UTM-1

Getting Started Guide


2 July 2012

Classification: [Protected] | P/N: 704886
Important Information

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=10947

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>
</table>
| 02 July 2012    | Added First Time Wizard for Gaia  
                  Added Gaia to Restoring Using the WebUI (on page 37) |
| 31 October 2011 | Removed CD from Shipping Carton Contents (on page 11). |
| 25 September 2011| When restoring using the console boot menu, from the Flow control list, select **NONE**, and not **Hardware**, as previously documented. |
| 26 August 2010  | First release of this document. |

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 UTM-1 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.

Japan Class A Compliance Statement:

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>9</td>
</tr>
<tr>
<td>Welcome</td>
<td>9</td>
</tr>
<tr>
<td>UTM-1 Overview</td>
<td>9</td>
</tr>
<tr>
<td>This document provides:</td>
<td>10</td>
</tr>
<tr>
<td>Shipping Carton Contents</td>
<td>11</td>
</tr>
<tr>
<td>Terminology</td>
<td>11</td>
</tr>
<tr>
<td><strong>Configuring UTM-1</strong></td>
<td>13</td>
</tr>
<tr>
<td>Installing UTM-1 in the Rack</td>
<td>13</td>
</tr>
<tr>
<td>Connecting Power Cables and Powering On</td>
<td>14</td>
</tr>
<tr>
<td>Available Software Images</td>
<td>14</td>
</tr>
<tr>
<td>Initial Configuration</td>
<td>14</td>
</tr>
<tr>
<td>Using the First Time Configuration Wizard on Gaia</td>
<td>16</td>
</tr>
<tr>
<td>Starting the Gaia First Time Configuration Wizard</td>
<td>16</td>
</tr>
<tr>
<td>Welcome</td>
<td>16</td>
</tr>
<tr>
<td>Available Releases</td>
<td>16</td>
</tr>
<tr>
<td>Authentication Details</td>
<td>17</td>
</tr>
<tr>
<td>Date and Time Setup</td>
<td>17</td>
</tr>
<tr>
<td>Device Name</td>
<td>17</td>
</tr>
<tr>
<td>Network Connection</td>
<td>17</td>
</tr>
<tr>
<td>Products</td>
<td>18</td>
</tr>
<tr>
<td>Security Management Administrator</td>
<td>19</td>
</tr>
<tr>
<td>Security Management GUI Clients</td>
<td>19</td>
</tr>
<tr>
<td>Dynamically Assigned IP</td>
<td>20</td>
</tr>
<tr>
<td>Secure Internal Communication (SIC)</td>
<td>20</td>
</tr>
<tr>
<td>Summary</td>
<td>20</td>
</tr>
<tr>
<td>Using the First Time Configuration Wizard on SecurePlatform</td>
<td>21</td>
</tr>
<tr>
<td>Starting the First Time Configuration Wizard</td>
<td>21</td>
</tr>
<tr>
<td>Welcome</td>
<td>21</td>
</tr>
<tr>
<td>Appliance Date and Time Setup</td>
<td>22</td>
</tr>
<tr>
<td>Network Connections</td>
<td>22</td>
</tr>
<tr>
<td>Routing Table</td>
<td>22</td>
</tr>
<tr>
<td>Host, Domain Settings, and DNS Servers</td>
<td>22</td>
</tr>
<tr>
<td>Management Type</td>
<td>23</td>
</tr>
<tr>
<td>Summary</td>
<td>24</td>
</tr>
<tr>
<td>Installing the SmartConsole GUI Clients</td>
<td>24</td>
</tr>
</tbody>
</table>
First Time Login to the Security Management Server ........................................... 25
  Login Process ................................................................................................. 25
  Authenticating and Fingerprint Comparison .................................................... 25
Configure and Install the Security Policy ............................................................ 25
  Create a New Policy Package ........................................................................... 26
  Define a Host .................................................................................................... 26
  Define a Network .............................................................................................. 27
  Create the Firewall Rules ................................................................................ 27
  Configuring Content Inspection ....................................................................... 27
  Install a Policy Package .................................................................................. 28
Advanced Configuration ...................................................................................... 28
  Connecting to the UTM-1 CLI ................................................................. 29
UTM-1 Hardware ............................................................................................... 31
  UTM-1 130 Ports ............................................................................................. 31
  LEDs on the UTM-1 130 ................................................................................ 32
  LEDs on all other UTM-1 Models ................................................................. 33
  Managing UTM-1 Using the LCD Panel ....................................................... 33
Restoring Factory Defaults ............................................................................... 37
  Restoring Using the WebUI ........................................................................... 37
    Gaia ............................................................................................................ 37
    SecurePlatform ............................................................................................ 38
  Restoring Using the Console Boot Menu ....................................................... 38
  Restoring Using the LCD Panel ..................................................................... 39
Registration and Support ................................................................................. 41
  Registration ..................................................................................................... 41
  Support .......................................................................................................... 41
Where to From Here? ......................................................................................... 41
Welcome

