Important Information

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=10948

For additional technical information, visit the Check Point Support Center
(http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02 July 2012</td>
<td>Added First Time Wizard for Gaia and for Multi-Domain Server</td>
</tr>
<tr>
<td></td>
<td>Added Gaia to Restoring Using the WebUI (on page 61)</td>
</tr>
<tr>
<td>23 February 2011</td>
<td>• Guide now applies to all Check Point software versions.</td>
</tr>
<tr>
<td></td>
<td>• Added Rack mounting instructions (&quot;Rack Mounting Smart-1 50/150&quot; on page 17).</td>
</tr>
<tr>
<td></td>
<td>• Updated the First Time Configuration Wizard Instructions</td>
</tr>
<tr>
<td>26 august 2010</td>
<td>First release of the document</td>
</tr>
</tbody>
</table>

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

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Smart-1 50/150 Getting Started Guide).
Health and Safety Information

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

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

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

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

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

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

- Disconnect the system board power supply from its power source before you connect or disconnect cables or install or remove any system board components. Failure to do this can result in personnel injury or equipment damage.
- Avoid short-circuiting the lithium battery; this can cause it to superheat and cause burns if touched.
• Do not operate the processor without a thermal solution. Damage to the processor can occur in seconds.

For California:

Perchlorate Material - special handling may apply. See http://www.dtsc.ca.gov/hazardouswaste/perchlorate

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

Proposition 65 Chemical

Chemicals identified by the State of California, pursuant to the requirements of the California Safe Drinking Water and Toxic Enforcement Act of 1986, California Health & Safety Code s. 25249.5, et seq. ("Proposition 65"), that is "known to the State to cause cancer or reproductive toxicity" (see http://www.calepa.ca.gov)

WARNING:

Handling the cord on this product will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Federal Communications Commission (FCC) Statement:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Information to user:

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

Canadian Department Compliance Statement:

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
Health and Safety Information

Japan Class A Compliance Statement:

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。VCCI-A

European Union (EU) Electromagnetic Compatibility Directive


This product is in conformity with Low Voltage Directive 2006/95/EC, and complies with the requirements in the Council Directive 2006/95/EC relating to electrical equipment designed for use within certain voltage limits and the Amendment Directive 93/68/EEC.

Product Disposal

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Health and Safety Information</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>11</td>
</tr>
<tr>
<td>Welcome</td>
<td>11</td>
</tr>
<tr>
<td>Smart-1 Overview</td>
<td>11</td>
</tr>
<tr>
<td>This document provides:</td>
<td>12</td>
</tr>
<tr>
<td>Security Management Software Blades</td>
<td>12</td>
</tr>
<tr>
<td>SmartEvent</td>
<td>12</td>
</tr>
<tr>
<td>Shipping Carton Contents</td>
<td>13</td>
</tr>
<tr>
<td>Terminology</td>
<td>13</td>
</tr>
<tr>
<td>SmartEvent Terminology</td>
<td>14</td>
</tr>
<tr>
<td>Multi-Domain Security Management/Provider-1 Terminology</td>
<td>14</td>
</tr>
<tr>
<td>Rack Mounting Smart-1 50/150</td>
<td>17</td>
</tr>
<tr>
<td>Safety Instructions</td>
<td>17</td>
</tr>
<tr>
<td>Determining Space and Weight Requirements</td>
<td>18</td>
</tr>
<tr>
<td>Rack Mounting Hardware and Tools</td>
<td>19</td>
</tr>
<tr>
<td>Disconnecting the Appliance Rail from the Mounting Bracket</td>
<td>20</td>
</tr>
<tr>
<td>Attaching the Appliance Rails to the Appliance</td>
<td>21</td>
</tr>
<tr>
<td>Attaching the Appliance Handles or Bracket Ears (Optional)</td>
<td>22</td>
</tr>
<tr>
<td>Attaching the Mounting Brackets to the Rack</td>
<td>22</td>
</tr>
<tr>
<td>Installing Smart 1 50/150 in the Rack</td>
<td>24</td>
</tr>
<tr>
<td>Configuring Smart-1</td>
<td>27</td>
</tr>
<tr>
<td>Connecting the Power Cables and Power On</td>
<td>27</td>
</tr>
<tr>
<td>Available Software Images</td>
<td>28</td>
</tr>
<tr>
<td>Using the First Time Configuration Wizard</td>
<td>28</td>
</tr>
<tr>
<td>Using the First Time Configuration Wizard on Gaia</td>
<td>29</td>
</tr>
<tr>
<td>Starting the Gaia First Time Configuration Wizard</td>
<td>29</td>
</tr>
<tr>
<td>Welcome</td>
<td>29</td>
</tr>
<tr>
<td>Available Releases</td>
<td>30</td>
</tr>
<tr>
<td>Authentication Details</td>
<td>30</td>
</tr>
<tr>
<td>Date and Time Setup</td>
<td>30</td>
</tr>
<tr>
<td>Device Name</td>
<td>30</td>
</tr>
<tr>
<td>Network Connection</td>
<td>31</td>
</tr>
<tr>
<td>Appliance Type</td>
<td>31</td>
</tr>
<tr>
<td>Products</td>
<td>32</td>
</tr>
<tr>
<td>Security Management Administrator</td>
<td>32</td>
</tr>
<tr>
<td>Security Management GUI Clients</td>
<td>32</td>
</tr>
</tbody>
</table>
Secure Internal Communication (SIC) ................................................................. 32
Summary .............................................................................................................. 32
Using the First Time Configuration Wizard on SecurePlatform ...................... 34
Starting the First Time Configuration Wizard .................................................... 34
Welcome .............................................................................................................. 35
Appliance Date and Time Setup ......................................................................... 35
Network Connections ........................................................................................ 35
Routing Table ..................................................................................................... 35
DNS and Domain Settings .................................................................................. 35
Security Management Installation Type ............................................................ 36
Security Management ......................................................................................... 36
SmartEvent and SmartReporter Suite Installation Type .................................... 37
Web/SSH and GUI Clients Configuration ............................................................ 37
Secure Internal Communication ......................................................................... 38
Download SmartConsole Applications .............................................................. 38
Summary .............................................................................................................. 38
Using the First Time Configuration Wizard on Multi-Domain Server .............. 38
Appliance Date and Time Setup ......................................................................... 38
Network Connections ........................................................................................ 39
Routing Table ..................................................................................................... 39
DNS and Domain Settings .................................................................................. 39
Web/SSH and GUI Clients Configuration ............................................................ 39
Multi-Domain Security Management Installation Type .................................... 40
Multi-Domain Server Configuration ................................................................. 40
Multi-Domain Security Management Administrator ....................................... 41
Secure Internal Communication ......................................................................... 41
Download SmartConsole Applications .............................................................. 41
Summary .............................................................................................................. 41
Installing the SmartConsole GUI Clients ............................................................ 41
Advanced Configuration ..................................................................................... 42
Connecting to the Smart-1 CLI .......................................................................... 42
Migration from Existing Provider-1 Machines ..................................................... 42
Configuring SmartEvent ..................................................................................... 45
Preparing SmartEvent on Security Management Server .................................. 45
Preparing SmartEvent on the Multi-Domain Server ......................................... 46
Enabling Connectivity with Multi-Domain Security Management ................... 47
Configuring the SmartEvent Clients ................................................................. 47
  Defining the Internal Network for SmartEvent ............................................... 47
  Defining Correlation Units and Log Servers for SmartEvent ......................... 47
  Creating a Consolidation Session for SmartReporter ...................................... 48
Smart-1 Hardware ............................................................................................... 51
Smart-1 50 Front Panel ....................................................................................... 52
Smart-1 150 Front panel .................................................................................... 53
LCD Display Screen .......................................................................................... 53
Customer Replaceable Parts ................................................................. 55
   Power Supplies .............................................................................. 55
   Hard Disk Drives ........................................................................... 56
   Cooling Fans .................................................................................. 58

Restoring Factory Defaults ................................................................ 61
   Restoring Using the WebUI .............................................................. 61
   Gaia ................................................................................................. 61
   SecurePlatform .............................................................................. 62
   Restoring Using the Console Boot Menu ........................................... 62
   Restoring Using the LCD Panel ......................................................... 63

Lights Out Management ...................................................................... 67
   Introduction ..................................................................................... 68
   Initial Login ..................................................................................... 68
   Basic Configuration Options ......................................................... 69
   Remotely Controlling the Appliance ................................................ 69
   Remotely Controlling the Power of the Appliance ......................... 69
   Managing LOM Card Users ............................................................. 69
   Configuring LOM Keyboard and Mouse .......................................... 71
   Configuring LOM Network .............................................................. 71
   Setting the Date and Time .............................................................. 71
   Defining a LOM Login Message ..................................................... 71

Registration and Support .................................................................... 73
   Registration .................................................................................... 73
   Support .......................................................................................... 73
   Where to From Here? ..................................................................... 73
Welcome

Thank you for choosing Check Point’s Smart-1. We hope that you will be satisfied with this system and our support services. Check Point products are the most up to date and secure solutions available today.

