs (if available)**

31. Download and install the latest HFA available (if higher than HFA 02) on the Check Point Web site. Detailed instructions for installing the HFA are provided in the HFA release notes.

**Note:** HFAs higher than HFA 02 are outside the evaluated configuration. See *Check Point HFA Downloads* for more details.

**Installation Settings**

32. From the console, initialize the *ThisModule* dynamic object (see also *Administration Guide* section *Management Rules*). Type:

```
dynamic_objects -n ThisModule -r <ip1> <ip1> <ip2> <ip2> ... -a
```

(Where *ip1*, *ip2*, ... are the IP addresses configured on the module. Note that it is important to specify each IP address twice as above.)

For example, if an enforcement module named gw1 has two interfaces: 10.0.0.100, and 192.168.10.1, enter the following command:

```
dynamic_objects -n ThisModule -r \ 10.0.0.100 10.0.0.100 192.168.10.1 192.168.10.1 -a
```
33. Enter the following commands to disable functionality that is not available in the evaluated configuration:

cpd_config -d avsu
cpd_config -d RemoteLic
cpd_config -d SicUpgrade

cd $FWDIR/conf
sed -e 's/.*/aciufpd.*///' fwauthd.conf | cat >fwauthd.conf
sed -e 's/.*/stormd.*///' fwauthd.conf | cat >fwauthd.conf
sed -e 's/.*/sdsd.*///' fwauthd.conf | cat >fwauthd.conf

dbset package:FireWall-1:process:ifwd ""

34. Run cpconfig, and disable SecureXL (option 8 in the cpconfig menu).

35. Run clish, and disable the snmp daemon:

set snmp daemon off

36. Configure interfaces, static routing information, static DNS and ARP resolution, VLAN support, etc. - as necessary. See the CLI Reference Guide for more information. Do not use the following clish commands:

- System Configuration Commands:
  - add/set dhcp
  - set dns
  - download image
  - set mail-relay
  - set dumpserver
  - add/set ntp

- High Availability and IP Clustering Commands
- SNMP Commands
- IPv6 Commands
- Network Security and Access Commands
- Routing Commands except for the (allowed) commands: set static-route and show route.
Note: The topology information configured for the enforcement module object in SmartDashboard (see CC Evaluated Configuration Administration Guide section Creating the Security Gateway Object must correspond to the definitions on the enforcement module itself.

37. You may now also perform any or all of the configuration steps described in Chapter 7 - Installation Settings that require enforcement module console access before you move on to the next step. These steps describe additional installation settings that have been documented and evaluated as being compatible with the evaluated security policy.

FIPS Mode Configuration

38. Copy the sic_policy.conf file provided on the Nokia installation CD to the $CPDIR/conf directory, overwriting the existing file.

39. Run clish, and type: set fips on restart

The system reboots and starts in FIPS mode.

Note: All other installation steps should be performed before enabling FIPS Mode. Enabling FIPS Mode disables some of the commands that are needed to perform many of these steps. If FIPS Mode was enabled prematurely, the administrator may exit this mode using the following command:

set fips off without-restore

Once the enforcement module is in FIPS mode, the administrator establishes SIC trust between the SmartCenter Server and the enforcement module, and performs Security Policy installation, as described in CHAPTER 9 of the CC Evaluated Configuration Administration Guide.
The VPN-1 Power/UTM product provides a large number of administrator-controlled settings. A significant part of these settings can be controlled using SmartConsole, and is therefore available after the product is operational. (See the Administration Guide for instructions and constraints for the use of SmartConsole in the evaluated configuration.)

Some settings can only be controlled using the CLI or dbedit tools. These are installation settings that may not be changed after the product is operational, when administrators no longer log in to the SmartCenter Server or appliances. The following procedures may be performed when implementing the evaluated configuration. The installation settings
described in this chapter have been documented and evaluated as being compatible with the evaluated security policy.

Installation settings that are not listed here should not be modified from their default values.