Thank you for choosing Check Point’s UTM-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.

UTM-1 Overview

Check Point UTM-1 delivers integrated unified threat management to protect your organization from today’s emerging threats. Based on proven Check Point security technologies such as Stateful Inspection, Application Intelligence, and SMART (Security Management Architecture), UTM-1 provides simplified deployment and management while delivering uncompromising levels of security.
Introduction

UTM-1 supports the Check Point Software Blade architecture, providing independent, modular and centrally managed security building blocks. Software Blades can be quickly enabled and configured into a solution based on specific security needs.

The following Software Blades are included in UTM-1:

Security Gateway Software Blades

- Firewall – proven, enterprise-class firewall.
- IPSec VPN – encrypted secure connectivity to corporate networks, remote users, branch offices and business partners.
- IPS – High performance integrated IPS solution with extensive threat coverage.
- URL Filtering – Best-of-breid Web filtering covering more than 20 million URLs. Protects users and enterprises by restricting access to dangerous Web sites.
- Anti-Virus & Anti-Malware – Leading anti-virus protection including heuristic virus analysis. Stops viruses, worms and other malware at the gateway.
- Anti-Spam & Email Security – Multi-dimensional protection for the messaging infrastructure. Stops spam, protects servers and eliminates attacks through email.

Security Management Software Blades

- Network Policy Management – Comprehensive network security policy management for Check Point gateways and blades, via SmartDashboard, a single, unified console.
- Endpoint Policy Management – Centrally deploy, manage, monitor and enforce security policy for all endpoint devices across any sized organization.
- Logging & Status – Comprehensive information in the form of logs, and a complete visual picture of changes to gateways, tunnels, remote users and security activities.

For additional software blades, see the Check Point Web site (http://www.checkpoint.com/products/softwareblades/architecture/)

This document provides:

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

Note - This guide applies to all UTM-1 models. However, screen shots may apply only to the highest model in the range.
Shipping Carton Contents

This section describes the contents of the shipping carton.

**Contents of the Shipping Carton**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td>A single UTM-1 appliance</td>
</tr>
<tr>
<td>Rack Mounting Accessories (Not applicable to UTM-1 130)</td>
<td>Hardware mounting kit</td>
</tr>
<tr>
<td>Cables</td>
<td>• 1 Power cable</td>
</tr>
<tr>
<td></td>
<td>• 1 Standard network cable</td>
</tr>
<tr>
<td></td>
<td>• 1 Serial console cable</td>
</tr>
<tr>
<td>Documentation</td>
<td>• Quick Start Guide</td>
</tr>
<tr>
<td></td>
<td>• Getting Started 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 UTM-1 terms are used in this guide:

- **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.

- **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.

- **Locally managed deployment**: When all Check Point components responsible for both the management and enforcement of the security policy (the Security Management server and the gateway) are installed on the same machine.
Introduction

- **Centrally managed deployment**: When the gateway and the Security Management server are installed on separate machines.