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

For more about the Internet Security Product Suite and other security solutions, see the Check Point Web site (http://www.checkpoint.com), or call Check Point at 1(800) 429-4391. For more technical information about Check Point products, consult the Check Point Support Center (http://supportcenter.checkpoint.com).

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

Smart-1 Overview

Smart-1 appliances deliver Check Point’s market leading security management software blades on a dedicated hardware platform specifically designed for mid-size and large enterprise security networks. Based upon Check Point’s software blade architecture, Smart-1 appliances deliver a unified management solution for network, IPS and endpoint security with unsurpassed extensibility.

- Provides a comprehensive set of security management Software Blades
Introduction

- Maximize efficiency with a single unified management console for network and endpoint security
- Reduce costs and conserve resources with up to 12 TB of built-in storage capabilities
- Ensure operational continuity for the most demanding environments
- Simplify large scale security policy provisioning with Multi-Domain Security Management (Provider-1)

This document provides:

- A brief overview of essential Smart-1 concepts and features
- A step by step guide to getting Smart-1 up and running

Note - Screen shots in this guide may apply only to the highest model to which this guide applies.

Security Management Software Blades

Smart-1 Appliances includes the following Security Management Software Blades:

- Network Policy Management
- Endpoint Policy Management
- Logging & Status
- SmartProvisioning
- Monitoring
- User Directory
- Management Portal
- SmartEvent (SmartEvent Intro, Reporting and Event Correlation)
- Multi-Domain Security Management

SmartEvent

Smart-1 includes SmartEvent, which is made up of SmartEvent Intro, Reporting and Event Correlation. SmartEvent provides centralized reporting and real-time security event correlation and management of your security data. Security teams no longer need to comb through the massive amount of data generated by the devices in their environment. Instead, they can focus on deploying resources on the important threats and trends that pose the greatest risk to their business.
You can configure Smart-1 as a Security Management server with SmartEvent. In R75 and higher, you can also configure Smart-1 as a dedicated server for SmartEvent.

**Shipping Carton Contents**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td>A single Smart-1 appliance</td>
</tr>
<tr>
<td>Rack Mounting Accessories</td>
<td>Hardware mounting kit</td>
</tr>
<tr>
<td>Cables</td>
<td>• 2 power cables (Smart-1 50)</td>
</tr>
<tr>
<td></td>
<td>• 3 power cables (Smart-1 150)</td>
</tr>
<tr>
<td></td>
<td>• 1 standard LAN cable</td>
</tr>
<tr>
<td></td>
<td>• 1 serial console cable</td>
</tr>
<tr>
<td>Documentation</td>
<td>• Getting Started Guide</td>
</tr>
<tr>
<td></td>
<td>• Quick Start Guide</td>
</tr>
<tr>
<td></td>
<td>• Image Management Guide</td>
</tr>
<tr>
<td></td>
<td>• User license agreement</td>
</tr>
</tbody>
</table>

**Terminology**

The following Smart-1 terms are used in this guide:

- **Security Gateway**: The security engine that enforces the organization’s security policy and acts as a security enforcement point.

- **Security Policy**: The policy created by the system administrator that regulates the flow of incoming and outgoing communication.

- **Security Management server**: The server used by the system administrator to manage the security policy. The organization’s databases and security policies are stored on the Security Management server and downloaded to the gateway. Smart-1 is a Security Management server.

- **SmartConsole**: GUI applications that are used to manage various aspects of security policy enforcement. For example, SmartView Tracker is a SmartConsole application that manages logs.

- **SmartDashboard**: A SmartConsole GUI application that is used by the system administrator to create and manage the security policy.
• **Management High Availability (HA):** Refers to a configuration in which a primary Security Management server has one or more backup secondary Security Management servers which are ready to take over in case of failure of the primary Security Management server.

**SmartEvent Terminology**

• **SmartEvent and Reporter Suite:** Includes SmartEvent and SmartReporter.
  
  • **SmartEvent:** A system that reads logs and generates events based on an Event Policy. An IPS event-only version is also available. Based on the configuration, SmartEvent contains these components:
  
  ▪ **SmartEvent Client** (or **SmartEvent Intro Client**): A GUI that displays events (or IPS events) in many graphical, list and map forms and provides user control of the policy.
  
  ▪ **SmartEvent Server** (or **SmartEvent Intro Server**): Holds the event (or IPS event) database, event queries, object values and policy definition.
  
  ▪ **SmartEvent Correlation Unit:** An engine which reads logs and creates events.

• **SmartReporter:** A system that reads logs and generates statistical and data reports. SmartReporter contains these components:
  
  ▪ **SmartReporter Client:** A GUI to generate, define and display reports.
  
  ▪ **SmartReporter Server:** Contains reports, report definitions and report schedules.
  
  ▪ **Log Consolidator:** Reads logs, consolidates them according to the consolidation policy and adds them to the SmartReporter database.

**Multi-Domain Security Management/Provider-1 Terminology**

The following terms relate to **Multi-Domain Security Management**:

• **Multi-Domain Server:** The Multi-Domain Server houses Multi-Domain Security Management system information including details of the Multi-Domain Security Management deployment, its administrators and customer management datum. There are two Multi-Domain Server types: the Manager, which runs the Multi-Domain Security Management deployment, and the Container, which holds the Domain Management Server. The Manager is the administrator’s entry point into the Multi-Domain Security Management environment. A Multi-Domain Server can be a Manager, a Container, or both.

• **Domain Management Server:** The Multi-Domain Security Management equivalent of the Security Management Server for a single customer. Through the Domain Management Server, an administrator creates security policies and manages the customer gateways.

• **SmartDomain Manager:** The primary interface used to handle customer security management by Multi-Domain Security Management administrators. The SmartDomain Manager is used to update Customer and gateway information, and to assign and navigate between global policies.
Changes in Multi-Domain Security Management/Provider-1 Terminology

These product names changed starting with R75. The changed names are used throughout this guide:

<table>
<thead>
<tr>
<th>Name Before R75</th>
<th>Name Starting with R75 (Used in this Guide)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider-1</td>
<td>Multi-Domain Security Management</td>
</tr>
<tr>
<td>Provider-1 MDG</td>
<td>SmartDomain Manager</td>
</tr>
<tr>
<td>Multi-domain server (MDS)</td>
<td>Multi-Domain Server</td>
</tr>
<tr>
<td>Customer</td>
<td>Domain</td>
</tr>
<tr>
<td>Customer Management Add-on (CMA)</td>
<td>Domain Management Server</td>
</tr>
<tr>
<td>Customer Log Module (CLM)</td>
<td>Domain Log Server</td>
</tr>
<tr>
<td>Multi-Domain Log Module (MLM)</td>
<td>Multi-Domain Log Server</td>
</tr>
</tbody>
</table>
These instructions show how to install Smart-1 50 and 150 in a standard 19 inch rack.

