31 August 2021

LOM HTML5-BASED CARD FOR 6000, 7000, 16000, 26000, 28000, TE2000XN APPLIANCES

Administration Guide
Check Point Copyright Notice

© 2021 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:
Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c) (1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:
Refer to the Copyright page for a list of our trademarks.
Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

LOM HTML5-based Card for 6000, 7000, 16000, 26000, 28000, TE2000XN Appliances Administration Guide

Latest Version of this Document in English
Open the latest version of this document in a Web browser. Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 August 2021</td>
<td>First release of this document</td>
</tr>
<tr>
<td>31 August 2021</td>
<td>Updated for TE2000XN appliances</td>
</tr>
</tbody>
</table>
# Table of Contents

**Introduction** 6
- LOM Port on an Appliance 6
- WebUI Requirements 6

**First-Time Setup** 7

**LOM Card Configuration** 11
- Configuring an IP Address 11
- Configuring DNS Settings and Changing the Host Name 13
- Configuring Link Speed and Duplex Settings 14
- Configuring an SSL Certificate 15
- Configuring LOM Card Services 17
- Configuring Date and Time Settings 19

**Users and Access** 20
- Signing In to the LOM Card Interface 20
- Signing Out of the LOM Card Interface 20
- Making a New User Account 21
- Changing a User's Privilege Level and Disabling a User Account 23
- Changing a User's Password 24
- Deleting a User Account 25
- Login Block Settings (Failed Login Attempts) 26
- Connecting the LOM Card to a RADIUS Server 27
- Connecting the LOM Card to an LDAP Server 28
- Adding an LDAP Group 29
- Changing the Privilege Level of an LDAP Group 30
- Renaming an LDAP Group 31

**Power Management** 32
- Turning On the Appliance 33
- Turning Off the Appliance 35
- Restarting the Appliance 37

**Host Device Sensors** 38

**Remote Media Access** 39
- Limiting Access to Remote Media by IP Address 39
- Configuring Remote Media Settings 41
- Image Redirection 42
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>KVM (Console Session) Access</td>
<td>43</td>
</tr>
<tr>
<td>Maintenance</td>
<td>46</td>
</tr>
</tbody>
</table>
Introduction

This document applies to these appliances:

- 6000 (excludes 6500, 6800) and 7000
- 16000, 16600HS, 26000, 28000, and 28600HS
- TE2000XN

The Lights Out Management (LOM) application lets you remotely control Check Point appliances over a dedicated management channel. This management channel also works when the appliance is turned off or is not responding, if the appliance is connected to a power source.

LOM Port on an Appliance

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Link indicator:</td>
</tr>
<tr>
<td></td>
<td>- OFF - No Link</td>
</tr>
<tr>
<td></td>
<td>- On (Green) - Link is established</td>
</tr>
<tr>
<td></td>
<td>- Blink (Green) - Link is active</td>
</tr>
<tr>
<td>2</td>
<td>Activity/Speed indicator:</td>
</tr>
<tr>
<td></td>
<td>- OFF - 10Mbps data rate is used</td>
</tr>
<tr>
<td></td>
<td>- On (Green) - 100 Mbps data rate is used</td>
</tr>
<tr>
<td></td>
<td>- On (Amber) - 1Gbps data rate is used</td>
</tr>
</tbody>
</table>

WebUI Requirements

To connect to the Lights Out Management (LOM) card WebUI, use a supported web browser:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
First-Time Setup

The LOM Card loads automatically when the host appliance is connected to a power source.

**Note** - Because the LOM Card's certificate is signed privately, your web browser does not trust the Certificate Authority that generated it. After you finish first time setup, you can replace the SSL certificate with your own certificate. See "Configuring an SSL Certificate" on page 15.

**Step 1 - Start the LOM Card for the first time and change the password**

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 1    | Install the LOM Card in a compatible appliance.  

  - For 6000 (excludes 6500, 6800) and 7000:  
    See [5000, 6000, 7000, 15000, and 23000 Appliances Installing LOM Card](#)  
  - For 16000, 16600HS, 26000, 28000, 28600HS, and TE2000XN:  
    See [16000, 26000, 28000, and TE2000XN Appliances Installing LOM Card](#)  
| 2    | Connect an RJ45 network cable between a computer and the applicable port on the LOM Card.  
| 3    | On the connected computer, configure a static IPv4 address in the same subnet as the default IP address of the LOM Card.  

  The default IPv4 address of the LOM Card is **192.168.0.100**.  
  The static IP address on the connected computer must be in the subnet **192.168.0.0 / 255.255.255.0**.  
  For example: **192.168.0.50**.  
| 4    | On the connected computer, in a web browser, connect to the default IPv4 address of the LOM Card:  

  **https://192.168.0.100**  
| 5    | Enter the default username and password: **admin** and **admin**.  
| 6    | Click **Login**.  

  Guidelines to change the password for the default user come into view.  
| 7    | In the fields, enter a new password for the default user. The password must follow these rules:  

  - At least eight characters  
  - No spaces  
  - Is case sensitive  
  - Must not contain all of the user's account name  
  - Must contain characters from three of these categories:  
    - English uppercase characters ("A' through 'Z")  
    - English lowercase characters ("a' through 'z")  
    - Base 10 digits (0 through 9)  
    - Non-alphanumeric characters (~ ! @ # $ % ^ & *)
### First-Time Setup

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Click <strong>Submit</strong>. The <strong>Welcome to LOM first time wizard</strong> page opens.</td>
</tr>
</tbody>
</table>

