

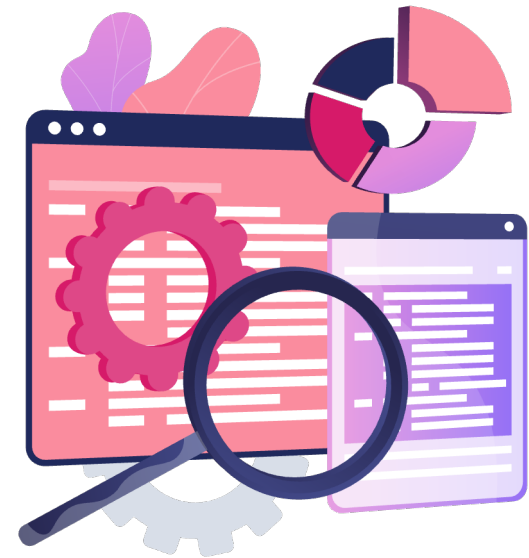
## CHAPTER 2

# CHECK POINT GATEWAY AND SERVER DEPLOYMENT

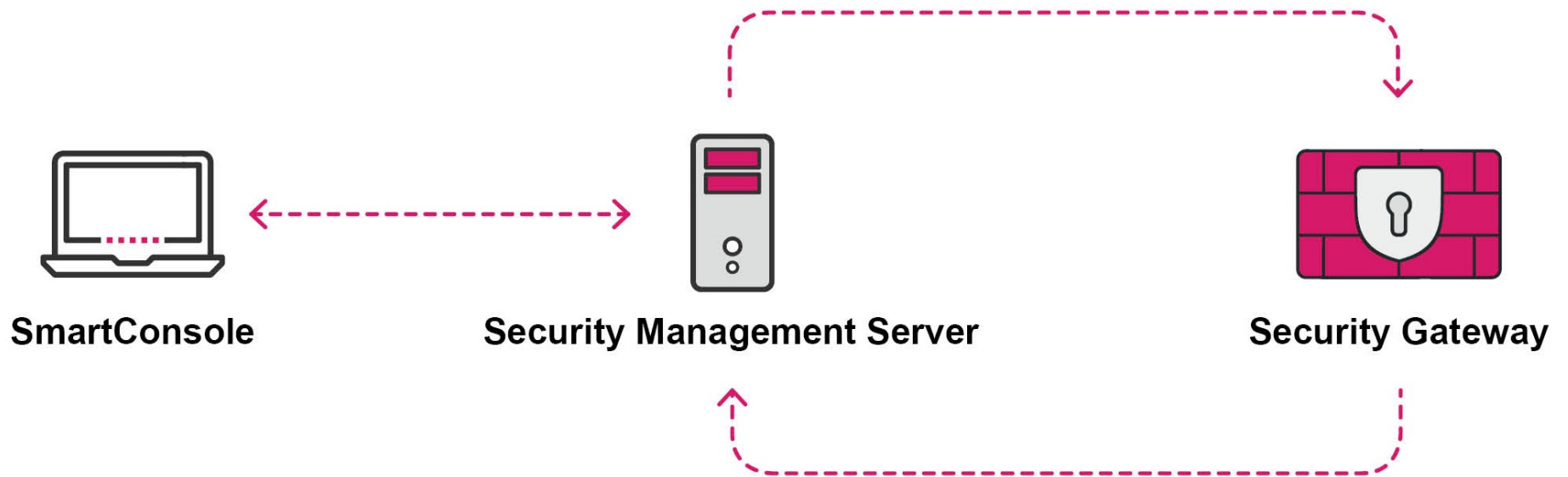
**YOU DESERVE THE BEST SECURITY**

## Learning Objectives

- Describe the basic functions of the Gaia operating system.
- Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain solution.



# Deployment Overview



Three-Tiered Architecture

# Gaia Operating System Overview



## Gaia Operating System Interfaces

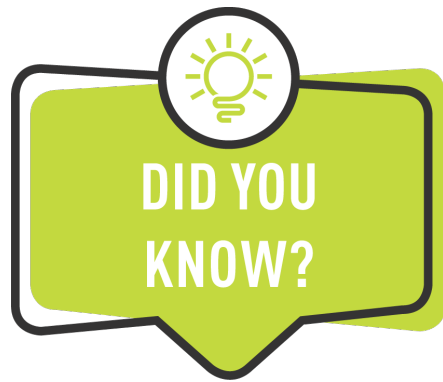
- Requires operating-level settings:
  - IP addresses
  - Network interfaces
  - Routing parameters
  - System updates and backup settings
  - User authentication, permissions, roles

### CLI (Command Line Interface)

- Gaia Clish
- Bash

### GUI (Graphical User Interface)

- Gaia Portal browser-based shell



In computing, a shell is a software program that lets users interact with a computer by giving it instructions.