Safety Instructions

Before installing your appliance in a rack cabinet, review the following guidelines:

- Make sure that the room air temperature is below 35°C (95°F).
- Do not block any air vents. Normally, 15 cm (6 in.) of air space in the rear and 5 cm (2 in.) in the front provides proper airflow.
- Install the appliances in the cabinet starting at the bottom and going up.
- Install the heaviest appliance at the bottom of the rack cabinet.
- Do not extend more than one device out of the rack cabinet at the same time.
- Connect the server to a properly grounded outlet.
- Do not overload the power outlet when installing multiple devices in the rack cabinet.
Determining Space and Weight Requirements

Allow sufficient vertical space in the rack for the appliance:

<table>
<thead>
<tr>
<th>Model</th>
<th>Height</th>
<th>Weight (Kg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart-1 50</td>
<td>2U (3.5 inch , 88.9 mm)</td>
<td>28</td>
</tr>
<tr>
<td>Smart-1 150</td>
<td>3U (5.25 inch, 133.3 mm)</td>
<td>38</td>
</tr>
</tbody>
</table>

⚠️ Important - The Smart-1 appliance is very heavy. To lift and install it:
- Two people are required for Smart-1 50.
- Three people are required for Smart-1 150.

The distance from the center of any hole to the center of the third hole above it is equivalent to 1U.

The mounting holes in a standard 19-inch (482.6 mm) server rack rail are arranged as follows:

When installing appliances, start measuring from the center of the two holes with closer spacing. Otherwise, the screw holes on the appliance may not match those on the rack.
# Rack Mounting Hardware and Tools

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Qty.</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Appliance rail</td>
<td>2</td>
<td>Attaches to the Smart-1 50/150 appliance. Both rails are identical.</td>
</tr>
<tr>
<td>(2)</td>
<td>Mounting Bracket</td>
<td>2</td>
<td>Attaches to the rack vertical rails. Both brackets are identical.</td>
</tr>
<tr>
<td>(3)</td>
<td>Screws for Rack Mounting</td>
<td>8</td>
<td>Secures the mounting bracket to the rack vertical rails</td>
</tr>
<tr>
<td>(4)</td>
<td>Square washers for rack mounting</td>
<td>8</td>
<td>Secures the mounting bracket to the rack vertical rails.</td>
</tr>
<tr>
<td></td>
<td>mounting screws</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Round washers for rack mounting</td>
<td>8</td>
<td>Secures the mounting bracket to the rack vertical rails.</td>
</tr>
<tr>
<td></td>
<td>screws</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Qty.</td>
<td>Use</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------</td>
<td>------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>(5)</td>
<td>Screws for Smart-1 50 M3*6</td>
<td>8</td>
<td>Secures the appliance rail to Smart-1 50</td>
</tr>
<tr>
<td>(6)</td>
<td>Screws for Smart-1 150 #6-32*6</td>
<td>6</td>
<td>Secures the appliance rail to Smart-1 150</td>
</tr>
<tr>
<td></td>
<td>Appliance bracket ear for Smart-1 50</td>
<td>2</td>
<td>Attaches to the Smart-1 50 front panel. Both bracket ears are identical.</td>
</tr>
<tr>
<td></td>
<td>Screw for Smart-1 50 appliance bracket ear</td>
<td>6</td>
<td>Attaches the Smart-1 50 bracket ears to the appliance</td>
</tr>
<tr>
<td></td>
<td>Handle for Smart-1 150</td>
<td>2</td>
<td>Attaches to the Smart-1 150 front panel. Both handles are identical.</td>
</tr>
<tr>
<td></td>
<td>Screw for Smart-1 150 handle</td>
<td>4</td>
<td>Attaches the Smart-1 150 handles to the appliance</td>
</tr>
</tbody>
</table>

**Rack Mounting Tools**

- Philips screwdriver. A magnetic head is recommended to hold screws in place and retrieve dropped screws. A powered screwdriver is useful.

**Disconnecting the Appliance Rail from the Mounting Bracket**

Disconnect the appliance rail from the mounting bracket.

You don't need to do this in the server room.

1. Fully extend the combined appliance rail and mounting bracket.
2. Press plastic release catch in the direction of the arrow to disconnect the appliance rail from the mounting bracket.
Attaching the Appliance Rails to the Appliance

Attach the Appliance Rails to the Appliance. Use the same appliance rails for Smart-1 50 and for Smart-1 150.

You don't need to do this in the server room.

1. Identify the front of an appliance rail. One end of the rail is marked with FRONT.
2. Position the appliance rail on the side of the appliance:
   a) Line up the front end of the rail with the front panel of the appliance,
   b) Slide the appliance rail backwards until the correct holes in the appliance rail line up with the holes in the side of the appliance:
      ▪ On the Smart-1 50, line up the four holes marked 50 with the holes in the appliance.
      ▪ On the Smart-1 150, line up the three holes marked 150 with the holes in the appliance.
3. Attach the appliance rail to the side of the Smart-1 appliance.
   - For Smart-1 50 use four M3*6 screws
   - For Smart-1 150 use three #6-32*6 screws
4. Repeat for the other side of the appliance.
Attaching the Appliance Handles or Bracket Ears (Optional)

The appliance ear bracket (for Smart-1 50) and the appliance handles (for Smart-1 150) are optional. Use them as a

- Handle, to make it easier to grab the front of appliance and slide it in and out. The Smart-1 150 is very heavy. You can use the handles to help move and lift the appliance.
- Buffer that prevents the appliance jamming in the rack in the closed position.

You can also use the appliance ear brackets to prevent the appliance from sliding in and out of the rack, by attaching the bracket ears to the rack vertical rail.

You don’t need to be in the server room to attach the appliance handles or ear brackets to the appliance.

To connect the appliance bracket ears or handles to the front of the appliance:

1. Attach the appliance ear bracket to one side of the appliance. For Smart-1 50 use three screws. For Smart-1 150 use two screws.
2. Repeat for the other side of the appliance.

Attaching the Mounting Brackets to the Rack

Attach the mounting brackets to the rack:

1. While standing in the front of the rack, place a mounting bracket in position on one side of the rack
2. Attach the mounting bracket to the rack vertical rail at the front using two screws:
   a) Place a round washer on a rack mounting screw, then a square washer
   b) Attach the mounting bracket to the rack vertical rails using the screw and washers. For now, do not fully tighten the screw.
c) Repeat for the second screw.

3. Go to the back of the rack.
4. Attach the mounting bracket to the rack vertical rail at the back using the same number of screws and washers. Tighten the two screws normally.

5. Go the front of the rack.
6. Tighten the two screws that attach the mounting bracket to the rack vertical rail.
7. Repeat for the other side of the rack: Attach the mounting bracket to the other side of the rack.

Installing Smart 1 50/150 in the Rack

Carefully install the Smart-1 50/150 in the rack.

⚠️ **Important** - The Smart-1 appliance is very heavy. To lift and install it:

- Two people are required for Smart-1 50.
- Three people are required for Smart-1 150.
1. Line up the appliance rail on the appliance with the mounting bracket rails.

2. Carefully slide the appliance into the mounting bracket rails.
3. Push the appliance in until the appliance locks in the rails.
Chapter 3

Configuring Smart-1

In This Chapter

Connecting the Power Cables and Power On 27
Available Software Images 28
Using the First Time Configuration Wizard 28
Using the First Time Configuration Wizard on Gaia 29
Using the First Time Configuration Wizard on SecurePlatform 34
Using the First Time Configuration Wizard on Multi-Domain Server 38
Installing the SmartConsole GUI Clients 41
Advanced Configuration 42
Migration from Existing Provider-1 Machines 42

The basic workflow for configuring Smart-1 is:

1. Connect the cables and power on.
2. Perform the initial configuration using the First Time Configuration Wizard.
3. Install the SmartConsole GUI clients.

Connecting the Power Cables and Power On

1. Connect the power cable(s).
2. Turn on the Power button to start the appliance.

Note - When a power supply fails or is not connected to the outlet, an alarm sounds continuously. If you hear the alarm, check that all power supplies are connected to the outlets. If needed, replace the faulty power supply immediately, and connect the new unit to the A/C outlet. See "Removing the Power Supply (on page 55)".
Available Software Images

Smart-1 comes with multiple software images. Select the software image that you want to use.

Reverting to a software image takes a few minutes. To follow the progress and see when the appliance is ready, connect to the appliance using a serial console.

For more about software images, see the Smart-1 Image Management Guide for the applicable version (http://support.checkpoint.com).

Note - Gaia is available for R75.40 and higher.

Using the First Time Configuration Wizard

Do the initial configuration with the First Time Configuration Wizard. Smart-1 150 appliances use the Multi-Domain Server First Time Configuration Wizard.

For Smart-1 50 appliances, the First Time Configuration Wizard options depend on whether your appliance is running on the Gaia or the SecurePlatform operating system.