### Step 2 - Configure the LOM Card Settings

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the <strong>Welcome to LOM first time wizard</strong> page, click <strong>Next</strong>. The <strong>IPV4 Configuration</strong> page opens.</td>
</tr>
<tr>
<td>2</td>
<td>In the <strong>Host Name</strong> field, enter a name to show for the host appliance in the LOM Card interface. Permitted: alphanumeric characters, dash (-), underscore (_). Forbidden: special characters, spaces.</td>
</tr>
</tbody>
</table>
| 3    | You must configure an IPv4 address for the LOM Card. Select how the LOM Card obtains its IPv4 address:  
  - Select **DHCP** to get an IPv4 address automatically.  
  - Select **IP Setting** to configure a static IPv4 address. If you select this option, configure the applicable:  
    - **IPv4 Address**  
    - **Net Mask**: A subnet mask is required to configure the LOM Card.  
    - **Gateway**: If you configure a subnet that is not directly connected to the LOM Card, then a default gateway is required to configure the LOM Card. |
| 4    | Click **Next**. The **IPV6 Configuration** page opens. |
| 5    | **Optional**: You can configure an IPv6 address for the LOM Card. Select an IPv6 configuration for the LOM Card:  
  - **Disabled** - The LOM Card gets no IPv6 address.  
  - **Enable DHCP IPv6** - The LOM Card gets an IPv6 address automatically.  
  - **Enable Static** - The LOM Card gets a static IPv6 address. If you select this option, configure the applicable:  
    - **IPv6 Index**  
    - **IP Address (IPv6)**  
    - **Subnet Prefix Length**  
  
  **Note** - After you finish the First Time Configuration Wizard, you can remove the IPv4 configuration and use only an IPv6 configuration for the LOM Card. See "Configuring the LOM Card’s IPv4 or IPv6 Address" on page 11. |
| 6    | Click **Next**. The **DNS Configuration** page opens. |
### Step 7: Optional

If it is necessary for the LOM Card to synchronize its internal clock with an NTP server, you must configure the applicable NTP settings. If you specify the NTP server by its host name instead of its IP address, you must configure a DNS server.

- If you configured a static IPv4 address, you can enter the IPv4 addresses for up to three DNS servers. The LOM Card accesses the DNS servers in the order listed. For example, if the LOM Card fails to access DNS Server 1, then it accesses DNS Server 2.
- If you configured a static IPv4 address and do not want to configure a DNS Server, leave all three fields blank.
- If you configured DHCP for IPv4, then you cannot configure a DNS server in the First Time Wizard. You can configure a DNS server after you complete the First Time Wizard. See "Configuring DNS Settings and Changing the Host Name" on page 13.

#### Instructions

- **Click Next.**

  The **Remote Control** page opens.

### Step 8

Click **Next**.

The **Remote Control** page opens.

### Step 9

Select access restrictions for **KVM**.

**KVM** - Abbreviation for "keyboard, video, and mouse". Allows users to control the appliance's command line interface (CLI) with a keyboard and mouse.

Select one of these access settings for **KVM**:

- **Subnets of specified IP addresses** - Lets users access KVM only from IP addresses in specific subnets. If you select this option, a text box opens. Enter one or more IP subnet addresses. Put a semicolon between IP subnet addresses, with no spaces.
  
  For example: 198.2.37.0;155.82.46.0;123.3.237.0

- **To all** - Allows KVM access to the LOM Card from all IP addresses.

- **Disabled** - Does not let users access KVM from any IP address.

### Step 10

Select access restrictions for **Virtual Media**.

**Virtual Media** - Ability to install software on the appliance from an ISO file (imitates a CD-ROM) or IMG file (imitates a hard disk and other types of external storage). Access the LOM card from your computer or from an external storage device connected to the appliance.

As you did for KVM access settings, select one of these access settings for Virtual Media:

- **Subnets of specified IP addresses**
- **To all**
- **Disabled**

### Step 11

Click **Next**.

The **Date and Time Settings** page opens.
<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 12   | Below **Time Method**, select a way to set date and time:  
  - **Set time manually**:  
    a. Below **Date & Time**, click the clock icon. A calendar appears.  
    b. Select the date.  
    c. Below the calendar, click the **clock** icon.  
    d. Use the arrows to select the hour, minute, and second.  
    e. Below **Time Zone**, select the time zone.  
  - **Use Network Time Protocol (NTP)**:  
    The LOM Card gets date and time from an NTP server.  
    a. Enter an IP address for a primary NTP server.  
    b. Optional: Enter an IP address for a secondary NTP server.  
    The LOM Card accesses this server if it fails to access the primary NTP server. |
| 13   | Click **Next**.  
The **Finish** page opens.  
A popup message opens to show you the LOM Card is reset. |
| 14   | To connect to the LOM Card again:  
  a. Close your browser session.  
  b. Open a new browser session.  
  c. Clear the browser cache.  
  d. After a minimum of one minute, enter the LOM Card's new IPv4 or IPv6 address into the browser. |
LOM Card Configuration

Configuring an IP Address

The LOM Card needs at least one of these:

- IPv4 address
- IPv6 address

**Note** - Initial IPv4 setup is part of the First Time Wizard. See "First-Time Setup" on page 7.

Configuring the LOM Card's IPv4 or IPv6 Address

1. Do one of these:
   - From the left navigation panel, click the Home view.
     In the LOM Information panel, in the Network Settings section, click Edit.
   - From the left navigation panel, click LOM view > Network Configuration > IP Settings.
     The IP Settings menu opens.

2. If desired, configure an IPv4 address.
   - To configure a static IPv4 address:
     a. Select **Enable IPv4**.
     b. Enter values for:
        - IPv4 Address
        - IPv4 Subnet
        - IPv4 Gateway
     - To configure a dynamic IPv4 address, select **Enable IPv4 DHCP**.

3. If desired, configure an IPv6 address:
   - To configure a static IPv6 address:
     a. Select **Enable IPv6**.
     b. Select an IPv6 Index.
     c. Enter an IPv6 Address.
     d. Enter a Subnet Prefix Length.
   - To configure a dynamic IPv6 address, select **Enable IPv6 DHCP**.

**Note** - If you previously configured a static IP Address and then enable DHCP, the fields for the static IP addresses stay populated and the background changes from white to gray. This means that the values are saved but inactive.

4. Click **Save**.
5. A popup message tells you to reconnect in a new browser session.
6. In a new browser session, reconnect to the device.

⚠️ **Important** - You can only access the device at an IPv4 or an IPv6 address that you saved.
Configuring DNS Settings and Changing the Host Name

Configure one or two DNS servers to resolve the NTP Server hostnames for automatic date and time. See "Configuring date and time automatically" on page 19.

The Host Name is the name for the LOM Card in the Home view. This name may be different from the name used for the appliance in the network interface. The Host Name is not related to web hosting. You can only change the Host Name when DNS is enabled.

