26 November 2017

Lights Out Management (LOM)

Administration Guide

Smart-1/5000/13000/15000/21000/23000 Appliances

Classification: [Protected]

Check Point
SOFTWARE TECHNOLOGIES LTD.

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.

More Information

Visit the Check Point Support Center http://supportcenter.checkpoint.com.

Latest Version of this Document

Download the latest version of this document http://downloads.checkpoint.com/dc/download.htm?ID=32414.

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

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 Lights Out Management (LOM) Administration Guide.

Revision History

Date	Description
26 Nov 2017	Fixed Firmware Update for 21000 Series Appliances ("Firmware Update" on page 35)
6 July 2016	Updated for 5000, 15000, and 23000 Appliances
18 November 2014	First release of this document

Contents

Using Lights Out Management WebUI

In This Section:

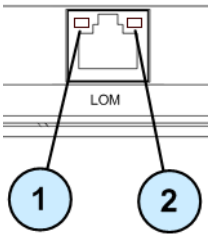
Introduction

This document applies to these appliances:

- Smart-1 225/3050/3150
- 5000 Appliances
- 13000 Appliances
- 15000 Appliances
- 21000 Appliances
- 23000 Appliances

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 not responding, if the appliance is connected to a power source.

LOM port



Item	Description
1	Link on Smart-1, 13000, and 21000 series appliances • OFF - No Link • ON (Amber) - Link is established • Blink (Amber) - Link is active Link on 5000, 15000, and 23000 series appliances • OFF - No Link • ON (Green) - Link is established • Blink (Green) - Link is active
2	Activity/Speed on Smart-1, 5000, 13000, 15000, and 23000 series appliances • OFF - 10 Mbps data rate is used • ON (Green) - 100 Mbps data rate used • ON (Amber) - 1 Gbps data rate is used Activity/Speed on 21000 series appliances • OFF - 10 Mbps data rate is used • ON (Green) - 1 Gbps data rate is used • ON (Amber) - 100 Mbps data rate is used

WebUI Requirements

- A supported web browser
- Java™ software installed on the local computer (minimum version 6u20)

These web browsers are supported:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome

Logging In to the WebUI

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

Note - As the LOM certificate is privately signed, the browser does not trust the certificate authority that generated it. After initial login, you can replace the SSL certificate with your own certificate ("SSL Settings" on page 26).

To log in to the LOM WebUI:

1. Make sure pop-ups are allowed in your web browser.
2. Connect a network cable to the LOM port.
3. Make sure that the computer is on the same network subnet.

For example:

IP address 192.168.0.x

Netmask 255.255.255.0

4. Enter the IP address of the LOM port into the browser.
   - Default: https://192.168.0.100

   A security certificate alert message opens.
5. In the security certificate alert window that opens, do this:
   - In Microsoft Internet Explorer - Click Continue to this website
   - In Google Chrome - Click Proceed anyway
   - In Mozilla Firefox - Click Advanced > Add Exception
6. In the LOM login window that opens, enter your user name and password.
   - Default user name: admin (with Administrator privileges)
   - Default password: admin
7. Change the default password.

   Note - For security reasons, the LOM enforces the change of password at the first login.
8. Click Login.