Go to the applicable section:

- Using the First Time Configuration Wizard on Gaia (on page 29)
- Using the First Time Configuration Wizard on SecurePlatform (on page 34)
Using the First Time Configuration Wizard on Gaia

Use the First Time Configuration Wizard to do the initial configuration of the Gaia appliance.

Note - The pages that you see in the wizard depend on the software image and the options you select. You will not see all the pages that are in this section.

Starting the Gaia First Time Configuration Wizard

To start the First Time Configuration Wizard:

1. Connect a standard network cable to the appliance management interface and to your management network.
   
   The management interface is marked MGMT. This interface is preconfigured with the IP address 192.168.1.1.

2. Connect to the management interface from a computer on the same network subnet.
   
   For example: IP address 192.168.1.x and net mask 255.255.255.0. This can be changed in the WebUI, after you complete the First Time Configuration Wizard.

3. To access the management interface, open a connection from a browser to the default management IP address: https://192.168.1.1.

4. The login page opens. Log in to the system using the default username and password: admin and admin.

5. Click Login.

   Note - The features configured in the First Time Configuration Wizard are accessible after completing the wizard using the WebUI menu. The WebUI menu can be accessed by navigating to https://<appliance_ip_address>.

6. The First Time Configuration Wizard runs.

Welcome

The Welcome page introduces the product.
Available Releases

The appliance comes with different software images. Select the software image that you want to install. You can change to another software image after the First Time Configuration Wizard is completed.

If you select a SecurePlatform software image, use the SecurePlatform First Time Configuration Wizard to configure the appliance.

Authentication Details

The default password gives you access to the appliance. For security purposes, change it to a more secure password.

Date and Time Setup

Set the system time and date for the appliance:

- Manually
- From a time server, using Network Time Protocol (NTP)

Device Name

Set the host name, domain name, and DNS servers for IPv4 addresses. The host name must start with a letter and cannot be named com1, com2,...,com9.

You can use the Gaia WebUI to configure IPv6 DNS servers.
**Network Connection**

**Connection Information** - Configure the IPv4 interface information for the management interface. You can change the Management IP address. Connectivity is maintained with an automatically created secondary interface. After you complete the First Time Configuration Wizard, you can remove this interface in the **Interface Management > Network Interfaces** page.

**DHCP Server** - You can configure the Gaia appliance to be a Dynamic Host Configuration Protocol (DHCP) server.

To define a DHCP server on the Gaia appliance MGMT interface:
1. In **DHCP Server**, select **Enabled**.
2. Define the **IP Pool**. This is the range of IPv4 addresses that the server assigns to hosts.

![First Time Configuration Wizard](image)

**Appliance Type**

Define the appliance type:

- Smart-1 appliance - Security Management server with SmartEvent
- Smart-1 SmartEvent appliance - Dedicated server for SmartEvent
Products

Products

- **Security Management** - The server used by the system administrator to manage the security policy. The organization’s databases and security policies are stored on the Security Management server and downloaded to the Security Gateway.

Advanced

- **Define Security Management as** - In a Management High Availability deployment, define this Security Management server as *Primary* or *Secondary*. For more about Management High Availability, see the applicable version of the *Security Management Administration Guide*.

Search for these guides in the Support Center ([http://supportcontent.checkpoint.com/solutions?id=sk67581](http://supportcontent.checkpoint.com/solutions?id=sk67581)).

Security Management Administrator

- **Note** - You only see this page when the Gaia appliance is a Security Management server.

Define the name and password of an administrator that can connect to the Security Management server using SmartConsole clients.

Security Management GUI Clients

- **Note** - You see this page when the appliance is a Security Management.

Define the clients that are allowed to connect to the appliance using a web browser or SSH client. These clients can manage the appliance using a web or SSH connection. For security reasons, we recommend that you do not use the *Any IP address* option.

Secure Internal Communication (SIC)

Define the Secure Internal Communication (SIC) *Activation Key*. The same key is used by the gateway object in SmartDashboard.

Summary

Click **Finish** to complete the First Time Configuration Wizard and configure the appliance. You can log in to the WebUI after some minutes.
Note - We recommend that you back up the system configuration. You can use the Gaia add backup command.
Using the First Time Configuration Wizard on SecurePlatform

Do the initial configuration of the SecurePlatform appliance with the First Time Configuration Wizard.

Note - The pages that you see in the wizard depend on the software image and the options you select. You will not see all the pages that are in this section.

Starting the First Time Configuration Wizard

1. Connect a standard network cable to the appliance’s management interface and to your management network.
   The management interface is marked MGMT. This interface is preconfigured with the IP address 192.168.1.1.

2. Connect to the management interface, from a computer on the same network subnet as the management interface.
   For example: IP address 192.168.1.x and netmask 255.255.255.0. This can be changed in the WebUI.

3. To access the management interface, open a connection from a browser to the default management IP address: https://192.168.1.1:4434.
   Note - Pop-ups must always be allowed on https://<appliance_ip_address>.

   The login page opens.

4. Log in with the default system administrator login name/password: admin/admin, and click Login.
   Note - The features configured in the wizard are accessible after completing the wizard via the WebUI menu. The WebUI menu can be accessed by navigating to https://<appliance_ip_address>:4434.

5. Change the administrator password, as prompted.
   The default password is provided to allow you access to Smart-1. For security purposes, you must change it to a more secure password.

6. In the Password recovery login token section, you can download a Login Token that can be used in the event a password is forgotten.
   We recommend that you save and store the password recovery login token file in a safe place.
The First-Time Configuration Wizard runs. The Wizard presents a number of windows, in which you are prompted to configure Smart-1.

Welcome
The Welcome page summarizes the steps of the First Time Configuration Wizard.

Appliance Date and Time Setup
Configure date and time in the Date and Time Setup page. Click Apply.

Network Connections
Configure the network connections in the Network Connections page.

Routing Table
Configure the routing settings on the Routing Table page.

DNS and Domain Settings
Set the Host, Domain and DNS Servers in the DNS and Domain Settings page.
The host name must start with a letter and cannot be named Com1, Com2, …, Com9.
Security Management Installation Type

Note - This page is only available in R75 or higher.

In the Installation Type page:

- **Security Management**: Configure Smart-1 as a Security Management server with all the management Software Blades, including SmartEvent.

- **Eventia Suite** (SmartEvent and Reporter Suite): Configure Smart-1 as a dedicated server for SmartEvent, and no other Software Blade. SmartEvent and Reporter Suite contains SmartReporter Server, SmartEvent Server, and SmartEvent Correlation Unit.

Security Management

If you choose to install a Security Management server, in the Security Management page:

- **Primary Security Management** is the Security Management server that will normally be active. To set up a Security Management server in a non-Management HA deployment,
choose this option. In a Management HA deployment, if the Primary Security Management server fails, the Secondary Security Management server takes over.

- **Secondary Security Management** is the Security Management server that takes over if the Primary Security Management server fails. This option applies only in a Management HA deployment.

- **Log Server** is the repository for log entries generated on gateways. Check Point gateways send their log entries to the Log Server.

**SmartEvent and SmartReporter Suite Installation Type**

Configure the SmartEvent and Reporter Suite applications to run on the server.

![SmartEvent and SmartReporter Suite Installation Type](image)

**SmartEvent**: A system that reads logs and generates events based on an Event Policy. An IPS event-only version is also available. **SmartReporter** is a system that reads logs and generates statistical and data reports. Choose one or more of these server components:

- **SmartReporter Server**: Contains reports, report definitions and report schedules.
- **SmartEvent Server**: Holds the event (or IPS event) database, event queries, object values and policy definition.
- **SmartEvent Correlation Unit**: An engine which reads logs and creates events.

For SmartEvent Intro, select both **SmartEvent Server** and **SmartEvent Correlation Unit**.

**Web/SSH and GUI Clients Configuration**

Define the clients that are allowed to connect to Smart-1 appliance using a Web browser, SSH client, or SmartConsole applications.

You can define a **Host** according to **Hostname** or **IP address**. Enter **Any** to manage Smart-1 from anywhere.

**Note** - It is not recommended to use the **Any** value for security reasons.

Additional options are available via the **WebUI** menu, after you complete the First Time Configuration Wizard.
Secure Internal Communication

If necessary, define the Secure Internal Communication (SIC) Activation Key that is used by the gateway object in SmartDashboard.