**Extending the Validity Period of a SIC Certificate**

The validity period of a SIC certificate may be extended to up to 20 years. Although this is not required, you should note that the evaluated configuration does not support certificate renewal. When an enforcement module SIC certificate expires, management connectivity is lost, and you will have to reinstall the module.

In order to change the validity period from its default of five years, the administrator logs into the SmartCenter Server console and uses the `expert` command to enter expert mode. He then edits the file named `$FWDIR/conf/InternalCA.C` and adds a line with the validity period of SIC certificates in seconds as follows:

```
:sic_cert_validity (# of seconds)
```

For example, for a period of 20 years (20*365*24*3600 = 630720000):

```
:sic_cert_validity (630720000)
```

If the setting exceeds 20 years the value drops to the default (5 years).

Perform `cpstop` and `cpstart` for this setting to be applied.

**Enabling Support for IP Options**

IP options 3 or 9 (source route options) must **not** be enabled in the evaluated configuration.

Other IP options are not considered security relevant in the context of the evaluated configuration. By default, any IP packets that contain IP options are dropped by the enforcement module, except for the "Router Alert"
option (0x94) for the IGMPv2 and PIM protocols. This provides protection against any vulnerabilities that might be associated with the use of IP options.

It is possible (although not recommended) for the administrator to enable support for IP options. The set of permitted options must be configured during installation; the `enable_ip_options` setting in SmartDashboard is then used to enable or disable this functionality. Contact Check Point support for instructions on configuring the set of allowed IP options.

**Scheduling Backups and Restoring from Backup**

It is possible to schedule SmartCenter Server backups using the `cpshell backup` command (see *Check Point SecurePlatform/ SecurePlatform Pro Guide* for more details). The backup files are kept in tar gzipped format (.tgz). By default, backup files are saved into `/var/CPbackup/backups`.

- The `-l` flag enables log backup (by default, logs are not backed up).
- The `--purge` flag deletes old backups; it should be used if the backups are made to a local disk instead of to removable media to ensure that disk resources are not exhausted.
- The backup should be created to a local filesystem (e.g. removable media) using the `--file` flag; the `--tftp` and `--scp` flags should *not* be used in the evaluated configuration.

Restoration from a backup is performed during the installation phase of the SmartCenter Server. Use the `restore` command:

```
restore --file <Filename>
```
Note: Backup files contain sensitive information (e.g. private keys). If backups are written to detachable media, ensure that backup files are secure from any unauthorized access.

There is no need to back up enforcement modules; all Security Policy information is maintained on the SmartCenter Server.

Configuring OCSP

Use of the OCSP protocol for checking certificate revocation status for certificates issued by a specific Certificate Authority is configured during the installation and configuration phase. This property is configured for the root CA and is inherited by subordinate CAs.

Note: CRLs will not be retrieved for a CA for which OCSP validation has been configured. OCSP responses are not cached.

Use dbedit or SmartDashboard to create the CA object. The dbedit commands needed to configure OCSP validation receive the following parameter values:

- `<root-CA>` The name of the CA object in the database
- `<OCSP-server>` The name for the OCSP responder object
- `<OCSP-URL>` The URL for the OCSP responder
- `<OCSP-cert>` The certificate for the OCSP responder (PEM)

Enter the following commands in dbedit, and install policy:

```
dbedit> create OCSP_server <OCSP-server>
dbedit> modify servers <OCSP-server> url <OCSP-URL>
dbedit> modify servers <OCSP-server> certificate <OCSP-cert>
dbedit> update servers <OCSP-server>
dbedit> modify servers <root-CA> OCSP_validation true
dbedit> addelement servers <root-CA> OCSP_servers servers:<OCSP-server>
dbedit> update servers <root-CA>
```

It is possible to set OCSP_validation for the CA object as above, but omit the definition of the OCSP responder object and the reference to that object in the CA object's OCSP_servers attribute. In this case, certificates
Installation Settings

issued by the CA must have the AuthorityInfoAccess extension containing the OCSP responder's URL, and the OCSP responder's certificate returned in the OCSP response must be signed by the CA that issued the certificate, and include id-kp-OCSPSigning in the extendedKeyUsage certificate extension, as defined in the OCSP RFC.