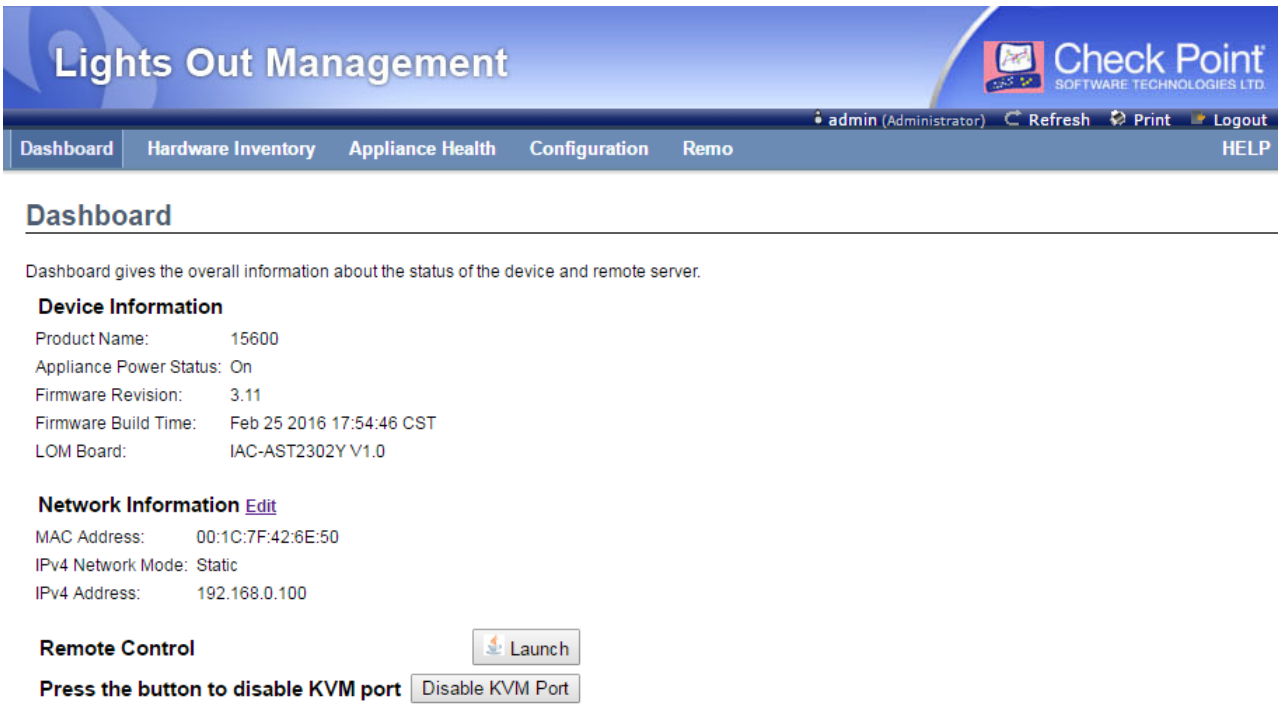
   The Dashboard window opens.

WebUI Dashboard

The Dashboard window shows this information about the appliance and LOM:

- Appliance model
- Appliance power status
- Firmware version
- Network configuration

- Remote console launcher



Note - When you are using the LOM WebUI, we recommend that you do not use the browser refresh function. Instead, use the **Refresh** menu item built into the LOM WebUI.