Download SmartConsole Applications

Configuring a security policy requires you to install the SmartConsole applications. In the Download SmartConsole Applications window, you can download SmartConsole and install it on Windows machines. For a detailed list of supported Windows operating systems for SmartConsole refer to the release notes of your Check Point version in the Check Point Support Center (http://supportcenter.checkpoint.com).

Summary

The Summary page appears.

Click Finish to complete the First-Time Configuration Wizard. The Appliance automatically restarts. This may take several minutes.

Note - It is recommended to backup the system configuration for system recovery purposes. The backup menu can be accessed via the WebUI interface under the Appliance menu.

Using the First Time Configuration Wizard on Multi-Domain Server

Use the First Time Configuration Wizard to do the initial configuration of the Multi-Domain Server Smart-1 appliance.

Note - The pages that you see in the wizard depend on the software image and the options you select. You will not see all the pages that are in this section.

Appliance Date and Time Setup

Configure date and time in the Date and Time Setup page. Click Apply.
Network Connections

Configure the network connections in the Network Connections page.

You can change the Management IP address. Connectivity is maintained with an automatically created secondary interface. You can remove this interface after you complete the First Time Configuration Wizard in the Network > Network Connections page.

Routing Table

Configure the routing settings on the Routing Table page.

DNS and Domain Settings

Set the Host, Domain and DNS Servers in the DNS and Domain Settings page.

The host name must start with a letter and cannot be named Com1, Com2, … , Com9.

Web/SSH and GUI Clients Configuration

Define the clients that are allowed to connect to Smart-1 appliance using a Web browser, SSH client, or SmartConsole applications.

You can define a Host according to Hostname or IP address. Enter Any to manage Smart-1 from anywhere.

Note - It is not recommended to use the Any value for security reasons.

Additional options are available via the WebUI menu, after you complete the First Time Configuration Wizard.
Multi-Domain Security Management Installation Type

- **Multi-Domain Server**: Configure Smart-1 with the Multi-Domain Server system information including details of the Multi-Domain Server deployment, its administrators and customer management.

- **Multi-Domain Log Server**: Configure Smart-1 to host the Domain Log Server (virtualized log servers).

Multi-Domain Server Configuration

- **Primary Multi-Domain Server**: Configure Smart-1 as a Multi-Domain Server in a non-High Availability deployment.
  
  For a High Availability deployment, configure Smart-1 as the primary Multi-Domain Server.

- **Secondary Multi-Domain Server**: Configure Smart-1 as the secondary Multi-Domain Server in a High Availability deployment.
Multi-Domain Security Management Administrator

Define the Multi-Domain Server administrator that is a Multi-Domain Server Superuser.

Secure Internal Communication

If necessary, define the Secure Internal Communication (SIC) Activation Key that is used by the gateway object in SmartDashboard.

Download SmartConsole Applications

Configuring a security policy requires you to install the SmartConsole applications. In the Download SmartConsole Applications window, you can download SmartConsole and SmartDomain Manager to install on Windows computers.

For more about the compatible Windows operating systems for SmartConsole and SmartDomain Manager, see the Release Notes of your version in the Check Point Support Center (http://supportcenter.checkpoint.com).

Summary

The Summary page appears.

Click Finish to complete the First-Time Configuration Wizard. The Appliance automatically restarts. This may take several minutes.

Note - It is recommended to backup the system configuration for system recovery purposes. The backup menu can be accessed via the WebUI interface under the Appliance menu.

Installing the SmartConsole GUI Clients

1. The WebUI menu can be accessed by navigating to https://<appliance_ip_address>:4434.
2. Login using the administrator username and password configured in step 4 of the Advanced Initial Configuration step.
3. Download the SmartConsole Installation package Product Configuration > Download SmartConsole > Download.
4. If Multi-Domain Security Management is deployed, follow the same procedure to download the SmartDomain Manager.

You have now completed the Smart-1 configuration.

To start working with your Smart-1 appliance as a Security Management Server refer to the Security Management Server Administration Guide.
To start working with your Smart-1 appliance as Multi-Domain Security Management, refer to the *Multi-Domain Server Administration Guide*.

## Advanced Configuration

### Advanced configuration on SecurePlatform

Advanced configuration on SecurePlatform can be done using the `sysconfig` menu which can be accessed using the command line interface only. For example, configuring the appliance to be a DHCP server.

*Note - The `sysconfig` menu is only available after running the First Time Configuration Wizard in the WebUI.*

CLI access can be obtained by console connection or through SSH.

### Advanced configuration on Gaia (Only for Smart-1 50)

Advanced configuration on Gaia can be done using the WebUI or the CLI.

CLI access can be obtained by console connection or through SSH.

## Connecting to the Smart-1 CLI

You can connect to the command line interface of the Smart-1 appliance using:

- The provided serial console cable (DTE to DTE) and terminal emulation software such as HyperTerminal (from Windows) or Minicom (from Unix/Linux systems).
  
  Connection parameters for Smart-1 appliances are: 9600bps, no parity, 1 stop bit (8N1), flow control *None*.

- An SSH connection to the management interface (if SSHD is configured).

## Migration from Existing Provider-1 Machines

Smart-1 introduces a simple and easy to use tool that enables migration from existing NGX R65 and higher Provider-1 machines into the Smart-1 appliance.

This script exports the entire existing MDS database into one .tgz file on the source machine that can be imported to the Smart-1 machine.

**To migrate from an existing NGX R65 and higher Provider-1 machine into the Smart-1 appliance:**

Before starting the migration:
The exported configuration is approximately the size of the MDS installation. Therefore, before starting the migration make sure you have enough free disk space on the source and target machines.

**On the source machine:**

1. Get the `p1_upgrade_tools.tgz` package  
   ([http://supportcontent.checkpoint.com/solutions?id=sk43266](http://supportcontent.checkpoint.com/solutions?id=sk43266)).

2. Extract the package contents

3. Run the `export_mds.sh` tool (make sure it has executable permissions)

   ```bash
   # export_mds.sh <path to store exported mds configuration>
   ```

**On the Smart-1 appliance:**

1. Verify that no customers are defined, and that there are no global objects and policies on the Smart-1 machine. Administrators and/or GUI clients will be overwritten.

2. Transfer the exported mds file to the `/var` partition on the Smart-1 machine.

3. Run the import tool:

   ```bash
   # $MDS_SYSTEM/install/mds_import.sh <full path to the imported configuration>
   ```

4. Start the mds.

   Note that the first start-up of the mds after import takes considerably longer than subsequent start-ups.
Chapter 4

Configuring SmartEvent

In This Chapter

Preparing SmartEvent on Security Management Server 45
Preparing SmartEvent on the Multi-Domain Server 46
Enabling Connectivity with Multi-Domain Security Management 47
Configuring the SmartEvent Clients 47

This section explains how to get up and running with SmartEvent.

Preparing SmartEvent on Security Management Server

To configure SmartEvent, first establish connectivity between the components.

1. Launch SmartDashboard.
2. In SmartDashboard, create a new host for each computer that contains a component of SmartEvent:
   a) Select Manage > Network Object > New > Check Point > Host
   b) In the General Properties window, click Communication and enter the activation key.
   Note - If the Security Management Server and SmartEvent are installed on different sides of the firewall, add a rule that allows SIC traffic between them.
   c) The version is not entered automatically if the SmartEvent version is newer than the version of the Security Management Server. If so, select the most recent version available from the Version drop-down list.
   d) In the Management Software Blades list, select the blades that are installed on the new host.
3. Install the database on all log servers from which SmartEvent reads data: select Policy > Install Database and select the log servers as the targets.
4. To allow the SmartEvent Intro server to block attacks from specific IP addresses, configure the Security Management Server to accept SAM commands from the SmartEvent Intro server:

   a) On the Security Management Server, edit the `$CPDIR/conf/sic_policy.conf` file:
      Search for the section `[Inbound rules]`, and add the following line under `# sam proxy`:
      
      DN_Mgmt ; Reporting_Tool; ANY; sam ; sslca

   b) From the command line in the Security Management Server computer, run the following commands:
      
      `cpstop`
      `cpstart`

---

**Preparing SmartEvent on the Multi-Domain Server**

The first stage configuring SmartEvent is to establish connectivity between the components.