In this case, the only dbedit commands that need to be entered are:

dbedit> modify servers <root-CA > OCSP_validation true
   dbedit> update servers <root-CA>

Configuring SecurID

To allow an enforcement module to communicate with a SecurID-based authentication server (RSA ACE/Server) on a directly connected network, generate and copy the sdconf.rec file from the ACE/Server to /var/ace/sdconf.rec on the enforcement module.

Note: When the VPN-1 Power/UTM Gateway has multiple interfaces, the SecurID agent in VPN-1 Power/UTM will in some cases use the wrong interface IP to decrypt the reply from ACE/Server, and authentication will fail.

To overcome this problem, place a new text file named sdopts.rec in the same directory as sdconf.rec. The file should contain the following line:

CLIENT_IP=<ip>

where <ip> is the primary IP address of the enforcement module, as defined on the ACE/Server. This is the IP address of the interface to which the server responses are routed.

SecureClient Mobile Download

By default, enforcement modules configured to support Visitor Mode provide only the SSL Network Extender client software for user download. The SecureClient Mobile client software is distributed on the
Installation Settings

product CD-ROMs, and installed by the user on the mobile device as described in the *Virtual Private Networks Administration Guide*, Chapter 17 – *SecureClient Mobile*, section *Client Side Installation*.

To allow users to download the SecureClient Mobile client software from the enforcement module, copy the SecureClient Mobile .cab file from the windows\SecureClient_Mobile directory on CD2 to the enforcement module directory $FWDIR/conf/extender/CSHELL. Add a reference to the file in the $FWDIR/conf/extender/index.html file under the cpextender.msi download.

*Note:* The index.html file may be overwritten if you reinstall the software or apply HFAs. Therefore, it is advisable to keep an offline backup of any edits performed on the module so that they can be reapplied if needed.

**Enabling Offline SmartDefense Updates**

SmartDefense Updates are normally downloaded from the Web directly to the SmartConsole host, as described in the *Firewall and SmartDefense* guide. However, this is not allowed in the evaluated configuration - the SmartConsole host is installed on a LAN that is protected by a firewall that is configured not to let this update request go through.
Enabling offline SmartDefense updates adds an **Offline Update** button to the **SmartDefense** tab of the SmartDashboard that is used for loading the SmartDefense update from a file:

1. On the SmartConsole machine, use the MS registry editor. To do so click the **Start** button and select **Run…** - in the **Run** window type `regedit` and click **OK**:
2. Set the DWORD under the registry path `HKEY_CURRENT_USER\Software\CheckPoint\Management Clients\6.0.3\GA\Check Point SmartDashboard\General Settings\SmartDefense\EnableOfflineUpdate` to 1 (double-click on the attribute Name in order to edit it).

3. Exit the regedit program by selecting the menu item `File->Exit`.

**Configuring Support for Diffie–Hellman Groups 15–18**

You may enable support for Diffie-Hellman Groups 15-18 by defining them in the VPN-1 database, as explained in SecureKnowledge Solution ID: sk27054. Although this is an optional step, note that it may only be performed during the installation phase; if it is not performed during installation, you will only be able to use the default groups: 1, 2, 5, and 14.

1. Log into the SmartConsole Microsoft Windows machine as an operating system Administrator.
Note: Close SmartDashboard if it is open because keeping it open may lock the Database.

2. On the SmartConsole machine, run:
   C:\Program Files\CheckPoint\SmartConsole\R65\PROGRAM\GuiDBedit.exe.

3. Log in using a certificate-based administrator account:

![Database Tool Login](image)
4. In the Tables pane, navigate to **VPN > encryption**:
5. Right-click the objects pane (top right) and select **New…** - the **Create Object** window will appear.