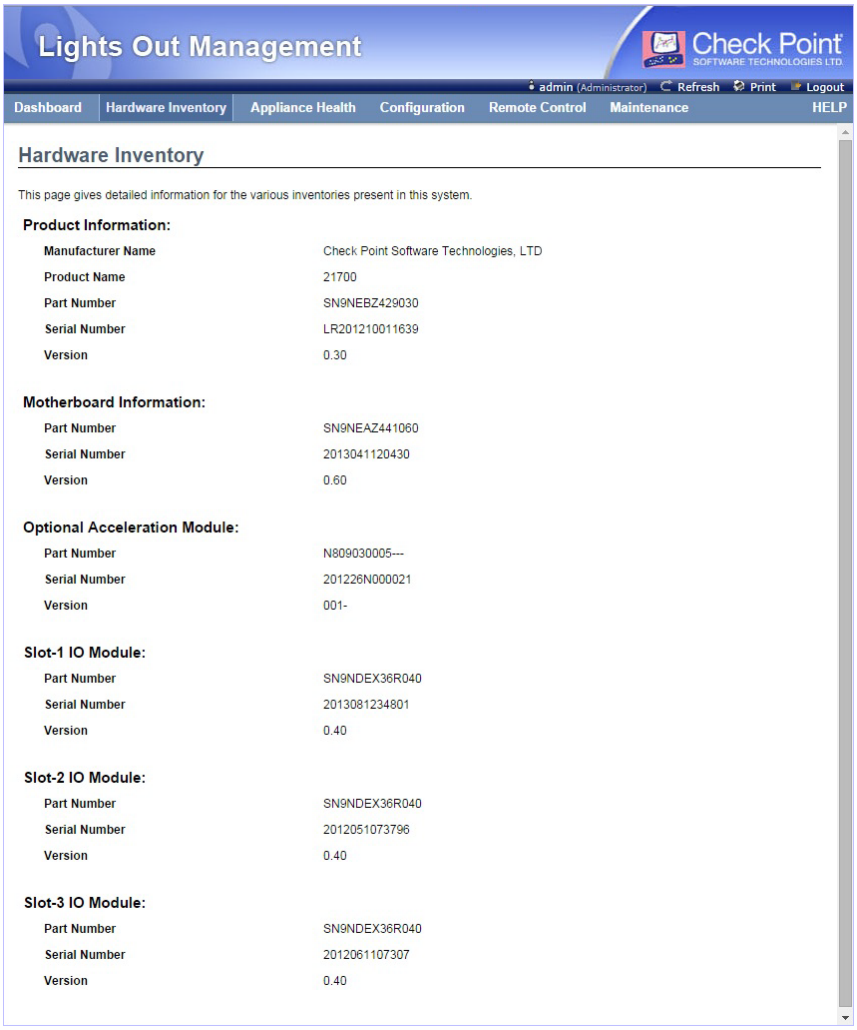
Showing Hardware Information

The **Hardware Inventory** window shows information about the appliance and hardware components. This information includes:

- Product name
- Serial number
- Hardware revision

To show the hardware information:

From the menu bar, click **Hardware Inventory**.



Monitoring Appliance Health

In This Section:

Monitoring Appliance Health

Use the Sensor Readings window to show the status and settings of the hardware sensors on the appliance.

The limits for the sensors are defined according to these thresholds:

- **LNR - Lower Non-Recoverable** - The sensor reading is outside of the operational range. The system will fail.

  Recommendation: Contact Check Point support.
- **LC - Lower Critical** - The sensor reading is outside of the normal range. The system can become unstable.

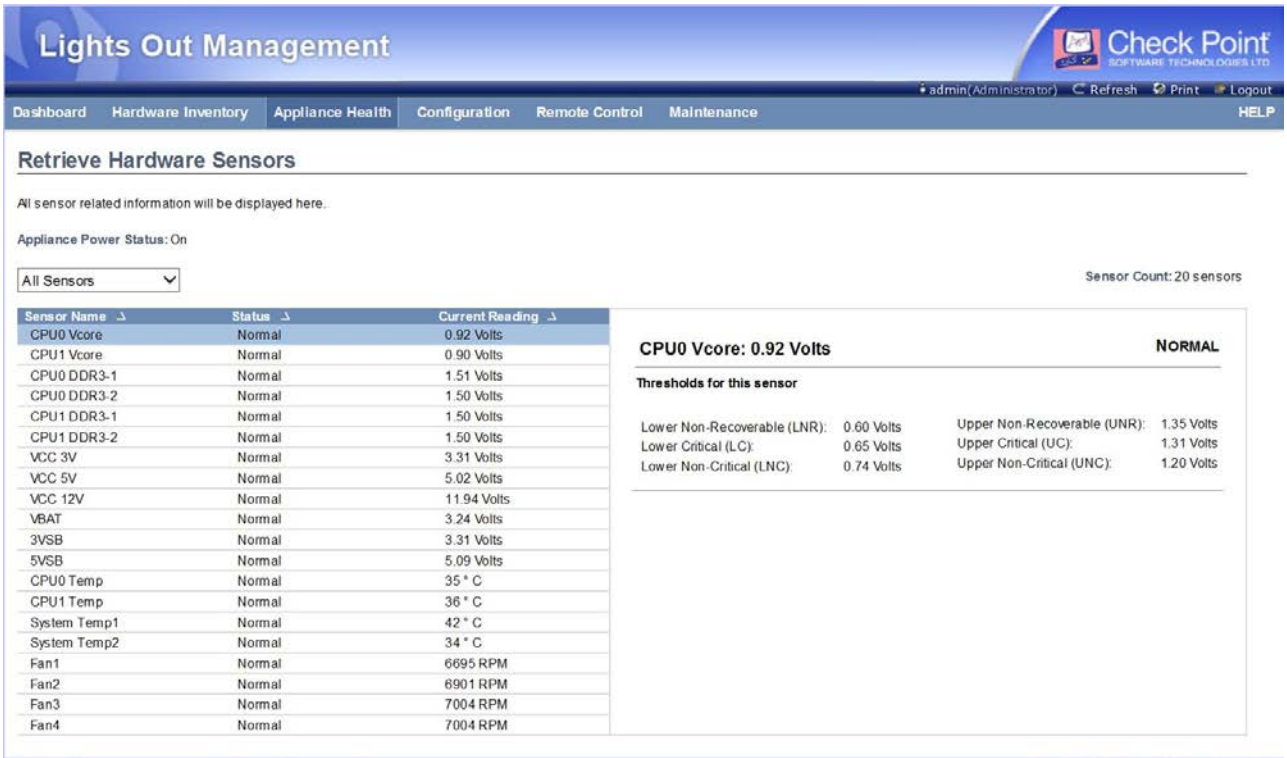
  Recommendation: Continue monitoring. If the problem persists, contact Check Point support
- **LNC - Normal (Lower Non-Critical)** - The sensor reading is at the lower end of the normal range. The system is okay.