1. Launch Global SmartDashboard.

2. In SmartDashboard, create a new host for each computer that contains a component of SmartEvent:
   a) Select **Manage > Network Object > New > Check Point > Host**
   b) In the **General Properties** window, click **Communication** and enter the activation key.

   **Note** - If the Multi-Domain Server and SmartEvent are installed on different sides of the firewall, add a rule that allows SIC traffic between them.

   c) The version is not entered automatically if the SmartEvent version is newer than the version of the Multi-Domain Server. If so, select the most recent version available from the **Version** drop-down list.

   d) In the **Management Software Blades** list, select the blades that are installed on the new host.

3. Select **Close** and **OK**.

4. From the **File** menu, select **Save**.

5. From the SmartDomain Manager:
   a) Do **Install Global Policy** on all CMAs participating with SmartEvent.
   b) For each CMA participating with SmartEvent, open its SmartDashboard, select **Policy > Install Database**, and select only the Log Servers and the CMA from which you want the SmartEvent Intro or SmartReporter components to read logs.
Enabling Connectivity with Multi-Domain Security Management

1. Open the SmartEvent Intro client, go to Policy tab > General Settings > Objects > Customers, and add all the CMAs with which you will be working.
2. Objects will be synchronized from the CMAs. The synchronization progress can be monitored from the status window in the Overview pane.

Configuring the SmartEvent Clients

You must perform these configurations to make the components of the SmartEvent functional.

After you have accomplished the tasks for SmartEvent Intro, events will begin to appear in the SmartEvent Intro client.

After you have accomplished the tasks for SmartReporter, logs will be created and sent to the SmartReporter database. Reports can then be created.

Defining the Internal Network for SmartEvent

To help SmartEvent Intro determine whether events originated internally or externally, the Internal Network must be defined. Certain network objects are copied from the management server to the SmartEvent Intro server during the initial synchronization and updated afterwards periodically. Define the Internal Network from these objects.

Note - If running SmartEvent Intro in a Security Management Server environment, the internal network will be defined automatically from firewall topology information. You can customize the internal network definition.

In a Multi-Domain Security Management environment, define an internal network for each CMA.

To define the Internal Network:
1. Start the SmartEvent Intro Client.
2. From the Policy view, select General Settings > Initial Settings > Internal Network.
3. Add objects (hosts, networks, groups, IP ranges) that define your environment's internal network.

Defining Correlation Units and Log Servers for SmartEvent

1. From the Policy view of the SmartEvent Intro client, select General Settings > Initial Settings > Correlation Units.
2. Select Add.
Configuring SmartEvent

3. Click the button of the **Correlation Unit** field.
4. In the **Select Objects** window, select a Correlation Unit.
   
   **Note** - In a Multi-Domain Security Management environment, add the log servers for each CMA.

5. Click **OK**.
6. Click **Add** and select the Log Servers available as data sources to the Correlation Unit.
7. Select **Save**.
8. From the **Actions** menu, select **Install Events policy**.

At this point, SmartEvent Intro will begin to read logs and detect events.

To learn how to manage and fine-tune the system using the SmartEvent Intro Client, see the **SmartEvent Administration Guide** for your software version on the Check Point Support Center (http://supportcenter.checkpoint.com).

---

Creating a Consolidation Session for SmartReporter

The Consolidation session reads logs from the log server and adds them to the SmartReporter database.

- If there is a single log server in the environment, the Consolidation session is automatically created.
- If there is more than one log server, you must create the Consolidation session for each log server.

**To create a Consolidation session:**

1. In the **Selection Bar** view, select **Management > Consolidation**.
2. Select the **Sessions** tab.
3. Click **Create New** to create a new session.
   
   The **New Consolidation Session** window appears.
4. Select the log server from which logs will be collected and will be used to generate reports.
5. Click **Next**.
   
   The **New Consolidation Session** window appears.
6. Choose whether to use the default source logs and database tables, or select custom source logs and database tables for consolidation.

If you selected **Select default log files and database**, click **Finish** to complete the process. The source of the reports will be preselected logs. The report data will be stored in the default database table named CONNECTIONS. The preselected logs are the sequence of log files that are generated by Check Point products. The preselected logs session will begin at the beginning of the last file in the sequence, or at the point the sequence was stopped.

If you want to customize the Consolidation session refer to the **SmartReporter Administration Guide** for your software version on the Check Point Support Center (http://supportcenter.checkpoint.com).

---
Chapter 5

Smart-1 Hardware

In This Chapter

Smart-1 50 Front Panel 52
Smart-1 150 Front panel 53
LCD Display Screen 53
Customer Replaceable Parts 55

This chapter provides instructions for installing and removing hardware components on the Smart-1 appliance.
# Smart-1 50 Front Panel

![Smart-1 50 Front Panel Diagram](image)

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LCD display screen</td>
</tr>
<tr>
<td>2</td>
<td>Screen operation keys</td>
</tr>
<tr>
<td>3</td>
<td>USB ports</td>
</tr>
<tr>
<td>4</td>
<td>Console port - for a serial connection to the appliance using a terminal emulation program such as HyperTerminal</td>
</tr>
<tr>
<td>5</td>
<td>LOM (Lights-out Management) port</td>
</tr>
<tr>
<td>6</td>
<td>Management configuration port</td>
</tr>
<tr>
<td>7</td>
<td>Built-in ethernet ports (Lan1-Lan3)</td>
</tr>
<tr>
<td>8</td>
<td>slot for optional fiber channel SAN card. For setup instructions see sk43364 (<a href="http://supportcontent.checkpoint.com/solutions?id=sk43364">http://supportcontent.checkpoint.com/solutions?id=sk43364</a>)</td>
</tr>
<tr>
<td>9</td>
<td>4 hard disk drives</td>
</tr>
</tbody>
</table>
Smart-1 150 Front panel

1. USB ports
2. LOM (Lights-out Management) port
3. Console port - for a serial connection to the appliance using a terminal emulation program such as HyperTerminal
4. Management configuration port
5. Built-in ethernet ports (Lan1-Lan3)
7. 12 hard disk drives
8. LCD display screen
9. Screen operation keys

**LCD Display Screen**

Smart-1 appliances (other than Smart-1 25) have an LCD screen that can be used to perform basic management operations. The management IP address, netmask and default gateway of
the Check Point appliance can be configured. The appliance can also be rebooted and shut down.

**LCD Screen Operation Keys**

<table>
<thead>
<tr>
<th>To</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the main menu</td>
<td>⬆</td>
</tr>
<tr>
<td>Navigate within the menu</td>
<td>↖ or ↗</td>
</tr>
<tr>
<td>Select a menu option</td>
<td>⬆</td>
</tr>
<tr>
<td>Go back to a previous menu</td>
<td>⬇</td>
</tr>
</tbody>
</table>

**Menu Options**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Sub-menu</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set MGMT IP</td>
<td>Set the management interface's IP address</td>
</tr>
<tr>
<td></td>
<td>Set Netmask</td>
<td>Set the management interface's network mask</td>
</tr>
<tr>
<td></td>
<td>Set Default GW</td>
<td>Set the management interface's default gateway</td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reboot</td>
<td>Reboot the appliance</td>
</tr>
</tbody>
</table>

**When Entering an IP Address**

<table>
<thead>
<tr>
<th>To</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move to the next digit</td>
<td>⬆</td>
</tr>
<tr>
<td>Move back to the previous digit</td>
<td>⬇</td>
</tr>
<tr>
<td>Approve the change</td>
<td>⬆ when cursor is located on the last digit</td>
</tr>
<tr>
<td>Cancel the IP change</td>
<td>⬇ when cursor is located on the first digit</td>
</tr>
<tr>
<td>To</td>
<td>Press</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>Change current digit</td>
<td>✰ or ✦</td>
</tr>
</tbody>
</table>

**Customer Replaceable Parts**

To ensure maximum availability and ease of maintenance, the Smart-1 appliance contains the following customer replaceable parts:

- **Smart-1 50:**
  - Two power supplies
  - Four hard disk drives
  - Two cooling fans

- **Smart-1 150:**
  - Three power supplies
  - Up to twelve hard disk drives
  - Three cooling fans

Unless directed to do so by Check Point technical support, customers are prohibited by warranty and support agreements from replacing any parts. Customers are prohibited from opening the Smart-1 case under any circumstances.