# Security Operations Framework

Software

Security Management Server - Management processes  
Security Gateway - Firewall and VPN processes

Kernel

Security Management Server – Gaia only (no enforcement modules)  
Security Gateway - Gaia + Firewall & VPN Kernels

Hardware

Security Management Server - Smart-1 appliances or open server  
Security Gateway - Quantum Security Gateway

# Gaia Command Line Interface

- Easy-to-use CLI for command execution.
- Enhanced Help system with auto-completion.
- Two types:
  - Gaia Clish (default)
  - Bash (Expert mode)

```
<form ref={el => this.serchForm = el}>
  <div className="row">
    <div className="form-group col-3">
      <select name="bedrooms" className="form-control" onChange={this.fetchProperties}>
        <option value="0">Bedrooms</option>
        {[ ...Array(+this.state.startParams.max_bedrooms).keys() ].map( (value) =>
          <option key={value} value={value+1}>{value+1}</option>
        )}
      </select>
    </div>
    <div className="form-group col-3">
      <select name="bathrooms" className="form-control" onChange={this.fetchProperties}>
        <option value="0">Bathrooms</option>
        {[ ...Array(+this.state.startParams.max_bathrooms).keys() ].map( (value) =>
          <option key={value} value={value+1}>{value+1}</option>
        )}
      </select>
    </div>
    <div className="form-group col-3">
      <select name="storeys" className="form-control" onChange={this.fetchProperties}>
        <option value="0">Storeys</option>
        {[ ...Array(+this.state.startParams.max_storeys).keys() ].map( (value) =>
          <option key={value} value={value+1}>{value+1}</option>
        )}
      </select>
    </div>
    <div className="form-group col-3">
      <select name="garages" className="form-control" onChange={this.fetchProperties}>
        <option value="0">Garages</option>
        {[ ...Array(+this.state.startParams.max_garages).keys() ].map( (value) =>
          <option key={value} value={value+1}>{value+1}</option>
        )}
      </select>
    </div>
    <div className="form-group col-3">
      <input type="name" placeholder="Name" name="name" className="form-control" onChange={this.fetchProperties} />
    </div>
  </div>
</form>
```



# Accessing the Gaia Clish

## 1. Connect using:

- SSH (secure shell)
- Gaia Portal (web browser)
- SmartConsole

## 2. Log in with the Clish username and password.

- Default is **admin** and **admin** (on appliances)
- Configured during Gaia install (on open servers)



# Accessing Export Mode



1. After logging into Clish, run the following command:  
`expert`
2. When prompted, type the password.
3. Type `exit` to exit Expert mode and return to Clish.

# Working with Gaia Commands

Syntax:

```
operation feature parameter
```

Command	Description
<code>show commands</code>	View all commands the user has permissions to run.
<code>show commands feature &lt;TAB&gt;</code>	View list of features.
<code>show commands op &lt;SPACE&gt; &lt;TAB&gt;</code>	Show all possible operations.
<code>show version all</code>	Show full system version information.



## Guidelines for Gaia Commands

- Log out of the CLI after completing your session.
- Limit access to the Export mode to only those who are trained and experienced with CLI usage and operation.
- The syntax for many commands is case-sensitive.