6. In the **Create Object** window, Under **Class**, choose "IKE.Diffie_Hellman_parameters_object".
7. In the **Object** textbox, type the Group name and click **OK**. For example for group 15 type: "Group 15 (3072 bit)". For each group you can get the name from the SecureKnowledge page:
8. Set **DH_group_number** to the number described in the SK. For example for Group 15 set the number to 15:
   - In the objects pane, select the object you want to edit. In this example it is: **Group 15 (3072 bit)**.
   - The object’s parameters will appear in the bottom window.
   - Select the parameter you want to edit - **DH_group_number**.
   - Go to the value and right click on it.
   - Select the **Edit** option.
   - The **Edit window** will appear with the default value.
   - Change the value to 15 and press **OK**.
9. Follow the same method outlined in the previous step and set \texttt{mod > value} to the MODP string given in the SK for every desired group.

\textbf{Note:} Cut and paste the MODP string from the SK into GuiDBEdit. \textbf{Important:} Take care that no space characters are copied at the end of the string.

10. Repeat the steps described above for all desired Diffie-Hellman Groups and set the parameters values from the SK.
11. You may save either all objects using **File > Save All**, or select the object you want to save on the objects pane, right-click and select **Save**. When finished, select **File > Exit** to exit GuiDBedit.
First Time Login

The login process, in which administrators use SmartConsole applications to connect to the SmartCenter Server consists of a bidirectional operation, in which the administrator and the SmartCenter Server authenticate each other and create a secure channel of communication between them using Check Point’s Secure Internal Communication (SIC) mechanism.

In the evaluated configuration, the Administrator is required to authenticate using a SIC certificate. During the installation of the SmartCenter Server (see above: `cpconfig`), a cpconfig administrator account is defined with user name/password authentication.

The First Time Login procedure is performed after SmartCenter Server installation, and after at least one SmartConsole is installed. It involves the following steps:

- Logging in via SmartConsole to the SmartCenter Server using the cpconfig administrator account
- Confirming that the SmartCenter Server certificate fingerprint presented during login is the same as the fingerprint generated during SmartCenter Server installation; this fingerprint once approved is stored on the SmartConsole host and is used to authenticate the SmartCenter Server in subsequent logins.
- Creating default evaluated configuration Permissions Profiles
- Creating a certificate-authenticated administrator account
- Deleting the cpconfig administrator account
SmartCenter Server Fingerprint Verification

**Note:** the following procedure must be performed from a SmartConsole GUI Client that was authorized in cpconfig to connect to the SmartCenter Server.

1. **SmartConsole First time Configuration** - launch SmartDashboard by selecting **Start > Programs > Check Point SmartConsole R65 > SmartDashboard** on the Windows desktop, and login using the cpconfig administrator’s User Name and Password:

   - Do *not* set either **Demo Mode** or **Read Only**.
   - Enter the cpconfig administrator’s User Name.
   - Enter the cpconfig administrator’s Password.
   - In the SmartCenter Server field, specify the name or IP address of the target SmartCenter Server.

   Click OK to proceed to the fingerprint approval window.
2. **Fingerprint verification**: manually authenticate the SmartCenter Server with the Fingerprint presented during the SmartCenter Server configuration process (cpconfig – see page 58).

- Type the Fingerprint file you have saved during the Configuration Tool settings. For example:

```
[Expert@dandi]# cat $CPDIR/conf/my_fingerprint
FAME TED SAD TUES DANK SOAK TRAY HAIR IDLE SAID DONE ONE

[Expert@dandi]#
```

- Compare the fingerprint from both machines, SmartCenter Server (see above) and SmartConsole (see below). If the fingerprint is identical, click the **Approve** button to continue.

![SmartDashboard Screenshot]

**Note**: If the fingerprint is not identical, **Quit** and retry; this might be a symptom of an attacker attempting to spoof the SmartCenter Server machine.
Evaluated Configuration Permissions Profiles

The evaluated configuration defines two permissions profiles: AuthorizedAdministrator and AuditAdministrator. The Administration Guide section Permissions Profiles describes the permissions allocated to each of these profiles.