Enabling the LOM Card's DNS Settings and Changing the Host Name

1. From the left navigation panel, click the LOM view > Network Configuration > DNS Settings.
2. Click DNS Enabled.
3. Below Host Name Setting, select one:
   - Automatic: Configures a Host Name for the LOM Card automatically.
   - Manual: Enter a Host Name for the LOM Card.
4. Below Domain Name Setting, select one:
   - Automatic: Configures a domain name for the LOM Card automatically.
   - Manual: Enter a domain name for the LOM Card.
5. Below Domain Name Server Setting, select one:
   - Automatic: Configures a DNS server automatically. Below IP Priority, select one:
     - IPv4
     - IPv6
   - Manual: Enter up to three DNS servers. The LOM Card accesses the DNS servers in the order they are listed. For example: If the LOM Card fails to access DNS Server 1, it then accesses DNS Server 2.
6. Click Save.
7. A popup message tells you to reconnect in a new browser session.
Configuring Link Speed and Duplex Settings

You can configure the link speed and duplex settings for the LOM Card network connection to match your environment.

Configuring the link speed and duplex mode of the LOM Card's connection to the network

**Note** - When you access the LOM Card port from a directly connected computer, traffic speed is faster than when you connect to the LOM Card port through other network devices.

1. From the left navigation panel, click LOM view > Network Configuration > Link Settings.
2. Choose one:
   - To have the link speed and duplex mode determined automatically, select Auto Negotiation.
     - The link speed defaults to the highest available speed, up to 1,000 Mbps.
     - The Duplex Mode defaults to Full Duplex if Full Duplex is available.
   - To turn off Auto Negotiation and to set the link speed and duplex mode manually, clear Auto Negotiation and configure these:
     - **Link Speed**: From the drop-down menu, select 100 Mbps or 10 Mbps.
     - **Duplex Mode**: Select Full duplex or Half duplex.
3. Click Save.
4. To see your changes, refresh the page in your web browser.
Configuring an SSL Certificate

You can generate a new SSL Certificate for the LOM Card or upload an existing SSL Certificate.

**Generating an SSL Certificate for the LOM Card**

1. From the left navigation panel, click **LOM view > Network Configuration > SSL Certificate**.
2. Select **Generate**.
3. A popup window opens called **Generate Certificate**.
4. Enter:
   - **Common Name (CN)**
     - Maximum length: 64 alphanumeric characters.
     - The special characters "#” and "$” are not allowed.
   - **Organization (O)**
     - Maximum length: 64 alphanumeric characters.
     - The special characters "#” and "$” are not allowed.
   - **Organization Unit (OU)**
     - Maximum length: 64 alphanumeric characters.
     - The special characters "#” and "$” are not allowed.
   - **City or Locality (L)**
     - Maximum length: 128 alphanumeric characters.
     - The special characters "#” and "$” are not allowed.
   - **State or Province (ST)**
     - Maximum length: 128 alphanumeric characters.
     - The special characters "#” and "$” are not allowed.
   - **Country (C)**
     - Must be two characters.
     - Special characters are not allowed.

**Best Practice:** Use Alpha-2 country codes described in the ISO 3166 international standard.

- **Email Address:** Email address of the organization
- **Valid for:**
  - Value in days.
  - Minimum: 1.
• Maximum: 3,650.
  □ Key Length: Preset for 2,048 bits.

Note - To view length and special character restrictions for each field, select the question mark icon in the upper right of the popup window.

5. Click Save.

6. After a few seconds, a popup message says "SSL certificate has been saved successfully."

7. Click OK.

Uploading an existing SSL Certificate for the LOM Card

1. From the left navigation panel, click LOM view > Network Configuration > SSL Certificate.
2. Under New Certificate, to the right of the field, click the folder icon.
3. Find the SSL certificate file on your computer. The certificate file must be in .pem format.
4. Below New Private Key, to the right of the field, click the folder icon.
5. Find the private key file on your computer and select it. The private key file must be in .pem format.
6. Optional: If there is a passphrase defined for the private key, enter it in the field below Passphrase.
7. Click Save.
Configuring LOM Card Services

You can configure the port and the user access for these LOM Card services:

- **Web** - access to the LOM Card web user interface
- **KVM** (Keyboard Video Mouse, also called Virtual Media) - access to the host appliance's Command Line Interface (CLI)
- **CD-media** - access to a virtual CD drive on the host appliance
- **HD-media** - access to a virtual hard disk drive on the host appliance

>Note - Maximum Sessions shows the maximum number of users allowed to use a service at the same time. Each service has a preset and unchangeable maximum number of users.

**Viewing or stopping a current user session**

1. From the left navigation panel, click LOM view > Network Configuration > Services.
2. A table shows LOM Card service status. The left column shows a list of LOM Card services. In the same row as a service, on the right side, select the three lines icon.

   ![Three lines icon](image)

3. The Service Sessions menu opens and shows a list of current user sessions for the service.
4. To stop a user session, click the red icon on the far right of the row that contains the User Name.

**Enabling or disabling a LOM Card service**

1. From the left navigation panel, click LOM view > Network Configuration > Services.

   A table shows LOM Card service status. The left column shows a list of LOM Card services.

2. In the same row as a service, on the right side, select the pencil icon.

   The Service Configuration menu opens.

3. Do one of these:
   - Select Active to enable the service.
   - Clear Active to disable the service.

   ![Important](image) - When you clear Active and click Save, you disable the service immediately, including for your own user account.

4. Click Save.

   The changes that you configured are saved.
Changing the port or timeout for a LOM Card service

1. From the left navigation panel, click LOM view > Network Configuration > Services.
2. A table shows LOM Card service status. The left column shows a list of LOM Card services. In the same row as a service, on the right side, select the pencil icon.

   The Service Configuration menu opens.
3. In Secure port, enter a new port number.
4. In Timeout, enter a timeout time for the service.
   - Web and KVM timeout range: 300 to 1800 seconds.
   - Web timeout does not happen if there is an active KVM Console session.
   - Timeout values: multiples of 60 seconds.
5. Click Save.

   The changes that you configured are saved.

Viewing an audit log of user sessions

1. From the left navigation panel, click LOM view > Audit Log.
2. Filter the log for a range of dates.
   a. Click the left clock icon and select a start date.
   b. Click the right clock icon and select an end date.

   Note - To filter for one day, select the same day as the start date and the end date.