- **UTM-1 cluster**: Refers to two UTM-1 devices with synchronized Security Management servers and gateways.
Chapter 2

Configuring UTM-1

In This Chapter

- Installing UTM-1 in the Rack
- Connecting Power Cables and Powering On
- Available Software Images
- Initial Configuration
- Using the First Time Configuration Wizard on Gaia
- Using the First Time Configuration Wizard on SecurePlatform
- Installing the SmartConsole GUI Clients
- First Time Login to the Security Management Server
- Configure and Install the Security Policy
- Advanced Configuration

To configure UTM-1, perform the following steps:

Step 1: Install UTM-1 onto the rack.
Step 2: Connect the cables and power on.
Step 3: Use the First Time Configuration Wizard.
Step 4: Install the SmartConsole GUI clients.
Step 5: Login to SmartDashboard and compare the fingerprint.
Step 6: Configure and install the security policy.

Installing UTM-1 in the Rack

Note - Does not apply to UTM-1 130.

Install the system in the rack with the network ports facing the front of the rack.
Connecting Power Cables and Powering On

For UTM-1 130
1. Connect the power cable to power supply unit.
2. Connect the power supply unit to the power port at the rear of the appliance.
3. Connect the power cable to an A/C outlet.
   UTM-1 turns on immediately.

For all other UTM-1 models
1. Connect the power cable.
2. On the back panel, turn on the Power button to start the appliance.

Available Software Images
UTM-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 UTM-1 Image Management Guide for the applicable version (http://support.checkpoint.com).

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

Initial Configuration
Do the initial configuration of the appliance with the First Time Configuration Wizard.
There are different First Time Configuration Wizard options for the Gaia and the SecurePlatform operating system.
Go to the applicable section:

- Using the First Time Configuration Wizard on Gaia (on page 16)
- Using the First Time Configuration Wizard on SecurePlatform (on page 21)
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 INT. 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 INT 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.

![](image)

**Products**

Select the Gaia products that are installed on the appliance.

**Advanced**

Use these options to configure an appliance that is a cluster member or in a High Availability deployment.

- **Unit is part of a cluster** - the options are:
  - **ClusterXL** - For more about ClusterXL configurations, see the applicable version of the *ClusterXL Administration Guide*.
  - **VRRP** - For more about VRRP clusters, see the applicable version of the *Gaia Administration Guide*.

- **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).

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.
**Dynamically Assigned IP**

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

A **Dynamically Assigned IP (DAIP)** gateway is a gateway where the external interface IP address is assigned dynamically by the ISP.

Select this option if this Security Gateway uses dynamically assigned IP addresses.

**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**

To start 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 INT. 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 to the system using the default 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 gives you access to the appliance. For security purposes, you must change it to a more secure password.
   In the Password recovery login token section, download a Login Token to use if you forget the password. We recommend that you save the password recovery login token file in a safe storage.
6. The **First Time Configuration Wizard** runs.
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.

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.

Host, Domain Settings, and DNS Servers

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

The host name must start with a letter and cannot be named com1, com2...,com9.

In the DNS section, set the DNS servers for the appliance.
Management Type

Set how the appliance is managed in the Management Type page.

- **Locally Managed Deployment:** The appliance is a Security Gateway and a Security Management server. The Security Management server manages the Security Policy that is enforced by the Security Gateway.

- **Centrally Managed Deployment:** The appliance is a Security Gateway, without a Security Management server. The Security Gateway is managed by a remote Security Management server.

Locally Managed Deployment

This section describes how to configure the appliance for locally managed deployment.

**Check Point Cluster**

Configure the cluster type. If you select *This appliance is part of a UTM-1 Cluster*, the options are:

- Primary cluster member
- Secondary cluster member

For information about clusters, see the *ClusterXL Administration Guide* (http://supportcenter.checkpoint.com) for your Check Point version.

**Web/SSH and GUI Clients Configuration**

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.

You can define a Host according to Hostname or IP address. Enter a comma-separated list of IP addresses from which you manage the appliance. Enter Any to manage the appliance from anywhere.

*Note* - Do not use the Any value for security reasons.