  Recommendation: No action required.
- **UNC - Normal (Upper Non-Critical)** - The sensor reading is at the upper end of the normal range. The system is okay.

  Recommendation: No action required.
- **UC - Upper Critical** - The sensor reading is outside of the normal range. The system can become unstable.

  Recommendation: Continue monitoring. If the problem persists, contact Check Point support.
- **UNR - Upper Non-Recoverable** - The sensor reading is substantially outside of the operational range. The system will fail.

Recommendation: Contact Check Point support.



To show the sensor readings:

1. Select **Appliance Health > Retrieve Hardware Sensors**.
2. From the drop-down menu, select **All Sensors** or a hardware sensor.

   The window shows the list of all sensors or the data for the selected sensor. Select a sensor from the list, and see its specified values on the right hand side of the screen.

   You can click **View this Event Log** to open the **Event Log** window ("Event Log" on page 11) and show the logs for the specified sensor.

Event Log

The **Event Log** window shows all events that were logged. These events include hardware health events as well as LOM system events such as restarts, login, and configuration changes.

The log shows system-critical events, with the date, time, and severity of each event.

These are the drop-down menus that filter the logs:

- **Types of events** - Only show logs for the specified event type
- **Hardware sensors** - Only show logs that are generated by the specified hardware sensor

These are the time zone settings for the log time stamp:

- **BMC Timezone** - The time zone that is configured on the appliance
- **Client Timezone** - The time zone for the Internet browser on the local client

To filter the event logs:

1. Select **Appliance Health > Event Log**.
   The **Event Log** window opens.
2. From a drop-down menu, select the filter.
   The **Filter** window shows the filtered logs.

To delete the event logs:

Click **Clear All Event Logs**.

Configuring Settings

In This Section:

Users Settings

Use the **User Management** window to configure the settings and privileges for the LOM users. You must have administrator privileges to change these settings.

To show user information and privileges:

Select **Configuration** > **Users**. The **User Management** window opens.

Field Name	Description
User ID	User ID number
Username	Login name of the user
User Access	Shows if the user is **Enabled** to log in to LOM
Network Privilege	Assigned role of the user

Configuring Users

Use the **Modify User** window to change the settings of a user for LOM.

To configure a user:

1. Select **Configuration** > **User**.
   The **User Management** window opens.
2. Create or configure the user:
   - To create a user, select a **UserID** and click **Add User**
   - To change the settings for a user, select a user and click **Modify User**

   The **Modify User** window opens.
3. Configure information and privileges of the user.

4. Change the password (when necessary):
   a) Select **Change Password**.
   b) Enter a new password in the **New Password** field.
   c) Re-enter the password in the **Confirm New Password** field to confirm.
5. Click **Add** or **Apply**.

Field Name	Description
Username	Login name of the user
Change Password	When selected, you can change the password for a user
Password Size	Maximum length of the password
New Password	Enter a new password
Confirm New Password	Enter the new password again
User Access	Select **Enable** to let the user log in to the LOM
Network Privilege	Assigned role of the user
Skip Complex Passwords Rules	Select **Enable** to choose a simple password without the rules.

Users and Privileges

You can configure LOM user accounts with these privileges:

- **Administrator** - Can configure settings in all windows and launch JViewer console
- **No Access** - Access privileges are suspended, but the user account is not deleted
- **Operator and User -** Cannot configure LOM settings.

This table shows a list of viewable settings per account type.