**Power Supplies**

This section presents the procedures for removing and installing a power supply unit. It is not necessary to power off the appliance before adding or removing a power supply.

**Removing the Power Supply**

**To remove a power supply unit:**

1. If the power supply alarm sounds, press the red alarm button to the right of the power supply. This will stop the alarm.
2. Remove the power cord.
3. Loosen the retaining screw located above the power socket.
4. Pull the extraction handle to remove the power supply unit.

**Note** - Use only the extraction handle to remove the power supply unit. To prevent damaging the power supply, do not pull on the retaining screw, power cord clip or any other part of the unit.
Installing the Power Supply

To install a replacement power supply:
1. Insert the power supply into its slot and push firmly until it clicks into place.
2. Tighten the retaining screws.
3. Insert the power cord.

Hard Disk Drives

Smart-1 50 contains 4 hot-swappatable redundant hard disk drives (RAID 10).

Smart-1 150 can contain up to 12 hot-swappatable hard disk drives.

Implemented by a dedicated LSI Logic RAID controller, Smart-1 performs RAID 10 mirroring and striping across all of the installed hard disk drives.

<table>
<thead>
<tr>
<th>Description</th>
<th>Use the raidconfig SecurePlatform command to perform basic maintenance and monitoring procedures on the Smart-1 RAID array</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>raidconfig [status / rebuild /extendstorage / extendfs / alarmon / alarmoff]</td>
</tr>
<tr>
<td>Parameters</td>
<td>Parameter</td>
</tr>
<tr>
<td></td>
<td>status</td>
</tr>
<tr>
<td></td>
<td>rebuild</td>
</tr>
<tr>
<td></td>
<td>extendstorage</td>
</tr>
<tr>
<td></td>
<td>extendfs</td>
</tr>
<tr>
<td></td>
<td>alarmon</td>
</tr>
<tr>
<td></td>
<td>alarmoff</td>
</tr>
</tbody>
</table>

Removing a Hard Drive

Any single hard disk can be safely removed without risking the integrity of the RAID array or compromising the data.

The hard disk drives are numbered 1-4 on Smart-1 50 from left to right, and 1-12 on Smart-1 150 from left to right, top to bottom. The upper left hard drive is #1, upper right hard drive is #4. On Smart-1 150 the lower right hard drive is #12.
Warning - When removing more than one hard drive, please DO NOT REMOVE both of the hard drives in the following pairs in order to maintain your RAID array integrity:

- In Smart-1 50, hard drives 1+2 or 3+4 should not be removed together.
- In Smart-1 150, also hard drives 5+6, 7+8, 9+10, or 11+12.

For example, you may replace hard disk drives 1+3 or disks 2+4.

To remove a hard disk drive:
1. Unlock the drive.
2. Slide the release latch toward the left.
3. Remove the drive from its slot.

Installing a Hard Disk Drive

To install a hard disk drive:
1. Slide the replacement hard disk drive into the slot.
2. Push the extraction handle until it closes and the drive clicks into place.
3. If the command `raidconfig status` shows that the new hard disk drive is not rebuilding, run the command `raidconfig rebuild` to initiate the rebuild of the RAID array on the new disk drive.

Smart-1 150 Raid Storage

Smart-1 150 can contain up to 12 hard drives. If the appliance has been purchased with less than 12 hard drives and you would like to add more storage capacity, follow the guidelines and instructions below.

RAID Storage Guidelines

- Additional hard drives should always be added in multiples of four - the appliance should always contain 4, 8 or 12 hard drives.
- For each group of 4 hard drives, the RAID controller creates a separate RAID 10 array. The initial setup is 4 hard drives configured in one RAID 10 array.
- When four additional hard drives are inserted, one additional RAID 10 array built of four hard drives will be added.
- When eight additional hard drives are inserted, two additional RAID 10 arrays, each built of four hard drives will be added.
- When less than four additional hard drives are inserted, storage will not be extended.
Smart-1 Hardware

- When more than four but less than eight additional hard drives are inserted, storage will be extended using only four drives, i.e. only one additional four-hard-drive RAID 10 array will be added.

- Additional storage is always added to the /dev/vg_splat/lv_log logical volume.

**Extending Appliance Storage**
1. Disconnect the power from the appliance.
2. Insert the additional hard drives into the appliance according to the guidelines above.
3. Power on the appliance.
4. Wait for the boot process to finish.
5. Make sure that the additional hard drives have been inserted correctly and are recognized by the system by running the command
   ```bash
   /sbin/raidconfig status
   ```
6. Stop all Check Point processes by running `cpstop` or `mdsst`p
7. Stop all other processes that are using `/var/log`. To see a list of these processes, run `lsof /var/log`
8. Add the additional storage to the file system by running the command
   ```bash
   /sbin/raidconfig extendstorage
   ```

In the event that the storage extension process fails:
1. Run the command
   ```bash
   /opt/MegaRAID/MegaCli/MegaCli -CfgForeign -Clear -a0
   ```
2. Repeat steps 5 to 8 above.

**Verifying Hard Drive Extension**
1. Run the `/sbin/raidconfig status` command to view the status of the hard disk drives. Additional hard disk drives should appear configured in additional four discs’ RAID 10 arrays.
2. Run the `lvdisplay /dev/vg_splat/lv_log` command. The additional storage should appear available under this logical volume.

**Cooling Fans**

The Smart-1 appliance contains three cooling fans. Each cooling fan operates independently of the other(s), providing redundancy in the event of failure.

This section presents the procedures for removing and installing a fan unit. It is not necessary to power off the appliance before adding or removing a fan unit.

**Removing Fan Units**

**To remove a fan unit:**
1. Loosen the retaining screws in the corners of the fan assembly.
2. Gently pull the fan unit out of the appliance.

**Installing Fan Units**

**To install a fan unit:**

1. Insert the fan unit into the appliance. Push firmly until it clicks into place.
2. Tighten the retaining screws in the corners of the fan assembly.
Chapter 6

Restoring Factory Defaults

In This Chapter

- Restoring Using the WebUI 61
- Restoring Using the Console Boot Menu 62
- Restoring Using the LCD Panel 63

You may restore the factory default images on the appliance using the WebUI, a console connection application (such as HyperTerminal) or the LCD panel.

⚠️ **Important** - Restoring factory default images will delete all information on the appliance including images, backup files, and logs.

## Restoring Using the WebUI

Use the WebUI of the applicable operating system to restore the appliance to the factory default settings. You can select one of the software images that are available on the appliance.

**Gaia**

Use the Gaia WebUI to restore the default factory settings.

**To restore a Gaia appliance with the WebUI:**

1. Open an Internet browser to the management IP address, `https://<appliance_ip_address>`
2. Log in to the WebUI of the appliance using the administrator username and password.
3. In the WebUI, click **Maintenance > Factory Defaults**
   - The **Factory Defaults** window opens.
4. Select the image version that you are restoring.
5. Click **Apply**.
SecurePlatform

Use the SecurePlatform WebUI to restore the default factory settings.

To restore a SecurePlatform appliance with the WebUI:
1. Open Internet Explorer and navigate to the management IP address, https://<appliance_ip_address>:4434
2. Log in to the WebUI of the appliance using the administrator username and password.
3. In the WebUI, click Appliance > Image Management
   The Image Management window opens.
4. Select the image version that you are restoring.
5. Click Revert.

Restoring Using the Console Boot Menu

To restore the appliance to its default factory configuration using the console boot menu:
1. Connect the supplied DB9 serial cable to the console port on the front of the appliance.
2. Connect to the appliance using a terminal emulation program such as Microsoft HyperTerminal or PuTTY.
3. Configure the terminal emulation program:
   • In the HyperTerminal Connect To window, select a port from the Connect using list.
   • In PuTTY select the Serial connection type.
4. Define the serial port settings: 9600 BPS, 8 bits, no parity, 1 stop bit.
5. From the Flow control list, select None.
6. Connect to the appliance.
7. Turn on the appliance.
8. The appliance initializes and status messages are shown in the terminal emulation program.