After you complete the First Time Configuration Wizard, more options are available using the WebUI menu.

**Download SmartConsole Applications**

Configuring a security policy for a Locally Managed UTM-1 (configured in the Management Type page) requires you to install the SmartConsole applications. In the Download SmartConsole Applications window, you can download SmartConsole and install it on Windows machines.

The release notes of your Check Point version in the Check Point Support Center (http://supportcenter.checkpoint.com), lists compatible Windows operating systems for SmartConsole.
Centrally Managed Deployment

This section describes how to configure the appliance for centrally managed deployment.

Gateway Type

Configure the gateway type for a Centrally Managed UTM-1.

Web/SSH and GUI Clients Configuration

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.

You can define a Host according to Hostname or IP address. Enter a comma-separated list of IP addresses from which you manage the appliance. Enter Any to manage the appliance from anywhere.

Note - Do not use the Any value for security reasons.

After you complete the First Time Configuration Wizard, more options are available using the WebUI menu.

SIC Setup

Configure the SIC (Secure Internal Communication) settings for a Centrally Managed appliance. Enter a SIC Activation Key. The same key is used by the gateway object in SmartDashboard.

Summary

The Summary page opens.

Click Finish to complete the First Time Configuration Wizard. You can log in to the appliance after some minutes.

Note - You should back up the system configuration. Open the WebUI interface and go to Appliance > Backup and Restore.

Installing the SmartConsole GUI Clients

If SmartDashboard was downloaded during the First Time Configuration Wizard, skip to First Time Login to the Security Management Server (on page 25).
The WebUI menu can be accessed by navigating to https://<appliance_ip_address>:4434 using Internet Explorer.

1. Log in to the WebUI with the administrator username and password.
2. Download the SmartConsole Installation package Product Configuration > Download SmartConsole > Download.

First Time Login to the Security Management Server

Login Process

In a Locally Managed deployment, the Security Management server is included in UTM-1.

In a Centrally Managed deployment, a Security Management server to manage the UTM-1 gateway has already been installed.

Administrators connect to the Security Management server through SmartDashboard using a process that is common to all SmartConsole clients. In this process, the administrator and the Security Management server are authenticated, and a secure channel of communication is negotiated.

Authenticating and Fingerprint Comparison

1. Launch SmartDashboard.
2. Enter the administrator username, password, and IP address of the Security Management server.
   Locally Managed deployment only: If a UTM-1 Cluster was configured, connect to the Security Management server on the primary cluster member.
3. Locally Managed deployment only: Manually authenticate the Security Management server with the Fingerprint presented. This step only takes place during first-time login, since when the Security Management server is authenticated, the Fingerprint is saved on the SmartConsole machine.

   Compare the Fingerprint with the fingerprint which is located in the WebUI in Product Configuration > Certificate Authority.
4. Locally Managed deployment only: If a UTM-1 Cluster option was selected in the UTM-1 Cluster page, the first-time UTM-1 Cluster wizard opens. Follow the wizard to complete the cluster configuration before installing a security policy.

Configure and Install the Security Policy

The security policy is implemented by defining an ordered set of rules in the Firewall Rule Base. A well-defined security policy is essential in order for UTM-1 to be an effective security solution.
The following is a very simple Firewall rule base:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Object</td>
<td>Any</td>
<td>http</td>
<td>Accept</td>
<td>Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>https</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Object</td>
<td>Any</td>
<td>dns</td>
<td>Accept</td>
<td>Log</td>
</tr>
<tr>
<td>Host Object</td>
<td>Any</td>
<td>ftp</td>
<td>Accept</td>
<td>Log</td>
</tr>
<tr>
<td>Host Object</td>
<td>Any</td>
<td>telnet</td>
<td>Accept</td>
<td>Log</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Log</td>
</tr>
</tbody>
</table>

The last rule in the rule base, known as the Cleanup Rule, is to drop all traffic that is not permitted by the previous rules. There is an implied rule that does this, but the Cleanup Rule allows you to log any access attempts.