Window	Operator Can View	User Can View
Dashboard	Yes	Yes (cannot see network settings)
Hardware Inventory	Yes	Yes
Retrieve Hardware Sensors	Yes	Yes
DNS	Yes	No
LDAP	Yes	No
LDAP-Advanced Settings	Yes	No
Mouse Mode	Yes	Yes
Network	Yes	No

Window	Operator Can View	User Can View
Network Link	Yes	No
NTP	Yes	Yes
RADIUS	Yes	No
Services	Yes	Yes
SSL – Upload	Yes	Yes
SSL – Generate	Yes	Yes
SSL – View	Yes	Yes
Users	Yes	No
Login Block	Yes	No
Console Redirection	Yes	Yes
Appliance Power Control	Yes	Yes
Firmware Update	No	No
Preserve Configuration	No	No
Restore Factory Defaults	No	No
System Administrator	No	No

Deleting Users

To delete a user:

1. Select **Configuration** > **User**.
2. Select a user and click **Delete User**.
   A confirmation window opens.
3. Click **OK**.
   The user is deleted.

Login Block Settings

Use the **Login Block Settings** window to configure the maximum number of failed login attempts to LOM for each IP address.

To configure the login block settings:

1. Select **Configuration** > **Login Block**.
   The **Login Block Settings** window opens.
2. Configure the settings for failed logins.

3. Click **Save**.

Setting	Description
Enable/Disable Login Block	When selected, enforces the login block policy according to its settings
Max Login Attempt	Sets the maximum number of login failures from an IP address
Login Block Timeout	Sets the number of minutes that an IP address is blocked from logging in to LOM
Management	Determine the users to include in the **Login Block** by enabling or disabling the user name.

RADIUS Settings

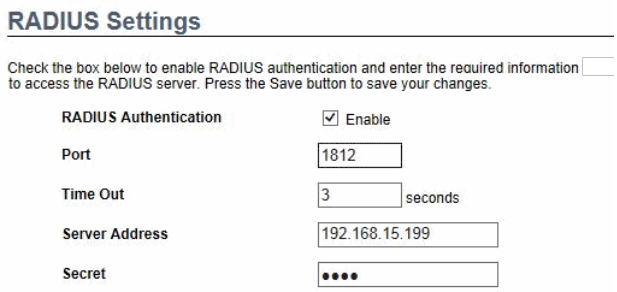
RADIUS settings must be configured in both the LOM and RADIUS server.

Use the **RADIUS Settings** window to configure LOM to connect to a RADIUS server. Specified users in the RADIUS database can log in to LOM.

Configuring RADIUS in LOM

To configure the RADIUS setting:

1. In the LOM WebUI, select **Configuration > RADIUS**.
   The **RADIUS Settings** window opens.



2. Configure the settings for RADIUS authentication.

Field Name	Description
RADIUS Authentication	When selected, enables RADIUS based authentication.
Port	Port of the RADIUS server (default `1812`).
Time Out	Number of seconds that LOM waits for a response from the RADIUS server. After this time, the RADIUS authentication fails and the user cannot log in to the LOM. The value is between 3 - 300 seconds.
Server Address	IPv4 address of the RADIUS server.
Secret	Case-sensitive text string. This value is the same as setting on the RADIUS server. The string contains between 4 - 31 characters.

3. Click **Save**.

Configuring the RADIUS Server Using Cisco ACS

To enable the configuration of the Cisco RADIUS server, use the Cisco Secure ACS GUI.

To create a user:

1. Open the Cisco Secure ACS GUI.
2. Click **Users and Identity Stores > Internal Identity Stores > Users**.
3. Click **Create**.
4. Add a **Name**, for example `lomadmin`.
5. In **Enable Password**, add a password and **Confirm Password**.

To create a network:

1. In the Cisco Secure ACS GUI tree, click **Network Resources > Network Devices and AAA Clients**.
2. Click **Create**.
3. Add a **Name**, for example `Lom_Device`.
4. Select **RADIUS**.
5. Add a **Shared Secret**.
6. Click **Submit**.

To create an Authorization Profile:

1. In the Cisco Secure ACS GUI tree, click **Policy Elements> Authorization and Permissions > Network Access > Authorization Profiles**.
2. Click **Create**.
3. In the **General** tab, add a **Name**, for example `Lom_Rule`.
4. Click the **RADIUS Attributes** tab.

5. For **Dictionary Type**, choose `RADIUS-IETF`.
6. For **RADIUS Attribute**, click **Select**.
7. In the **RADIUS Dictionary** window, select the **Attribute** `Reply-Message`.
8. Click **OK**.
9. In the **RADIUS Attributes tab**, for **Attribute Value**.
   a) Select `Static.`
   b) For the required field, enter `privilege=Administrator`
      Exactly as written. Case sensitive.