## Guidelines (Continued)

```
A-GW-01
```

### Gaia Clish

```
Unauthorized access of this server is prohibited and punishable by law.  
login: admin  
Password:  
Last login: Mon Oct  2 15:13:52 on tty1
```

```
A-GW-01
```

```
Unauthorized access of this server is prohibited and punishable by law.  
login: admin  
Password:  
Last login: Mon Oct  2 15:13:52 on tty1  
A-GW-01> expert  
Enter expert password:
```

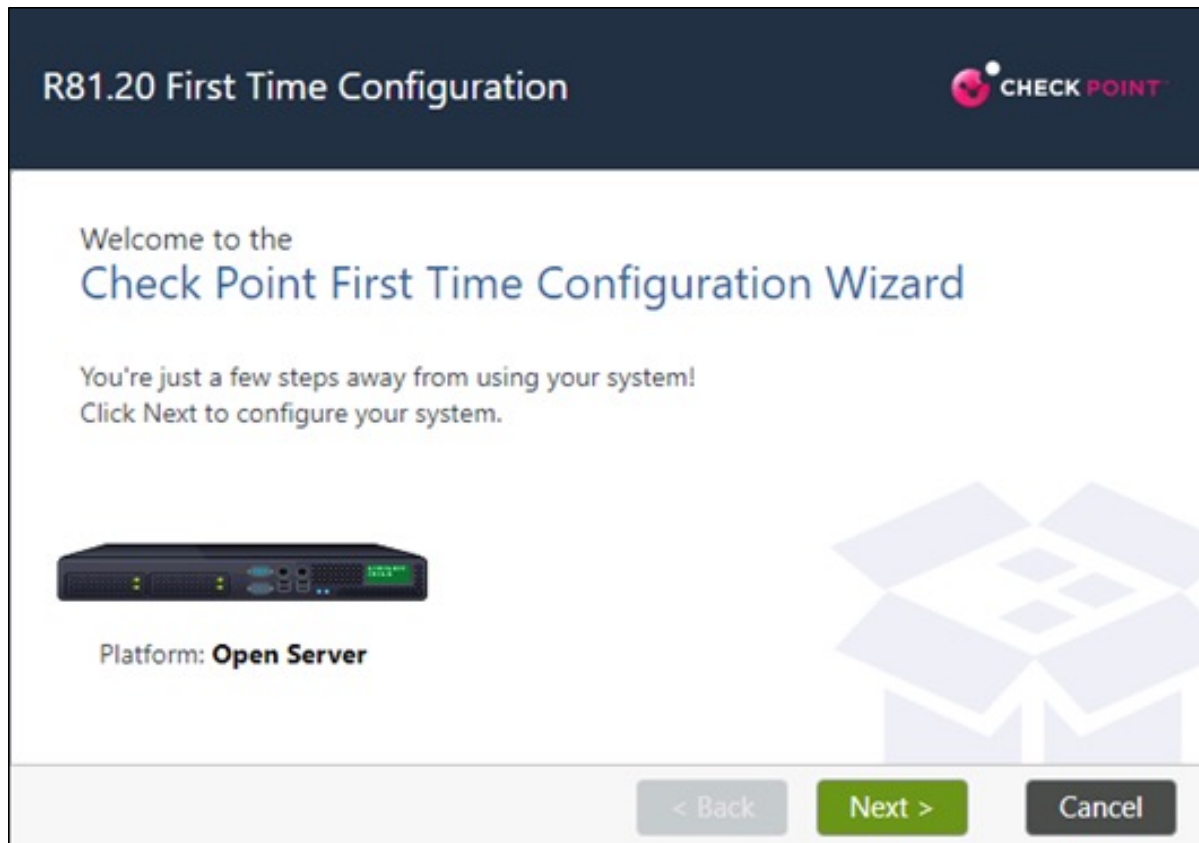
```
Warning! All configurations should be done through clish  
You are in expert mode now.
```

```
[Expert@A-GW-01:0]# _
```