   An audit log appears.
Configuring Date and Time Settings

You can configure date and time for the LOM Card manually, or configure the LOM Card to get date and time automatically from an NTP Server.

**Configuring date and time manually**

1. From the left navigation panel, click LOM view > Date and Time.
2. Clear **Automatic NTP Date & Time**.
3. To the right of the first field, click the clock icon.
   - A calendar appears.
4. Select the date from the calendar.
5. Below the calendar, click the clock icon.
6. Use the up and down arrow buttons to set the hour, minute, and second.
7. In the **Select Time Zone** drop down menu, select the time zone.
8. Click **Save**.
9. A popup message tells you to reconnect in a new browser session.
10. Click **OK**.
11. The browser session closes.
12. In a new browser session, log in to the LOM Card.
   - The LOM Card shows the correct time.

**Configuring date and time automatically**

1. Select **Automatic NTP Date & Time**.
2. Below **Primary NTP Server**, enter the IP address or domain name of an NTP server.
   - **Note** - To access the NTP server through a domain name, the LOM Card needs DNS configured. See "Configuring DNS Settings and Changing the Host Name" on page 13.
3. **Optional**: Below **Secondary NTP server**, enter the IP address or domain name of a second NTP server. If the LOM Card fails to connect to the Primary NTP Server, it connects to the Secondary NTP Server.
4. A popup message tells you to reconnect in a new browser session.
5. Click **OK**.
6. The browser session closes.
7. In a new browser session, log in to the LOM Card.
   - After one minute, the LOM Card synchronizes with the NTP server and shows the correct time.
Users and Access

Signing In to the LOM Card Interface

Procedure

1. Enter your username.
2. Enter your password.
3. Click Login.

One of two messages appears for an unsuccessful login attempt:

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Failed</td>
<td>Username or password is incorrect.</td>
</tr>
<tr>
<td>User access is denied. Please contact the administrator.</td>
<td>One of these is the case:</td>
</tr>
<tr>
<td></td>
<td>• An administrator denied the user's access privileges. See &quot;Changing a User's Privilege Level and Disabling a User Account&quot; on page 23.</td>
</tr>
<tr>
<td></td>
<td>• The user exceeded the maximum number of failed login attempts. See &quot;Login Block Settings (Failed Login Attempts)&quot; on page 26.</td>
</tr>
</tbody>
</table>

Signing Out of the LOM Card Interface

Procedure

1. In the top right corner of the Home view, click your username.
   A drop-down menu opens.
2. In the bottom right corner of the menu, click Sign Out.
Making a New User Account

In the LOM Card interface, you can configure a maximum of nine users.

Note - To have more users, configure the LOM Card to use a RADIUS Server or an LDAP Server. Each user logs in with a username and password.

Procedure

1. From the left navigation panel, click LOM view > User Configuration > User List.
2. Select a white rectangle with a plus sign in it.
   The New User popup window opens.
3. In the Username field, enter a username that fits these rules:
   - String of 4 to 16 alphanumeric characters
   - Starts with an alphabetical character
   - Is case sensitive
   - Does not include special characters
4. In the Password field, enter a password.
   Default rules:
   - At least eight characters
   - No spaces
   - Is case sensitive
   - Must not contain all of the user's account name
   - Must contain characters from three of these categories:
     - English uppercase characters ('A' through 'Z')
     - English lowercase characters ('a' through 'z')
     - Base 10 digits (0 through 9)
     - Non-alphanumeric characters (~ ! @ # $ % ^ & *)

Note - To disable the default password rules, select Skip Complex Password Rules.

5. Below Confirm Password, enter the new password again.

Important - For the new user to get access to the LOM Card, you must select Enable User Access.
6. Select a privilege level for the user:

- **Administrator**: Can use all features in the Home view.
- **Operator**: Can view all pages and settings in the Home view, but cannot change any settings or perform any actions. Cannot access the Remote KVM page.
- **User**: Can view these pages in the Home view: Sensor Reading, Event Log, Date and Time, SSL Certificate, Services, and Audit Log. Cannot change any settings or perform any actions. Cannot access the Remote KVM page.
- **No Access**: The user is saved in the system, but is not allowed to access the Home view.

7. Click **Save**.
Changing a User's Privilege Level and Disabling a User Account

For a user configured locally on the LOM Card, you can change the user's account privilege level, disable a user account, and configure settings for failed login attempts.

Procedure

1. From the left navigation panel, click LOM view > User Configuration > User List.
   Select a user by clicking the three dots in the top right of the box that contains the name of the user.
   Three dots icon:

2. Select Edit.

3. Select a privilege level:
   - **Administrator**: Can use all features in the Home view.
   - **Operator**: Can view all pages and settings in the Home view, but cannot change any settings or perform any actions. Cannot access the Remote KVM page.
   - **User**: Can view these pages in the Home view: Sensor Reading, Event Log, Date and Time, SSL Certificate, Services, and Audit Log. Cannot change any settings or perform any actions. Cannot access the Remote KVM page.
   - **No Access**: The user is saved in the system, but is not allowed to access the Home view.

4. Select how to apply Login Block Settings to the user (see "Login Block Settings (Failed Login Attempts)" on page 26):
   - **Enable**: Login block settings always apply to the user.
     - Example: If the Login Block Settings specify 5 Maximum Login Attempts and a Login Block Timeout of 15 minutes, then after 5 failed login attempts the user is blocked for 15 minutes.
   - **Disable**: Login Block Settings never apply to the user. The user is never blocked as a result of failed login attempts.
   - **Blocked**: Starting from when you click Save, blocks the user for the duration of the Login Block Timeout time.
     - Example: If the Login Block Timeout time listed in the Login Block Settings is 10 minutes, then starting from when you click Save the user is blocked for 10 minutes.
   - **Always Blocked**: Always prevents the user from entering.
Best Practices:
- To disable a user account for a short period, keep the privilege the same and clear the Enable User Access checkbox.  
  **Use Case:** Setting up an account a week or two before a new employee’s start date.
- To disable a user account for a long period, from the Privilege drop-down menu, select No Access.  
  **Use Case:** Disabling access for an employee going on extended leave.

5. Click **Save**.

   The changes to configurations are saved.

## Changing a User's Password

You can change a password for a user configured locally on the LOM Card.