   The required RADIUS attributes in this window are:

Field Name	Value
Dictionary Type	`RADIUS-IETF`
RADIUS Attributes	`Reply-Message`
Attribute Type	`String`
Attribute Value	`Static`
	`privilege=Administrator`

10. Click **Add**.
11. Click **Submit**.

To create an Access Policy:

1. In the Cisco Secure ACS GUI tree, click **Access Policies > Access Services > Default Network Access > Authorization**.
2. In the **Standard Policy** page of the **Network Access Authorization Policy**, click **Customize**.
3. In the **Customize Conditions** window, make sure `System:UserName` is in the **Selected** list.
4. Click **OK**.
5. In the **Standard Policy** page, click **Create**, to create a policy rule.
6. Select `System:Username` and `equals` and the user created earlier (in this example, `lomadmin`).
7. Add the Authorization profile to the rule:
   a) Click **Select**.
   b) Select the Authorization profile created earlier (in this example, `Lom_Rule`).
8. Click **OK**.
9. Click **Save Changes**.

Configuring Other RADIUS Servers

The instructions in this section apply to FreeRADIUS. For other RADIUS servers, refer to the RADIUS server documentation.

To configure a FreeRADIUS Server:

1. On the RADIUS server, set **Reply-Message** for the privilege for each user in the `User` file. Otherwise, LOM rejects the user account. The parameter in the file that defines privileges for LOM user is: `Reply-Message = "privilege=<LEVEL>"`. Make sure that there are no blank spaces in the privilege parameter.

   The privilege levels are:

   `Administrator`

   `Operator`

   `No-Access` (user cannot log in to LOM)

   Sample parameter for a user with administrator privileges:

   ```
   Reply-Message = "privilege=Administrator"
   ```

2. Configure the secret on the RADIUS server. This value is also entered in the **Secret** field.

   For example, In `clients.conf`, change the secret line to: `Secret = testing123`

LDAP and eDirectory Settings

Use the **LDAP Settings** page to configure LOM to connect to an LDAP server. You can select the LDAP groups that can log in to LOM. This page shows these details:

- LDAP or eDirectory server is enabled for LOM
- LDAP groups that can log in to LOM
- Privilege level for each LDAP group

Authentication Workflow

When a user tries to log in to LOM, the first successful authentication for the username and password is used. This is the order for authentication:

1. LOM internal user database
2. LDAP Role group 1
3. LDAP Role groups 2 - 5

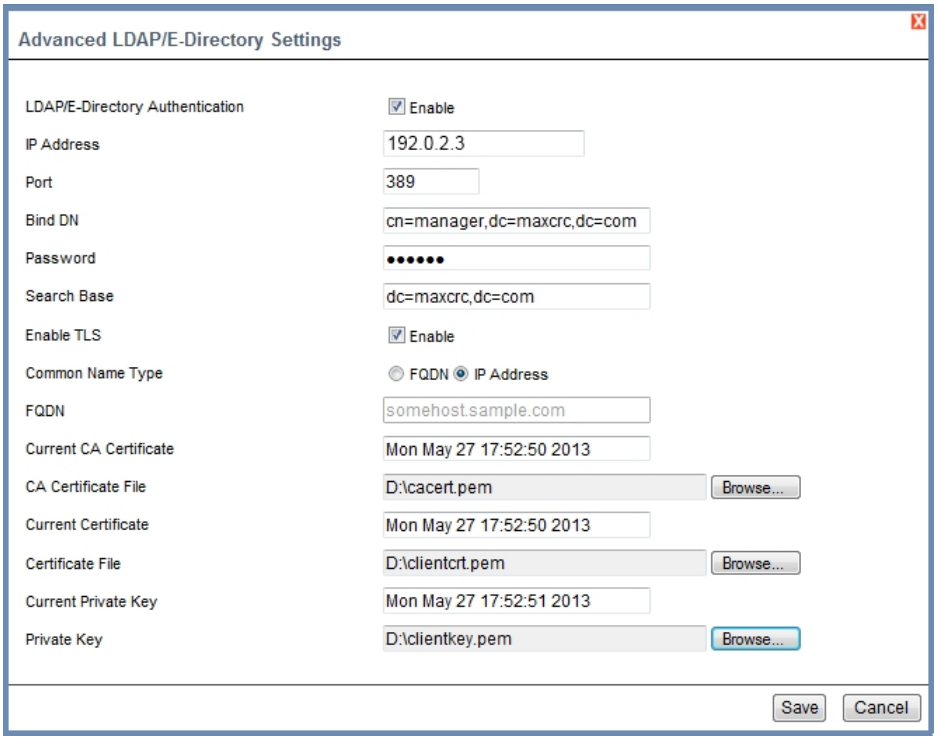
For example, LDAP Role group 1 has User privileges and LDAP Role group 3 has Administrator privileges. If John Smith is in both LDAP Role groups, he can only log in to LOM with User privileges.