### Expert Mode

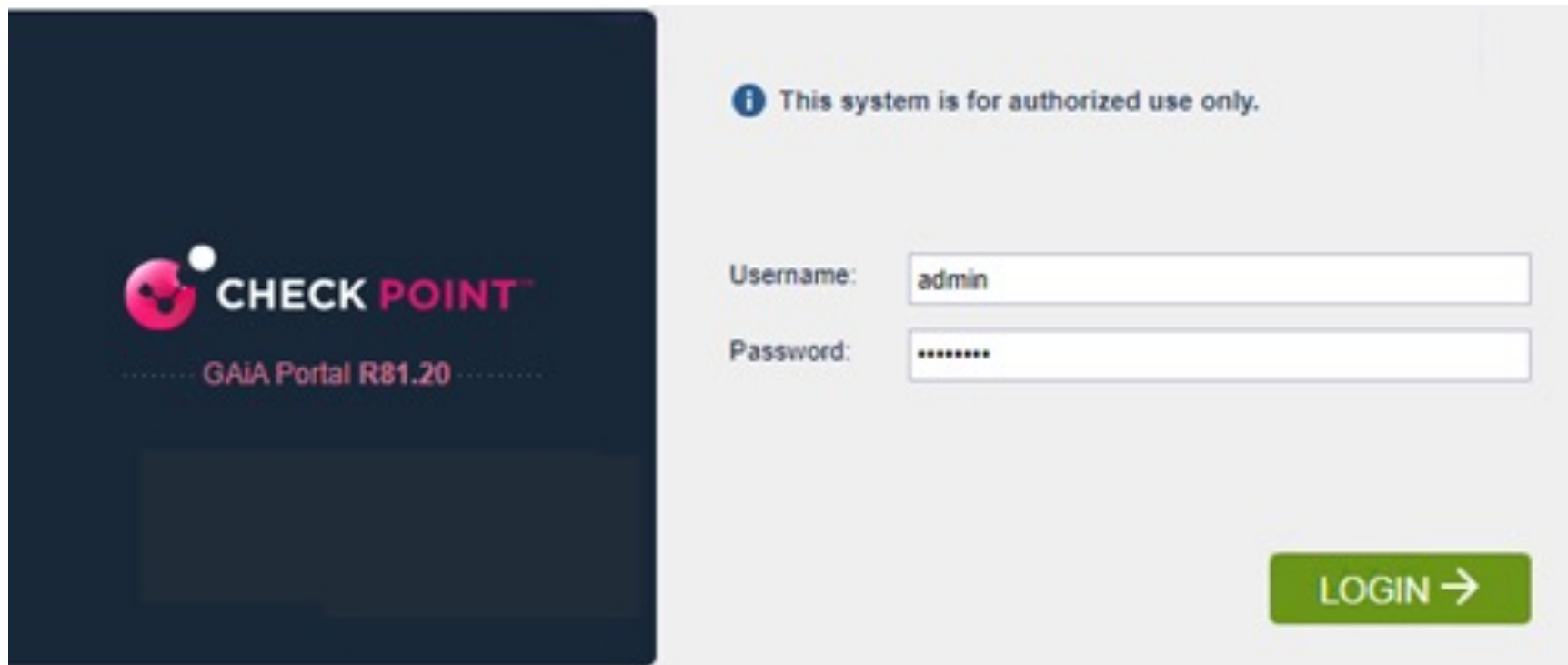
Be aware if you are you working in the Gaia Clish or Expert mode.

# First Time Configuration Wizard



Run using the  
CLI Expert mode  
or Gaia Portal.

# Running the First Time Configuration Wizard



The image shows a login interface for the Check Point GAIA Portal R81.20. On the left is a dark blue sidebar with the Check Point logo and the text "CHECK POINT" and "GAIA Portal R81.20". The main area is light gray and contains an information icon and the text "This system is for authorized use only." Below this are two input fields: "Username:" with the value "admin" and "Password:" with masked characters "\*\*\*\*\*". A green "LOGIN →" button is located at the bottom right.

**CHECK POINT**  
..... GAIA Portal R81.20 .....

**i** This system is for authorized use only.

Username:

Password:

**LOGIN →**



# Gaia Portal

- Web-based interface for appliances and open servers running Gaia.
- Features include:
  - Clientless access from supported browsers
  - First Time Configuration Wizard
  - Network Management
  - System Management
  - User Management
  - Maintenance
  - Web access to the CLI





## Clientless Access to Gaia Portal

- From a supported browser, navigate to:

`https://<IP Address of Gaia Management Interface>`



You can also access the Gaia Portal from SmartConsole.

# Gaia Portal Interface - Overview Page

1. View mode
2. Toolbar (top)
3. Navigation tree (left side)

The screenshot displays the Gaia Portal interface for an Open Server. The interface is divided into several sections:

- Navigation Tree (Left Side):** A tree view showing various system management options such as Network Management, System Management, and Advanced Routing. A red circle '3' highlights the tree.
- Toolbar (Top):** A top toolbar with a search bar and navigation icons. A red circle '2' highlights the toolbar.
- System Overview (Main Content):** A central panel displaying system information for a Check Point Security Gateway (R81.20). It includes details like Kernel (3.10.0-1160.15.2cpx86\_64), Edition (64-bit), Build Number (631), System Uptime (10 minutes), and Software Updates (no new recommended updates detected). A red circle '1' highlights the 'View mode' dropdown in the top left, and another red circle '2' highlights the top toolbar. A red circle '3' highlights the navigation tree.
- Blades (Right Side):** A vertical list of system blades with their respective status and statistics:
  - Firewall:** Packets accepted: 57669, Packets dropped: 2021, Peak number of connections: 537, Number of connections: 15.
  - IPSec VPN:** Total tunnels: 0, Remote Access: 0, tunnels: 0, Packets encrypted: 0, Packets decrypted: 0.
  - IPS:** (No statistics shown)
  - Application Control:** Update status: up-to-date
  - URL Filtering:** Update status: up-to-date
  - Anti-Virus:** (No statistics shown)
  - Anti-Bot:** (No statistics shown)
  - Threat Emulation:** (No statistics shown)
  - Threat Extraction:** (No statistics shown)
  - Anti-Spam and Mail:** (No statistics shown)
- Network Configuration (Bottom):** A table showing network interfaces and their status:

Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.1.1.1	-	Up
eth1	203.0.113.1	-	Up
eth2	192.168.11.1	-	Up
eth3	192.168.12.1	-	Up
lo	127.0.0.1	-	Up

The browser Back button is not supported. Do not use it.

# Basic and Advanced View Modes

**Basic Mode**

View mode: Basic

System Overview

Check Point Security Gateway | R81.20

Kernel: 3.10.0-1160.15.2cpx86\_64  
Edition: 64-bit  
Build Number: 631  
System Uptime: 30 minutes  
Software Updates: no new recommended updates detected

Platform: Open Server

Network Configuration

Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.1.1.1	-	Up
eth1	203.0.113.1	-	Up
eth2	192.168.11.1	-	Up
eth3	192.168.12.1	-	Up
lo	127.0.0.1	-	Up

Throughput

Blades

- Firewall
- IPSec VPN
- IPS
- Application Control
- URL Filtering
- Anti-Virus
- Anti-Bot
- Threat Emulation
- Threat Extraction
- Anti-Spam and Mail
- Data Loss Prevention
- Mobile Access

**Advance Mode**

View mode: Advanced

System Overview

Check Point Security Gateway | R81.20

Kernel: 3.10.0-1160.15.2cpx86\_64  
Edition: 64-bit  
Build Number: 631  
System Uptime: 31 minutes  
Software Updates: no new recommended updates detected

Platform: Open Server

Network Configuration

Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.1.1.1	-	Up
eth1	203.0.113.1	-	Up
eth2	192.168.11.1	-	Up
eth3	192.168.12.1	-	Up
lo	127.0.0.1	-	Up