### Procedure

1. From the left navigation panel, click **LOM view > User Configuration > User**.
2. Select a user by clicking the three dots in the top right of the box that contains the name of the user.
   
   Three dots icon: 

3. Select **Edit**.
4. In the **Password** field, enter a password.

   Default rules:
   - At least eight characters
   - No spaces
   - Is case sensitive
   - Must not contain all of the user’s account name
   - Must contain characters from three of these categories:
     - English uppercase characters (‘A’ through ‘Z’)
     - English lowercase characters (‘a’ through ‘z’)
     - Base 10 digits (0 through 9)
     - Non-alphanumeric characters (~ ! @ # $ % ^ & *)

   **Note** - To disable the default password rules, select **Skip Complex Password Rules**.

5. Click **Save**.

   The selected user's password is changed.
Deleting a User Account

You can delete an account for a user configured locally on the LOM Card.

Procedure

1. From the left navigation panel, click **LOM view > User Configuration > User List**.
2. Select a user by clicking the three dots in the top right of the box that contains the name of the user.
   
   ![Three dots icon:](image)
3. Select **Delete**.
5. Click **OK**.
   
   The selected user account is removed permanently.

Note - You cannot remove a user account while you are logged in with it.
Login Block Settings (Failed Login Attempts)

You can prevent users from accessing the LOM Card for a set time period after a specified number of failed login attempts.

Login Block Settings apply to all users that have Login Block User Management set to Enable. See “Changing a User's Privilege Level and Disabling a User Account” on page 23.

Procedure

1. From the left navigation panel, click LOM view > User Configuration > Login Block Settings.
2. Below Maximum Login Attempts, enter a number:
   - Minimum: 1
   - Maximum: 99
   - Default Maximum: 5
3. Below Login Block Timeout, enter a number of minutes:
   - Minimum: 1
   - Maximum: 180
   - Default Maximum: 15
4. Click Save.
   The login block settings are updated.

Note - After a firmware update, all login block settings return to default values. See "Maintenance" on page 46.
Connecting the LOM Card to a RADIUS Server

You can configure a RADIUS server to authenticate LOM Card users.

Procedure

1. From the left navigation panel, click LOM view > User Configuration > RADIUS Setup.
2. Select Enable RADIUS authentication.
3. Configure these settings:
   - Server address: must be IPv4 or IPv6 address
   - Port:
     - Default port: 1812
     - Port value range: 1 - 65535
   - Secret:
     - At least 4 characters
     - No spaces
     - Maximum: 32 characters
   - Timeout:
     - Default: 3 seconds
     - Range: 3 - 50 seconds
4. **Optional:** To connect a second RADIUS server as a backup:
   a. Select Enable 2nd Radius Authentication.
   b. Configure the settings.
5. Click Save.

The RADIUS server is configured to authenticate LOM Card users.
Connecting the LOM Card to an LDAP Server

You can configure an LDAP server to authenticate LOM Card users.

Procedure

1. Select an encryption type:
   - No Encryption
   - SSL
   - **StartTLS**: If you select this option, **FQDN** shows as an option below **Common Name Type**.

2. **Common Name Type**:
   - If you selected **No Encryption** or **SSL**, then **IP Address** is the only available option and is selected by default.
   - If you selected **StartTLS**, then an option shows for **FQDN**. **IP Address** is selected by default. Select **FQDN** to configure an FQDN as an alternative to an IP address.

3. Below **Server Address**, enter an IPv4 address, an IPv6 address, or an FQDN.

4. Enter these:
   - **Port**
   - **Bind DN**
   - **Password** (the LDAP bind password)
   - **Search Base**

5. Under **Attribute of User Login**, select one of these:
   - **cn**
   - **uid**

6. If you selected **StartTLS** encryption, select the folder icon.
   - Upload these required files from your computer:
     - **CA certificate file**
     - **Certificate File**
     - **Private Key**

7. Click **Save**.
   - The LDAP server is configured to authenticate LOM Card users.
Adding an LDAP Group

You can use the LOM Card interface to add groups to a configured LDAP server and to assign privilege levels to each group.

Procedure

1. From the left navigation panel, click **LOM view > User Configuration > LDAP Groups**.
2. Select a white rectangle with a plus sign in it.
3. A popup window opens called **New Group**.
4. Enter a **Group Name**.
5. Enter a **Group Domain**.
6. From the drop-down menu, select a **Group Privilege**. This privilege level applies to all members of the group.
   - **Administrator**: Can use all features in the Home view.
   - **Operator**: Can view all pages and settings in the Home view, but cannot change any settings or perform any actions. Cannot access the **Remote KVM** page.
   - **User**: Can view these pages in the Home view: **Sensor Reading**, **Event Log**, **Date and Time**, **SSL Certificate**, **Services**, and **Audit Log**. Cannot change any settings or perform any actions. Cannot access the **Remote KVM** page.
   - **No Access**: The user is saved in the system, but is not allowed to access the Home view.
7. Click **Save**.
   
   The LOM Card recognizes the LDAP group.
Changing the Privilege Level of an LDAP Group

You can change the privilege level of an LDAP group.

Procedure

1. From the left navigation panel, click **LOM view > User Configuration > LDAP Groups**.
2. Select the LDAP group by clicking the three dots in the top right of the box that contains the name of the LDAP group.
   - Three dots icon: ⋮
3. Select **Edit**.
4. From the drop-down menu, select a **Group Privilege**. This privilege level to apply to all members of the group.
   - **Administrator**: Can use all features in the Home view.
   - **Operator**: Can view all pages and settings in the Home view, but cannot change any settings or perform any actions. Cannot access the **Remote KVM** page.
   - **User**: Can view these pages in the Home view: Sensor Reading, Event Log, Date and Time, SSL Certificate, Services, and Audit Log. Cannot change any settings or perform any actions. Cannot access the **Remote KVM** page.
   - **No Access**: The user is saved in the system, but is not allowed to access the Home view.
5. Click **Save**.

The new privilege level applies to the LDAP group.
Renaming an LDAP Group

You can rename an LDAP group in the LOM Card WebUI.

**Procedure**

1. From the left navigation panel, click the LOM view > User Configuration > LDAP Groups.
2. Click the three dots in the top right corner of the rectangle that contains the name of the LDAP group.
   