<table>
<thead>
<tr>
<th>IDE Channel 2</th>
<th>Master Disk : LBA,ATA 100, 164GB</th>
</tr>
</thead>
</table>

**PCI device listing**

<table>
<thead>
<tr>
<th>Bus No.</th>
<th>Device No.</th>
<th>Func No.</th>
<th>Vendor/Device Class</th>
<th>Device Class</th>
<th>IRQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8086 2772</td>
<td>Display Ctrlr</td>
<td>030</td>
</tr>
<tr>
<td>0</td>
<td>29</td>
<td>0</td>
<td>8086 27CB</td>
<td>USB 1.0/1.1 UHCI Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>0</td>
<td>29</td>
<td>1</td>
<td>8086 27CB</td>
<td>USB 1.0/1.1 UHCI Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>0</td>
<td>29</td>
<td>2</td>
<td>8086 27CB</td>
<td>USB 1.0/1.1 UHCI Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>0</td>
<td>29</td>
<td>3</td>
<td>8086 27CB</td>
<td>USB 1.0/1.1 UHCI Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>0</td>
<td>31</td>
<td>1</td>
<td>8086 27DF</td>
<td>IDE Ctrlr/CIC Ctrlr</td>
<td>0101</td>
</tr>
<tr>
<td>0</td>
<td>31</td>
<td>2</td>
<td>8086 27DC</td>
<td>IDE Ctrlr/CIC Ctrlr</td>
<td>0101</td>
</tr>
<tr>
<td>0</td>
<td>31</td>
<td>3</td>
<td>8086 27DA</td>
<td>SMBus Ctrlr</td>
<td>0105</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>8086 109A</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>8086 109A</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>8086 109A</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>8086 109A</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>8086 109A</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>8086 109A</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>0</td>
<td>8086 1076</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
<tr>
<td>7</td>
<td>13</td>
<td>0</td>
<td>8086 1076</td>
<td>Network Ctrlr</td>
<td>0200</td>
</tr>
</tbody>
</table>

*Verifying DMI Pool Data .............*

**Press any key to see the boot menu (Booting in 4 seconds)**

9. When this message is shown, you have approximately four seconds to hit any key to activate the Boot menu.

10. From the Boot menu, select the relevant **Reset to factory defaults** image.

11. Press **Enter**.

---

**Restoring Using the LCD Panel**

To restore the Smart-1 appliance to its default factory configuration using the LCD Panel keys:

1. Reboot or power on the appliance.
2. When the countdown begins, press any of the arrow keys.

   ![Starting in 5 seconds](image)

   The Boot menu appears.

3. Using the arrow buttons, scroll to the relevant option:
Restoring Factory Defaults

- **Reset to SMC FCD** - for Security Management Server and then press the UP arrow.
- **Reset to PV-1 FCD** - for Multi-Domain Security Management and then press the UP arrow.

4. Confirm the reset by pressing the UP arrow.

![Restore to FCD? Press ↑ to start](image)

**Important** - All data on the appliance will be erased.

Pressing any other key causes the **Action Canceled** message to appear:

![Action Canceled Press any key](image)

At this point, pressing any key returns you to the boot menu.

5. Once you have confirmed the reset, wait for the appliance to restore the factory image. While the appliance is restored to the Software Blades default image, a **Reverting image don’t turn off** message displays continuously.
When the appliance has been restored to its default factory configuration, the appliance reboots and the **Initializing** message appears.

---

**Initializing**

*Please wait...*
This chapter discusses the Lights-Out Management (LOM) integrated card that is supplied with the Smart-1 50/150 appliance and basic configuration options.
**Introduction**

The Check Point Lights Out Management (LOM) is an optional card that you can use with Check Point appliances. You can remotely control Check Point appliances using a dedicated management channel. Lights Out Management can also work when the appliance is turned off or not responding.

**Initial Login**

To log in to the Lights Out Management WebUI:

1. Open a web browser and enter the default IP address of the LOM card: `192.168.0.100`. The login window appears.
2. Login with the default username (`admin`) and password (`admin`), all lower case.

   **Note** - Following 30 minutes of inactivity you are automatically be logged out.

**LOM Card Ports**

Make sure that all of these ports are open to use all the Lights Out Management features.

- 2068
- 5120
- 7578
Basic Configuration Options

The options in the main menu on Lights Out Management home page let you configure these settings:

- Remotely control the appliance
- Remotely control the power of the appliance
- Manage Lights Out Management users
- Configure Lights Out Management keyboard and mouse settings
- Configure Lights Out Management network settings
- Set date and time
- Define a Lights Out Management login message

Remotely Controlling the Appliance

The Appliance Control menu option enables you to access the appliance via a web interface (Java application). Prior to using this option, ensure that you have Java Runtime installed on the host machine.

To run the remote console:
1. Click the Appliance Control menu option.
2. Select KVM Console and then Open Console. A new window opens that enables you to remotely control the Smart-1 appliance.

Remotely Controlling the Power of the Appliance

Using the LOM card, it is possible to remotely switch ON the Smart-1 appliance even if the power is off, switch OFF the appliance, or reset the appliance.

**Note** - The main power switch at the rear of the appliance must be turned ON. If the switch is in the OFF position, remote power management is not possible.

To turn ON/OFF or reset the appliance:
1. Click the Appliance Control menu option.
2. Select Power Control, the relevant option and click Apply Changes.

Managing LOM Card Users

You can create, modify, and delete users. You can also assign privileges to users.
To create a user:
1. Click the **LOM User Management** menu option. The User Management page appears.
2. Select a row and click **Create**. The User Add dialog box appears.
3. Enter the following:
   - **User name**: a user name (maximum fourteen characters)
   - **Password**: a password for the login name. The password must have a minimum of 5 and a maximum of 14 characters.
   - **Confirm Password**: confirm the password.
   - **Network Privileges**: assign the Administrator or Operator privileges according to the table below.

### Network Privileges

<table>
<thead>
<tr>
<th></th>
<th>Administrator</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enter KVM console</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create user</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Modify user</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Delete user</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Date/time settings</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit login message</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Remote power management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Network setting</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Keyboard/mouse setting</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To modify a user:
1. Select an existing user from the list and click **Modify**. The User Modify dialog box appears.
2. Modify the fields as required.
3. To change the password, select **Change Password**.
4. Click **Modify User** to apply the changes.

To delete a user:
1. Select an existing user from the list and click **Delete**. A message appears.
2. Click **OK**.
Configuring LOM Keyboard and Mouse

To use the remote console feature described above, specify the operating system that the host machine is running.

To configure keyboard and mouse settings:
1. Click the KVM Settings menu option.
2. Select the relevant option:
   - Absolute (for Windows)
   - Relative (for Linux)
3. Click Apply Changes.

Configuring LOM Network

The network settings option enables you to change the default IP address and other basic network settings of Lights Out Management.

To configure the network settings:
1. Click the LOM Settings menu option and select Network.
2. Select Static and enter the following values.
   - IP address: the IP address of the LOM.
   - Subnet mask: the subnet mask of the LOM's local network.
   - Gateway IP address: the Default Gateway IP address.
   - Remote Console and HTTPS port: port number on which the Remote Console server and HTTPS server are listening.

Setting the Date and Time

This option enables you to manually change the date and time of the LOM card.

Defining a LOM Login Message

This option enables you to define the login message that appears when accessing LOM via a browser.

To edit a login message:
1. Click the Device Settings menu option and select Login Message.
2. Enter the login message text.
3. Click Apply Changes.
Chapter 8

Registration and Support

In This Chapter

Registration 73
Support 73
Where to From Here? 73

Registration

Smart-1 requires a specific license to operate. Obtain a license and register it

Connect to the WebUI of the appliance to find the MAC address that is required to obtain a license.

- Gaia - From Advanced mode, select Maintenance > Licenses.
- SecurePlatform - Select Information > Appliance Status.

Support

For additional technical information about Check Point products, consult the Check Point Support Center (http://supportcenter.checkpoint.com).

Where to From Here?

You have now learned the basics that you need to get started. The next step is to obtain more advanced knowledge of your Check Point software.

See the relevant documentation for your software version on the Check Point Support Center: Check Point documentation is available on the Check Point Support Center (http://supportcenter.checkpoint.com).

Be sure to also use the Online Help when you are working with the Check Point SmartConsole clients.