Create a security policy as follows:

**Create a New Policy Package**

1. In SmartDashboard, click **File > New**. The **Save** window appears.
2. Click **Save and continue**. The **New Policy Package** window appears.
3. Enter a name for the new policy, select a policy type and click **OK**.

**Define a Host**

Define the hosts to be used in the Firewall Rule Base.

To define a host:

1. Click **Manage > Network Objects > New > Node > Host**. The **Host Node** window appears.
2. Enter a **Name** and **IP Address** (for example, 10.10.10.51).
3. In the **NAT** page, select **Add Automatic Address Translation rules**.
4. From the Translation Method drop down menu, select Hide, and the option Hide behind Gateway, and click OK.

**Define a Network**

Define the networks to be used in the Firewall Rule Base.

To define a network:
1. Click Manage > Network Objects > New > Network.
2. Enter the Name and Network Address (for example, 10.10.10.0) and Net Mask.
3. On the NAT tab, select Add Automatic Address Translation rules.
4. From the Translation Method drop down menu, select Hide, and the option Hide behind Gateway, and click OK.

**Create the Firewall Rules**

Define the Firewall rules. To define a rule:
1. From the menu, select Rules > Add Rule and choose one of Bottom, Top, Below, Above.
2. In the Source column, right click and select Add..., choose an object and click OK.
3. In the Service column, right click, select Add..., choose a service and click OK.
4. In the Action column, right click and select Accept. The last rule in the rule base should be drop.
5. In the Track column, right click, select Add... and choose Log.
6. To view all activity that is being logged, click Window > SmartView Tracker.

**Configuring Content Inspection**

When content inspection is configured on the UTM-1 gateway, traffic for the appropriate protocols is forwarded to the security server. The security server forwards the data stream to the inspection engine — an Anti-Virus server, for example. The data is allowed or blocked based on the response of the inspection engine.

Content inspection is performed only on traffic that has been allowed by the Security Policy.

To enable content inspection on the gateway, in the General Properties page of the gateway, select one or more of the following Network Security Blades:

- URL Filtering
- Anti-Virus & Anti-Malware
- Anti-Spam & Email Security.

For more information about content inspection, see the "Anti-Virus and URL filtering" chapter and the "Anti-Spam and Mail" chapter in the Firewall Administration Guide (http://supportcenter.checkpoint.com).
Install a Policy Package

To install a Policy Package:

1. Create a policy using the security rule base.
2. Click Policy > Install from the menu.
3. Choose the installation components:
   a) **Installation Targets** — the Security Gateways on which the policy is installed.
      By default, all gateways that are managed by the Security Management server are available for selection. Alternatively, define specific gateways per Policy Package through the **Select Installation Targets** window (accessed by clicking **Select Targets**).
   b) For each installation target, choose the policy components (**Advanced Security**, **QoS** or **Desktop Security**) to be installed.
   c) The installation Mode — what to do if the installation is not successful for all targets (so different targets enforce different policies):
      - Install on each gateway independently, or
      - Install on all gateway, or on none of the gateways.
4. Click OK.
   The Installation Process window is displayed, allowing you to monitor the progress of the verification, compilation and installation.
   If the verification is completed with no errors and the Security Management server is able to connect to the gateway securely, the Policy installation succeeds.
   If there are verification or installation errors, the installation fails (in which case you can view the errors to find the source of the problem).
   If there are verification warnings, the installation succeeds with the exception of the component specified in the warning.

Advanced Configuration

**Advanced configuration on Gaia**

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

**Advanced configuration on SecurePlatform**

Advanced configuration on SecurePlatform can be done using the `sysconfig` menu from the CLI.

**Note** - The `sysconfig` menu is only available after running the **First Time Configuration Wizard** in the WebUI.
**Connecting to the UTM-1 CLI**

You can connect to the command line interface of the UTM-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 UTM-1 appliances are: 9600bps, no parity, 1 stop bit (8N1), flow control None.