   Three dots icon:
3. Select Edit.
4. Below Group Name, enter a new name.
5. Click Save.
   
   The new name appears for the LDAP group in the LOM Card WebUI.
## Power Management

This is a summary of the options for turning on, turning off, and restarting the appliance:

<table>
<thead>
<tr>
<th>Power Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power On</strong></td>
<td>Turns on the appliance. This is the only option that appears while the appliance is powered off.</td>
</tr>
<tr>
<td><strong>Power Off</strong></td>
<td>Performs a hard shutdown of the host appliance.</td>
</tr>
<tr>
<td><strong>Orderly Shutdown</strong></td>
<td>Sends a special control signal to the appliance that terminates all processes and turns off the appliance.</td>
</tr>
<tr>
<td><strong>Hard Reset</strong></td>
<td>Turns off the appliance immediately and then turns it on.</td>
</tr>
<tr>
<td><strong>Power Cycle</strong></td>
<td>Disconnects the electrical power from the appliance and immediately connects it again. This action is similar to pressing and releasing the power switch on the appliance. The LOM Card stays online during the Power Cycle.</td>
</tr>
</tbody>
</table>

**Notes:**
- This action is similar to pressing and holding the power switch on the appliance for a few seconds until the appliance turns off.
- This action does not disconnect electrical power from the appliance.

### Viewing the appliance power status in the Home view

1. From the left navigation panel, click the **Home view**.
2. In the **Device Information** panel, underneath the picture and hostname of your Check Point appliance, an indicator shows one of these:

   - **Power: 🔥 ON**
   - **Power: ✘ OFF**
Viewing the appliance power and process status in the Remote KVM window

1. From the left navigation panel, click the Home view.
2. In the Device Information panel, in the Console Session section, click Start.
3. The Remote KVM window opens.
4. Examine the Console screen (the black-background interface in the middle of the Console Session page).

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Powered Off</td>
<td>The appliance is off.</td>
</tr>
<tr>
<td>&quot;No Signal&quot;</td>
<td>The appliance is connected to power, but is off or does not work.</td>
</tr>
<tr>
<td>Starting the system</td>
<td>The appliance is in the middle of a reboot.</td>
</tr>
</tbody>
</table>

Turning On the Appliance

You can turn on the appliance in different ways.

Turning on the appliance from the Home view

1. From the left navigation panel, click the Home view.
2. In the Device Information panel, in the Power Action section, select Power On and click Go.

Chain of events:
1. A gray box with "Changing..." written in it covers the drop down menu.
2. The appliance turns on.
3. The power indicator changes to Power: ON.

Turning on the appliance in the Remote KVM window - from the Power Menu

1. From the left navigation panel, click the Home view.
2. In the Device Information panel, in the Console Session section, click Start.
3. The Remote KVM window opens.
4. From the top Power menu, select Power On.
5. In the browser popup, click OK to confirm the operation:
   You are about to perform a server power control operation

Chain of events:
1. The appliance turns on.
2. The Console screen shows "No Signal" for several seconds.
3. The Console screen shows the boot messages.
Turning on the appliance in the Remote KVM window - with the Power button

1. From the left navigation panel, click the **Home view**.
2. In the **Device Information** panel, in the **Console Session** section, click **Start**.
3. The **Remote KVM** window opens.
4. In the upper right of the screen, click the power button (the tooltip shows "Server is Powered Off").
5. In the browser popup, click **OK** to confirm the operation:

   You are about to perform a server power control operation.

Chain of events:

1. The appliance turns on.
2. The **Console** screen shows "No Signal" for several seconds.
3. The **Console** screen shows the boot messages.
Turning Off the Appliance

You can turn off the appliance in different ways.

These options are available in the Home view and in the Remote KVM window:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Off</td>
<td>This action is similar to pressing and holding the power switch on the appliance for 4 seconds until the appliance turns off. This action does <strong>not</strong> disconnect the electrical power from the appliance.</td>
</tr>
<tr>
<td>Orderly Shutdown</td>
<td>Sends a special control signal to the appliance that terminates all processes and turns off the appliance.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td>- This action is similar to running the &quot;<strong>shutdown -h 0</strong>&quot; command from the Expert mode on the CLI of the appliance.</td>
</tr>
<tr>
<td></td>
<td>- This action does <strong>not</strong> disconnect electrical power from the appliance.</td>
</tr>
</tbody>
</table>

Turning off the appliance from the Home view

1. From the left navigation panel, click the **Home view**.
2. In the **Device Information** panel, in the **Power Action** section, select the applicable option and click **Go**:
   - **Power Off**
   - **Orderly Shutdown**

Chain of events:

1. A gray box with "Changing..." written in it covers the drop down menu.
2. The appliance turns off and the power indicator changes to **Power: OFF**.
Turning off the appliance in the Remote KVM window - from the Power Menu

1. From the left navigation panel, click the **Home view**.
2. In the **Device Information** panel, in the **Console Session** section, click **Start**.
3. The **Remote KVM** window opens.
4. From the top **Power** menu, select the applicable option:
   - **Power Off**
   - **Orderly Shutdown**
5. In the browser popup, click **OK** to confirm the operation:

   You are about to perform a server power control operation

Chain of events:

1. If you selected the **Orderly Shutdown** option, then the **Console** screen shows "Halting" on the command line.
2. The appliance turns off.
3. The **Console** screen shows **Powered Off**.

Turning off the appliance in the Remote KVM window - with the Power button

1. From the left navigation panel, click the **Home view**.
2. In the **Device Information** panel, in the **Console Session** section, click **Start**.
3. The **Remote KVM** window opens.
4. In the upper right of the screen, click the power button (the tooltip shows "Server is Powered On").
5. In the browser popup, click **OK** to confirm the operation:

   You are about to perform a server power control operation

Chain of events:

1. The **Console** screen shows a progress circle indicator and this text:

   Network connection lost. Trying to reconnect.
2. The **Remote KVM** window shows the **Status** popup window with this text:

   Invalid Session Information To Reconnect. Session information is not available.

   Click **OK**.
3. The **Remote KVM** window closes.
4. The appliance turns off.
Restarting the Appliance

You can restart the appliance in different ways.