Throughput

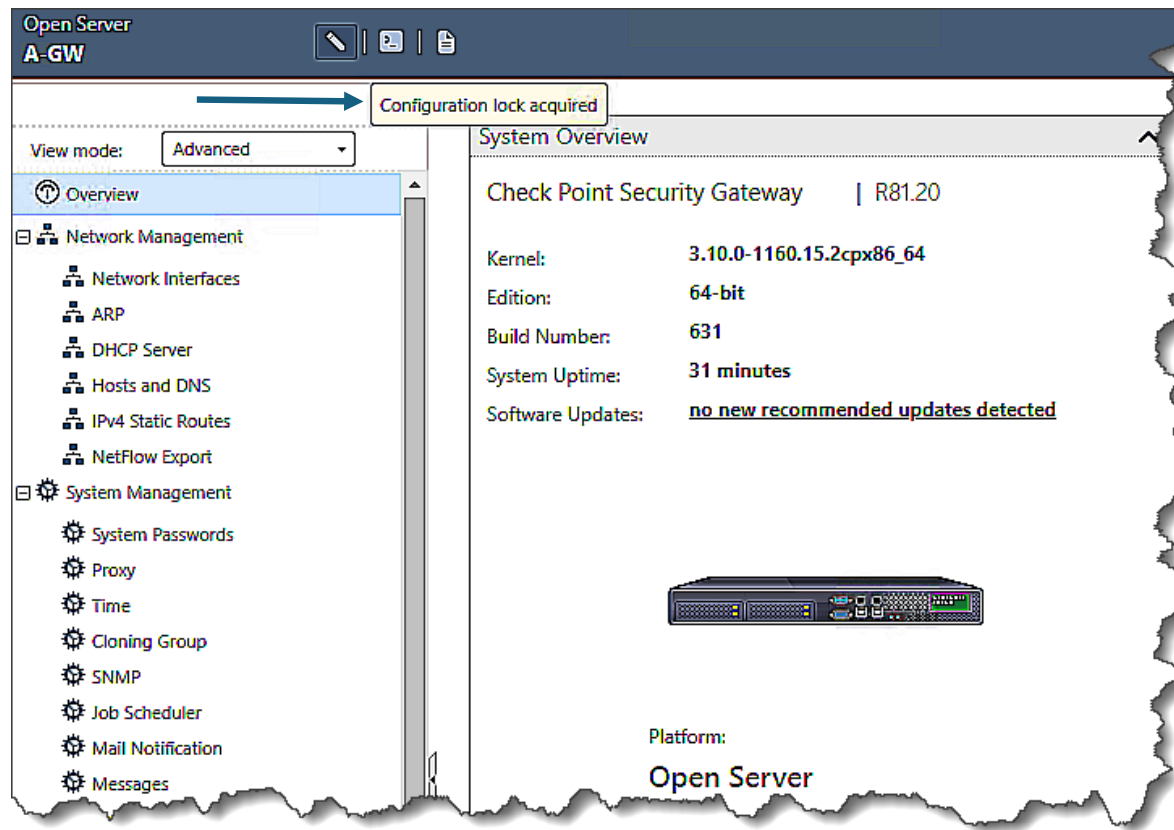
Blades

- Firewall
- IPSec VPN
- IPS
- Application Control
- URL Filtering
- Anti-Virus
- Anti-Bot
- Threat Emulation
- Threat Extraction
- Anti-Spam and Mail
- Data Loss Prevention
- Mobile Access

Advanced Routing

- DHCP Relay
- BGP
- IGMP
- IP Broadcast Helper
- PIM
- Static Multicast Routes
- MFC Static Entries
- RIP
- IP Reachability D

# Toolbar - Configuration Lock



If you log in and no other user has Read/Write access, you get an exclusive configuration lock with Read/Write access.

## Overriding the Configuration Lock

- If a user already has the configuration lock, you can override the user's lock.
- If you override the lock, the other user stays logged in with Read-Only access.
- If you do not override the lock, you cannot modify the settings.
- Read/Write access privileges are required to override a configuration lock.



Be careful about overriding the lock.  
Settings cannot be modified.

# Terminal



The image shows a screenshot of the Open Server A-GW management interface. The interface is divided into a left sidebar with navigation options, a main content area, and a terminal window on the right.

**Open Server A-GW**

View mode: **Advanced**

**Open terminal**

**System Overview**

Check **System Overview** | R81.20

Kernel: **64-bit**

Edition: **631**

Build Number: **31 minutes**

System Uptime: **31 minutes**

Software Updates: **no new recommended updates detected**

Platform: **Open Server**

**Terminal**

A-GW login: |

The terminal window is currently empty, showing the login prompt. A large grey arrow points from the 'no new recommended updates detected' text in the System Overview section to the terminal window.

Use the Terminal to run CLI commands.

# Scratchpad

The image shows a screenshot of the Open Server A-GW management interface. The interface is divided into three main sections: a left-hand navigation pane, a central content area, and a right-hand Scratchpad window.

**Open Server A-GW Interface:**

- View mode:** Advanced
- Overview:** Selected
- Network Management:**
  - Network Interfaces
  - ARP
  - DHCP Server
  - Hosts and DNS
  - IPv4 Static Routes
  - NetFlow Export
- System Management:**
  - System Passwords
  - Proxy
  - Time
  - Cloning Group
  - SNMP
  - Job Scheduler
  - Mail Notification
  - Messages

**System Overview Content:**

- Check Point Software: R81.20
- Kernel: 3.10.0
- Edition: 64-bit
- Build Number: 631
- System Uptime: 31 minutes
- Software Updates: **no new recommended updates detected**

**Scratchpad Window:**

- Blank white space for notes or copy/paste operations.
- Buttons: OK, Cancel

**Platform:** Open Server

A large grey arrow points from the 'Software Updates' section of the System Overview to the Scratchpad window, indicating the intended use of the Scratchpad for notes or copy/paste operations.