- An SSH connection to the management interface (if SSHD is configured).
Chapter 3

UTM-1 Hardware

In This Chapter

UTM-1 130 Ports 31
LEDs on the UTM-1 130 32
LEDs on all other UTM-1 Models 33
Managing UTM-1 Using the LCD Panel 33

This chapter contains information relating to the UTM-1 appliance LEDs, ports and LCD panel.

UTM-1 130 Ports

At the front of the appliance, UTM-1 130 has the following ports:

- **1 Gigabit Ethernet ports**
  The INT, SYNC/LAN1,LAN2 and DMZ ports support:
  - 1Gbit, 100Mbit and 10Mbit speeds.
  - Auto MDI-X, to automatically detect the required cable connection type (straight-through or crossover) and configure the connection appropriately.

- **100 Megabit Ethernet port**
  - The EXT port supports 100Mbit and 10Mbit speed, but does not support the Auto MDI-X standard.
  - When connecting this port, use the appropriate cable type: straight-through or crossover.
• **Console port** – for managing the appliance using RS-232 serial communication. Use the supplied serial cable.

The UTM-1 appliance has a single power port at the rear:

Connect the power supply unit to this port.

**LEDs on the UTM-1 130**

The front of the UTM-1 130 appliance has many LEDs, as shown.

The purpose and meaning of the various LEDs are as follows:

• **Power On/Off Indicator**: This green light is lit when the machine is ON. When the machine is OFF, the light is off.

• **HDD Operation Indicator**: An amber light that blinks when the hard drive is accessed.

• **Port Indicators**: There are two lights at the bottom of each LAN port. When the port is inactive, both are off.
  - **Activity Indicator**: This light is solid green when connected, and blinking green when encountering traffic.
  - **Speed Indicator**: When this light is yellow or orange, the port speed is 1000 Mbps. When it is green, the port speed is 100 Mbps.
LEDs on all other UTM-1 Models

**Note** - This section does not apply to UTM-1 130

The purpose and meaning of the various LEDs are as follows:

- **Power On/Off Indicator**: This green light is lit when the machine is ON. When the machine is OFF, the light is off.

- **HDD Operation Indicator**: When this green light is steady, the machine is ON and ready for login. When it is blinking, the machine is booting and it is not possible to login.

- **Reset Function**: This button forcibly reboots the appliance. The button is recessed into the appliance chassis to prevent accidental reboot. This button does not light up.

- **Port Indicators**: There are two lights at the bottom of each LAN port. When the port is inactive, both are off.
  - **Activity Indicator**: This light is solid green when connected, and blinking green when encountering traffic.
  - **Speed Indicator**: When this light is yellow or orange, the port speed is 1000 Mbps. When it is green, the port speed is 100 Mbps.

Managing UTM-1 Using the LCD Panel

**Note** - This section does not apply to UTM-1 130, which does not have an LCD panel

The appliance has an LCD panel that you can use to do basic management operations. You can enable DHCP. You can configure the management IP address, netmask, and default gateway of the appliance. You can reboot the appliance.
# 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>DHCP</td>
<td></td>
<td>Enable or disable IP address allocation using DHCP</td>
</tr>
<tr>
<td></td>
<td>Set Internal IP or Set Mgmt IP</td>
<td>Set the management interface IP address (cannot be edited when DHCP is enabled)</td>
</tr>
<tr>
<td></td>
<td>Set Netmask</td>
<td>Set the management interface network mask (cannot be edited when DHCP is enabled)</td>
</tr>
<tr>
<td></td>
<td>Set Default GW</td>
<td>Set the management interface default gateway (cannot be edited when DHCP is enabled)</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>

## LCD Panel Keys

<table>
<thead>
<tr>
<th>To</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the main menu</td>
<td>![Enter]</td>
</tr>
<tr>
<td>Navigate the menu</td>
<td>![Up] or ![Down]</td>
</tr>
<tr>
<td>Select a menu option</td>
<td>![Enter]</td>
</tr>
<tr>
<td>Go back to previous menu</td>
<td>![Esc]</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>Enter</td>
</tr>
<tr>
<td>Move back to the previous digit</td>
<td>Esc</td>
</tr>
<tr>
<td>Approve the change</td>
<td>Enter when the cursor is located on the last digit</td>
</tr>
<tr>
<td>Cancel the IP change</td>
<td>Esc when the cursor is located on the first digit</td>
</tr>
<tr>
<td>Change current digit</td>
<td>Up or Down</td>
</tr>
</tbody>
</table>
Chapter 4