These options are available in the **Home view** page and in the **Remote KVM** page:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Reset</td>
<td>Turns off the appliance immediately and then turns it on.</td>
</tr>
<tr>
<td>Power Cycle</td>
<td>Disconnects the electric power from the appliance for a very short period. Then, connects the power to the appliance, and reboots the appliance.</td>
</tr>
</tbody>
</table>

**Restarting the appliance from the Home view**

1. From the left navigation panel, click the **Home view**.
2. In the **Device Information** panel, in the **Power Action** section, select **Power Cycle** and click **Go**.

Chain of events:

1. A gray box with "Changing..." written in it covers the drop down menu.
2. After several seconds, this page refreshes.
3. The **Power Action** section shows the **Power Off** option.

**Restarting the appliance in the Remote KVM window - from the Power Menu**

1. From the left navigation panel, click the **Home view**.
2. In the **Device Information** panel, in the **Console Session** section, click **Start**.
3. The **Remote KVM** window opens.
4. From the top **Power** menu, select **Power Cycle**.
5. In the browser popup, click **OK** to confirm the operation:

   *You are about to perform a server power control operation*

Chain of events:

1. The **Console** screen shows "No Signal" briefly.
2. The appliance turns off.
3. The **Console** screen shows **Powered Off**.
Host Device Sensors

The model name and serial number of the host appliance appear in the Home view > Device Information panel.

Sensors provide current information about the appliance. For details about your appliance’s sensors, see the Gaia Administration Guide (Chapter Maintenance > Section Hardware Health Monitoring) for the Check Point version installed on the appliance.

Viewing sensor information

1. From the left navigation panel, click the Check Point Appliance view > Sensor Reading.
   To see updated sensor information, in the top horizontal toolbar select Refresh.
2. Sensors show in three status groups. A status group shows only if there is a minimum of one sensor in the group:
   - **Critical Sensors** - sensors with readings above the Upper Critical threshold or below the Lower Critical threshold.
   - **Normal Sensors** - sensors with readings in the normal range.
   - **Disabled Sensors** - sensors that are inactive. This can be for an expected reason (for example: some sensors are only active when the appliance is powered) or because a sensor is broken.
3. The sensor indication as of the last page refresh shows to the right of the Sensor Name, below Reading.
4. To see the critical and non-recoverable values set for a sensor, hover over it with your mouse.
5. To filter sensor information by sensor type, select a type of sensor from the Filter by type drop-down menu.
   For example, selecting Fan from the Filter by type drop-down menu shows only fan sensor information. Then, selecting All Sensors shows information from all sensors.

>Note - The list of sensors depends on the specific hardware of the appliance.

Viewing an Event Log of sensor events

Event logs appear if the current value of a sensor is lower or higher than the required threshold (for example, a fan speed is lower than required).

From the left navigation panel, click Check Point Appliance view > Event Log.
Filter information by date and by sensor.

>Note - You can filter for one sensor at a time.
Remote Media Access

Limiting Access to Remote Media by IP Address

You can configure access to Remote Media only for specific IP Addresses, or block it completely.

Configuring access to KVM (Console Session) for specific IP Addresses

1. From the left navigation panel, click the Check Point Appliance view.
2. Click KVM VMedia Settings.
3. Below Virtual Media, select access restrictions for Virtual Media:
   - **To all** - Allow access to Virtual Media (KVM) on the LOM Card from all IP addresses.
   - **Disabled** - Block access to Virtual Media (KVM) on the LOM Card from all IP addresses.
   - **Subnets of specified IP addresses** - Allow access to Virtual Media (KVM) on the LOM Card only from IP addresses in specific subnets.

   - Enter one or more IP subnet addresses in the empty field below the KVM checklist. Enter a semicolon (;) between IP subnet addresses, with no spaces.

   Example:
   
   198.2.37.0;155.82.46.0;123.3.237.0

   **Important** - If you select **Disabled** and then click **Save** (or if you select **Subnets of specified IP addresses** and do not enter the network subnet of your computer's web host), you lose access to the Console Session (KVM).

   To restore access to the Console Session (KVM) for yourself:
   a. Select one of these:
      • **All IP addresses**.
      • **Subnets of specified IP addresses**, and enter the network subnet of your computer's web host.
   b. Click **Save**.

4. Click **Save**.

   The selected Virtual Media (KVM) access restrictions take effect.
Configuring access to Virtual Media for specific IP Addresses

1. From the left navigation panel, click the Check Point Appliance view.
2. Click KVM VMedia Settings.
3. Below Virtual Media, select access restrictions for Virtual Media:
   - **To all** - Allows access to Virtual Media (KVM) on the LOM Card from all IP addresses.
   - **Disabled** - Blocks access to Virtual Media (KVM) on the LOM Card from all IP addresses.
   - **Subnets of specified IP addresses** - Allows access to Virtual Media (KVM) on the LOM Card only from IP addresses in specific subnets.
     - Enter one or more IP subnet addresses in the empty field below the KVM checklist. Enter a semicolon (;) between IP subnet addresses, with no spaces.
     
     Example:
     
     198.2.37.0;155.82.46.0;123.3.237.0

Important - If you select Disabled and then Save (or if you select Subnets of specified IP addresses and do not enter the network subnet of your computer's web host), you can no longer upload virtual media to the appliance. To restore Virtual Media access for yourself:

   a. Select one of these:
      - All IP addresses.
      - Subnets of specified IP addresses, and enter the network subnet of your computer's web host.

   b. Click Save.

4. Click Save.

The selected Virtual Media (KVM) access restrictions take effect.
Configuring Remote Media Settings

You can configure mount settings for CD/DVD on NFS or CIFS.

Procedure

1. From the left navigation panel, click the Check Point Appliance view > Remote Media Settings.
2. Click Remote Media Support.
3. Select Mount CD/DVD or Mount Storage Device.
4. Enter the server address of an NFS or CIFS server.
5. Enter the file path on the server.
6. Select the file system:
   - NFS
   - CIFS: Enter Domain Name, Username, and Password.
7. To use the same settings for HD media as for CD media, select Same settings for storage device images.
8. Click Save.

The selected mount settings take effect.
Image Redirection

You can redirect a CD/DVD image or a hard disk image to the host device.

Configuring Image Redirection

1. From the left navigation panel, click Check Point Appliance view > Image Redirection.
2. Find a file to upload from a drop-down menu in the column below Image Name in the row to the right of Media Type.
   