The two permissions profiles are created during installation so that they are available by default when the evaluated configuration becomes operational; however, only an AuthorizedAdministrator account is created during the installation process, as described below.

12. In SmartDashboard, select Manage > Permissions Profiles… and select New… Permissions Profile… from the Permissions Profiles window. The Permissions Profile Properties window is displayed. Name the new Permissions Profile AuthorizedAdministrator, and select the Permissions tab.
13. Set permissions for the AuthorizedAdministrator permissions profile to **Read/Write All** with the **Manage Administrators** permission:

14. Repeat to create a new permissions profile named AuditAdministrator. Set permissions for AuditAdministrator to **Customized**, deselect **LDAP Users Database** through **Eventia Reporter** and
UserAuthority Web Access through Event Correlation Policy permissions, and set remaining permissions to Read Only:
Creating an Authorized Administrator Account

15. Select Users and Administrators > Administrators > New Administrator. The Administrator Properties window is displayed. The administrator’s name attribute may be set to whatever value is desired. Assign the new administrator to the AuthorizedAdministrator permissions profile.

16. Using the Admin Certificates tab, click Generate and Save to generate the certificate, which will be used on all logins from now on. Save the certificate to removable media (e.g. a diskette) and hand it to the user it represents.

17. The Administrator can then authenticate himself with his Certificate:

Deleting the cpconfig Administrator

18. Login to the SmartCenter Server console using your operating system credentials.
19. Run the `cpconfig` command from the cpshell prompt. The following screen will be displayed:

![cpconfig screen](image)

20. Press “2” (Administrators), and press Enter. The defined cpconfig administrator will be listed:

![Administrator list](image)

21. When prompted “Do you want to modify this list”, press Enter to accept the default value (“y”).

22. When prompted “Do you want to delete an administrator”, press Enter to accept the default value (“y”).
23. You are now prompted to type in the Administrator name; type the cpconfig administrator’s account name and then press Enter. You will be notified that No administrator is currently defined:

![Image of a terminal window showing the prompt to modify administrator list and the removal of an administrator]

24. Confirm that you would like to continue by typing “y” and pressing Enter.

The cpconfig menu is displayed. Select “8” and press Enter to exit.
This appendix provides instructions on accessing the Check Point User Center. The User Center provides the following relevant resources:

- Product registration and licensing
- SecureKnowledge Solutions (SKs) that are referenced in this installation guide.
- Procedures for contacting Check Point support.

The procedures in this appendix can be used to guide you through these resources. Note that multiple paths exist through the User Center, so that the same procedures can be performed in other sequences as well.
User Center Registration and Access

1. Go to Checkpoint Home page www.checkpoint.com, and select the My Account option from the menu. The My Account page is displayed:
2. If you already have a **Username** and **Password**, you may enter them to access the User Center. If you do not already have a Username and Password, click the **Sign up Now** link. The **Create Your Profile** page is displayed:
3. In the **Create Your Profile** page, enter the requested information and click **Submit**. You are notified that your profile is complete and that an email with your new User Center password will be sent to the email address specified. Once you receive this email, you may access the User Center with the login name (**Username**) and password given in the email. An example of such an email is shown below:

<table>
<thead>
<tr>
<th>This is an email generated by the Check Point User Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thank you for joining the Check Point User Center.</td>
</tr>
<tr>
<td>Your login name is: <strong><a href="mailto:oritgal@hotmail.com">oritgal@hotmail.com</a></strong></td>
</tr>
<tr>
<td>Your password is: <strong>2zdrxscb</strong></td>
</tr>
<tr>
<td>Please login to Check Point User Center:</td>
</tr>
<tr>
<td><a href="https://usercenter.checkpoint.com/usercenter/index.jsp">https://usercenter.checkpoint.com/usercenter/index.jsp</a></td>
</tr>
<tr>
<td>To get started, please follow the instructions in the &quot;Accounts &amp; Products&quot; tab &gt; &quot;Getting Started&quot; sub tab.</td>
</tr>
<tr>
<td>Thank you,</td>
</tr>
<tr>
<td>Check Point Software Technologies</td>
</tr>
</tbody>
</table>
4. Once you successfully log in to the User Center, the User Center home page is displayed. The following is an example home page:
5. If this is your first User Center access, select **Accounts & Products** and click the **Create Account** link. The **Account Profile Create Account** page is displayed:
6. On the **Account Profile Create Account** page, enter the requested information and click **Submit**. The **Account Profile View** page is then displayed:

![Account Profile View](image)

**Note:** There are cases in which the distributor sends an order to Check Point for a customer and explicitly requests that Check Point create the customer’s User Center account on the user's behalf. In such a case, Check Point creates the account for that user. The user, after creating his profile and logging in, can access the account previously created by Check Point.

**Product Registration**

1. From the User Center, select **Accounts & Products** and click the **Add Products** link in order to add your Product to your account. The **Add Products** page is displayed:
2. Each case containing the Check Point VPN-1/FireWall-1 NGX software CD-ROMs is printed on the back with a unique Certificate Key. Enter your Certificate Key and click Submit. The system verifies that the Certificate Key entered belongs to your Product. If the Certificate Key has already been registered an error window is displayed. An example of this error window is shown below:
3. If the system verifies that the Certificate Key entered is being registered for the first time, the **Product List** page is displayed and the Product is listed as belonging to the given account:
4. Select the Product for which you want to get a license and click the Activate link. The Licensing Information page is displayed:

![Licensing Information - Step 1 of 1](image)

5. Enter the required information and click Activate. The Licensing Process Completed page is displayed:

![Licensing Information - Licensing Process Completed](image)
6. A Registration Confirmation email is sent to the specified email address. This email contains license information and instructions on how to import the license into your product. Click the **Get License** link for the product whose license you want to download. The **Get License** page is displayed.

7. Click the **Get License File** link to download the license file to removable media. Provide this file on the cpconfig license installation prompt, for both SmartCenter Server and enforcement module installations.
SecureKnowledge Solutions

You may use the following procedure to access the SecureKnowledge Solutions (SKs) referenced in this installation guide:

1. Go to Checkpoint Home page www.checkpoint.com, and select the Support option from the menu:
2. On the Support Center page, select the **SecureKnowledge** link:
3. Enter your User Center **Username** and **Password** in the **Login** page:
4. Enter the solution ID number (e.g. sk27054) in the **Search for:** text box, and then click **Search >>:**

5. The matching solution appears in the Results section on the page. Select it to view the solution page:
Note: SecureKnowledge Solutions are delivered by Check Point over https (protected using the SSL or TLS protocols). Use the facilities provided by your browser to verify the origin and integrity of the SecureKnowledge Solution (some browsers may perform this task automatically).

6. The following are MD5 and SHA-1 hashes for the scripts and utilities that can be downloaded from SecureKnowledge Solutions referenced in this Installation Guide. Verify the integrity of the downloads using these hashes:

<table>
<thead>
<tr>
<th></th>
<th>cd2iso</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1 signature</td>
<td>3879e834</td>
</tr>
<tr>
<td></td>
<td>0d5a81bb</td>
</tr>
<tr>
<td></td>
<td>8965e82a</td>
</tr>
<tr>
<td></td>
<td>d300fee1</td>
</tr>
<tr>
<td></td>
<td>0fc8a872</td>
</tr>
<tr>
<td>MD5 signature</td>
<td>fcf17ee3</td>
</tr>
<tr>
<td></td>
<td>75267d9f</td>
</tr>
<tr>
<td></td>
<td>d93cc4d6</td>
</tr>
<tr>
<td></td>
<td>8ee18983</td>
</tr>
<tr>
<td>File size</td>
<td>14,336 bytes</td>
</tr>
</tbody>
</table>