Restoring Factory Defaults

In This Chapter

- Restoring Using the WebUI 37
- Restoring Using the Console Boot Menu 38
- Restoring Using the LCD Panel 39

As part of the troubleshooting process, it may be necessary to restore the UTM-1 appliance to its factory default settings.

A UTM-1 appliance can be restored to the factory default image:

- Using the WebUI
- Through the console boot menu
- Using the LCD panel (not applicable to UTM-1 130)

⚠️ Important - Restoring factory defaults deletes all information on the appliance.

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>:443`.
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>
<tbody>
<tr>
<td>PCI device listing ...</td>
<td></td>
</tr>
<tr>
<td>Bus No. Device No. Func No. Vendor/Device Class Device Class</td>
<td>IRQ</td>
</tr>
<tr>
<td>0 2 0 8086 2772 0300 Display Ctrlr</td>
<td>10</td>
</tr>
<tr>
<td>0 29 0 8086 27CB 0C03 USB 1.0/1.1 UHCI Ctrlr</td>
<td>015</td>
</tr>
<tr>
<td>0 29 1 8086 27CB 0C03 USB 1.0/1.1 UHCI Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>0 29 2 8086 27CA 0C03 USB 1.0/1.1 UHCI Ctrlr</td>
<td>5</td>
</tr>
<tr>
<td>0 29 3 8086 27CB 0C03 USB 1.0/1.1 UHCI Ctrlr</td>
<td>10</td>
</tr>
<tr>
<td>0 31 1 8086 27DF 0101 IDE Ctrlr</td>
<td>14</td>
</tr>
<tr>
<td>0 31 2 8086 27CB 0101 IDE Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>0 31 3 8086 27DA 0C05 SMBus Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>1 0 0 8086 109A 0200 Network Ctrlr</td>
<td>10</td>
</tr>
<tr>
<td>2 0 0 8086 109A 0200 Network Ctrlr</td>
<td>11</td>
</tr>
<tr>
<td>3 0 0 8086 109A 0200 Network Ctrlr</td>
<td>5</td>
</tr>
<tr>
<td>4 0 0 8086 109A 0200 Network Ctrlr</td>
<td>15</td>
</tr>
<tr>
<td>5 0 0 8086 109A 0200 Network Ctrlr</td>
<td>10</td>
</tr>
<tr>
<td>6 0 0 8086 109A 0200 Network Ctrlr</td>
<td>11</td>
</tr>
<tr>
<td>7 12 0 8086 1076 0200 Network Ctrlr</td>
<td>10</td>
</tr>
<tr>
<td>8 13 0 8086 1076 0200 Network Ctrlr</td>
<td>11</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**

*Note* - This section is not applicable to UTM-1 130 which does not have an LCD panel.

To restore the appliance its default factory configuration using the LCD panel at the front of the appliance:

1. Reboot or power on the appliance.

2. When the countdown begins, press any of the four buttons to the right of the LCD panel:

   ![Starting in 5 seconds](image)

   The boot menu appears.

3. Using the arrow buttons, select the relevant image version and press **ENTER**

4. Confirm the reset by pressing the Arrow Up button ▲
Pressing any other button causes the **Action Canceled** message to display:

![Action Canceled message](image)

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

5. If you confirmed the reset by pressing the Arrow Up button ▲ in step 4, wait for the appliance to restore the factory image. As the appliance is restored to the 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 is displayed:

![Initializing message](image)
Chapter 5

Registration and Support

In This Chapter

Registration 41
Support 41
Where to From Here? 41

Registration

UTM-1 requires a specific license to operate. Obtain a license and register at the Check Point Appliance Registration site https://usercenter.checkpoint.com/usercenter/reg/utm.

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.

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.