   To show all files previously saved on the Remote Media Settings page, select Refresh Image List.
3. Use the buttons on the right side of the row to control the redirection.
   
   - Play button: Starts the redirection. Shows a popup message when redirection is complete.
   - Stop button: Stops the redirection.
   - Eject button: Removes the virtual disk from the host appliance.

Uploading a CD image from your computer

1. From the left navigation panel, click Home view.
2. In the Device Information panel, in the Console Session section, click Start.
3. The Remote KVM window opens.
4. In the top right corner, click Browse File.
5. Select a file to upload from your computer.
   
   Supported media file types: *.iso, *.nrg
   Supported formats: ISO9660, UDF (v1.02 - v2.60)
6. Click Start Media.
   
   A popup window opens.
7. Click OK.
KVM (Console Session) Access

You can access the command line interface (CLI) on the host appliance through a KVM session (keyboard-video-mouse).

Starting a KVM Console Session

1. From the left navigation panel, click Home view.
2. In the Device Information panel, in the Console Session section, click Start.
   The Remote KVM window opens.

Stopping a KVM Console Session

In the top left corner of the Remote KVM window, click Stop KVM.
   The Remote KVM window closes.

Refreshing the console video

If the console video does not behave as expected, you can refresh it manually.
   Below Video, select Refresh.
   The video refreshes.

Pausing the console session video

1. Below Video, select Pause Video.
2. To start the video again, select Resume Video.
   The video restarts.

Creating and entering hotkeys and macros into the console

Some keys or key combinations on your keyboard take effect on your computer's operating system rather than the console session.

Select a set hotkey or key combination from the Send Keys drop down menu to enter it into the console.

Creating a macro

1. From the Hot Keys drop-down menu, select Add New Keys.
3. Select Add.
4. Enter a key combination to make into a macro. Select buttons for the Windows, Alt+F4, or Print Screen keys. Do not enter these keys from your keyboard.
5. Select Insert.
   The macro is saved.
Entering a user-defined macro into the console

From the **Hot Keys** drop-down menu, select the macro.

The macro appears in the console.

Deleting a user-defined macro

1. From the **Hot Keys** drop-down menu, select **Add Hot Keys**.
2. Select the trash can icon adjacent to a macro to remove it.

The macro is deleted.

Changing the console video display quality

From the **Options** drop-down menu, select a number at the bottom of the menu.

- 0 = highest quality
- 7 = lowest quality

The console video quality changes.

Taking a screenshot of the console

1. From the **Video** drop-down menu, select **Capture Screen**.
   
   Your web browser downloads a screenshot.

2. Keep the screenshot on your computer.

Recording a video of the console

1. From the **Video Record** drop-down menu, select **Record Video**.
   
   By default, the video is recorded for the length of time set in **Record Settings**.

2. **Optional**: Select **Stop Recording** to stop the recording before the end of the time period set in the **Record Settings**.
   
   A recording generates until the point when you selected **Stop Recording**. Your web browser downloads a video.

3. Keep the video on your computer.
Configuring the length and quality of recorded console video

1. From the Video Record drop-down menu, select Record Settings.
2. Enter video length in seconds.
   - Minimum: 1 second
   - Maximum: 1800 seconds
3. Enter video compression as a decimal from 0.1 to 1.0.
   - Lowest quality: 0.1
   - Highest quality: 1.0
   - Increments: 0.1
4. Click OK.
   The selected settings change.
Maintenance

You can update the LOM Card's firmware. You can choose to preserve some or all of the LOM Card's configuration settings after the firmware update.

**Updating the LOM Card's firmware**

1. From the left navigation panel, click **LOM view > Maintenance > Firmware Update**.
2. Click the folder icon.
3. Find and select the firmware image on your computer.
4. Click **Verify Image File**.
   - If you uploaded an applicable image file, more menu options appear.
   - If you uploaded an image file that is not applicable, an error message appears:
     
     System detected unrecognized file. Please provide compatible firmware image.

     To continue, start the process again and select an applicable image file.
5. Choose which configuration settings to preserve after the update.
   - To preserve all configuration settings, select **Preserve all Configuration**.
   - To preserve some or no configuration settings, select **Edit Preserve Configuration**.
     a. The **Preserve Configuration** menu opens.
     b. Select the configurations to preserve.
     c. Click **Save**.

     The selected configurations are preserved after the update.
6. Click **Upload**.
7. The file uploads. A message shows version numbers for the **Current Image Version** and the **New Image Version**.
8. Select one (Note: These are the only two selectable menu options in the WebUI):
   - **Flash**: Completes the firmware upload. The LOM Card restarts.
   - **Cancel**: Cancels the firmware upload. The LOM Card restarts.
Restoring the LOM Card to factory default settings

1. From the left navigation panel, click **LOM view > Maintenance > Restore Factory Defaults**.
   - If you select a feature, the LOM Card restores the feature configuration to factory defaults after you click **Restore**.
   - If you do not select a feature, the LOM Card preserves the current feature configuration after you click **Restore**.

   **Optional** - To preserve the configuration for specific features:
   a. In the **Maintenance** menu, select **Preserve Configuration**.
   b. Select the configuration options to preserve.
   c. Click **Save**.

   **Important** - The LOM Card's IP address resets after you click **Restore**. To access the LOM Card after the firmware update finishes, you must connect to the LOM Card's default IP address and complete "First-Time Setup" on page 7.

2. Click **Restore**.
   The LOM Card reboots.

   **Note** - If you preserve NTP settings, after the reboot the LOM Card takes one minute to synchronize with the NTP server. After one minute, the LOM Card shows the correct date and time. See "Configuring date and time automatically" on page 19.

Approving System Administrator access

Check Point support may request for you to approve their access to your LOM Card WebUI.

1. From the left navigation panel, click **LOM view > Maintenance > System Administrator**.
2. Select **Enable User Access**.
3. Select **Change Password**.
4. In the **Password** and **Confirm Password** fields, enter a temporary password for this support session.
5. Click **Save**.

A Check Point support engineer uses these credentials to connect to your LOM Card WebUI:

- **Username** - sysadmin
- **Password** - the string you configured

**Important** - At the end of the support session:
1. Clear **Enable User Access**.
2. Click **Save**.