Use for notes or quick copy/paste operations.

# Navigation Tree



- Used to navigate to other pages, including:
  - Network Management
  - System Management
  - User Management
  - Maintenance



# Network Management

The screenshot displays a network management interface for a server named "A-GW". The interface is divided into a left sidebar and a main content area. The sidebar shows a "View mode" set to "Advanced" and a navigation menu with "Overview" selected. Under "Network Management", several options are listed: Network Interfaces, ARP, DHCP Server, Hosts and DNS, IPv4 Static Routes, and NetFlow Export. The main content area displays the "System Overview" for a "Check Point Security Gateway | R81.20". The system details are as follows:

Kernel:	3.10.0-1160.15.2cpx86_64
Edition:	64-bit
Build Number:	631
System Uptime:	31 minutes
Software Updates:	<u>no new recommended updates detected</u>

# System Management

Open Server  
A-GW


View mode: **Advanced**

- Overview
- Network Management
- System Management
  - System Passwords
  - Proxy
  - Time
  - Cloning Group
  - SNMP
  - Job Scheduler
  - Mail Notification
  - Messages
  - Display Format
  - Session
  - Crash Data
  - System Configuration
  - System Logging
  - Network Access
  - Host Access
  - LLDP

**System Overview**

Check Point Security Gateway | R81.20

Kernel: **3.10.0-1160.15.2cpx86\_64**  
Edition: **64-bit**  
Build Number: **631**  
System Uptime: **31 minutes**  
Software Updates: **no new recommended updates detected**



Platform:  
**Open Server**

# User Management

The screenshot displays the Open Server A-GW user management interface. The top bar shows the server name 'Open Server A-GW' and navigation icons. The left sidebar contains a navigation menu with the following items: Overview (selected), Network Management, System Management, Advanced Routing, User Management (expanded to show Change My Password, Users, Roles, Password, Authentication Servers, and System Groups), Roles, Password, Authentication Servers, and System Groups. The main content area is titled 'System Overview' and displays the following information:

Check Point Security Gateway | R81.20

Kernel:	3.10.0-1160.15.2cpx86_64
Edition:	64-bit
Build Number:	631
System Uptime:	31 minutes
Software Updates:	<u>no new recommended updates detected</u>

A tooltip is visible over the 'Roles' menu item, stating: 'Roles are sets of permissions assigned to users'. At the bottom of the interface, there is a small image of a server rack.

# Maintenance

Open Server  
A-GW

View mode: **Advanced**

- Overview
- Network Management
- System Management
- Advanced Routing
- User Management
- High Availability
- Maintenance
  - License Status
  - Snapshot Management
  - System Backup
  - Download SmartConsole
  - Shut Down

### System Overview

Check Point Security Gateway | R81.20


Kernel: **3.10.0-1160.15.2cpx86\_64**

Edition: **64-bit**

Build Number: **631**

System Uptime: **31 minutes**

Software Updates: **no new recommended updates detected**



# Check Point Upgrade Service Engine (CPUSE)

- Mechanism for software deployment on the Gaia operating system.
- Supports deployment of:
  - Single HotFixes (HF)
  - HotFixAccumulators (Jumbo)
  - Major Versions

Also known as Deployment Agent (DA).

## CPUSE - Features

- Key Features:

**Smart**

**Fast**

**Safe**

sk92449 - Check Point Upgrade Service Engine (CPUSE) -  
Gaia Deployment Agent

# Hotfixes

Private package – hotfix that is available only to limited audiences.

- Download types:
  - Manual
  - Automatic
  - Scheduled (daily, weekly, monthly, only once)

## Guidelines

- By default, downloaded and installed automatically.
- Full installation and upgrade packages require manual installation.
- Installation requirements:
  - Define mail notifications for completed package actions and new package updates.
  - Then run the software download and installation.



A CPUSE policy must be defined before a user can download and run updates.

CPUSE and Hotfixes are discussed in greater detail in Chapter 11.



## Review Questions

1. List the two main shells that the Gaia operating system provides.
2. Which shell is most restrictive?
3. What is the default shell?
4. What is the default password for Expert mode?

## Lab 2A

# Installing the Primary Security Management Server



## Lab 2B

### Installing a Security Gateway





## Lab 2C

### Configuring Objects in SmartConsole