Configuring an LDAP Server

Use the **LDAP Configuration Page** to configure LOM to connect to an LDAP server. You can select the LDAP groups that can log in to LOM.

You can also configure TLS to encrypt the connection between LOM and the LDAP server.

Note - The LDAP settings in this guide are based on the OpenLDAP standard. Some of the details can be different for other LDAP standards.



To configure authentication from an LDAP server:

1. For TLS encryption, do these steps:
   a) On the LDAP server, create these files:
      - CA certificate
      - Client certificate
      - Client key
   b) Log in to LOM.
2. Make sure that the **NTP Settings** (on page 25) are the same as the LDAP server.
3. Select **Configuration > LDAP/E-Directory**.
   The **LDAP/E-Directory Settings** window opens.
4. Click **Advanced Settings**.
   The **Advanced LDAP/E-Directory Settings** window opens.
5. Enter the settings for the LDAP server.
6. For TLS encryption, configure these settings:
   a) From **Enable TLS**, select **Enable**.
   b) Select **FQDN** or **IP Address**. For FQDN, enter the FQDN of the LDAP server.
   c) Click **Choose File** to upload each certificate file and the private key.
7. Click **Save**.
   Note: If you change the Advanced LDAP settings, it is possible that you must log in to the WebUI again.

Field Name	Description
LDAP/E Directory Authentication	When selected, enables LDAP groups to log in to LOM.

Field Name	Description
IP Address	IP address of the LDAP server.
Port	The default port is 389.
Bind DN	DN for binding user. Make sure that this user has the correct permissions for the groups and users that log in to LOM. Sample format for the DN: `cn=manager,ou=login,dc=domain,dc=com`
Password	Password for the binding user.
Search Base	Define the node for the search in the directory tree. You can specify to start the query from an OU, or the root. Samples for the **Search Base** query: • `ou=user,ou=login,dc=domain,dc=com` • `dc=sampledomain,dc=com`
Enable TLS	When selected, enables the TLS (Transport Layer Security) LDAP extension. Use this extension to supply extra security.
Common Name Type	Select if the CN for the certificate uses the **IP Address** or the **FQDN** (Fully Qualified Domain Name) of the LDAP server.
FQDN	For certificates that use a FQDN for the CN, enter the FQDN of the LDAP server.
Current CA Certificate File	Shows the date when the CA certificate was uploaded to the LDAP server. If this field is empty, the LDAP server does not have a CA certificate for LOM.
CA Certificate File	Click **Browse** to install the CA certificate file for the LDAP server.
Current Certificate File	Shows the date when the certificate file was uploaded to the LDAP server. If this field is empty, the LDAP server does not have a certificate for LOM.
Certificate File	Click **Browse** to install the certificate for the LDAP server.
Current Private Key	Shows the date when the private key file was uploaded to the LDAP server. If this field is empty, the LDAP server does not have a private key for LOM.
Private Key	Click **Browse** to install the key for the LDAP server.

Adding or Modifying an LDAP Group

After you configured the LDAP server, you can create or modify role groups from the LDAP server for LOM authentication. **Group Search Base** defines the node that LOM queries to authenticate LOM user. The LOM queries each group sequentially and uses the first successful authentication for a user.

To add or modify a role group:

1. Select **Configuration** > **LDAP/E-Directory**.
2. Select the Role Group ID and click **Add Role Group** or **Modify Role Group**.

   The **Role Group** window opens.
3. Configure the settings.
4. Click **Add** or **Modify**.

Field Name	Description
Role Group Name	Name for the group. Cannot contain blank spaces. **Note:** The **Role Group Name** must be the same as the group name setting on the LDAP server.
Role Group Search Base	Define the node for the search in the directory tree. You can specify to start the query from an OU, or the root. Samples for the **Search Base** query: • `ou=user,ou=login,dc=domain,dc=com` • `dc=sampledomain,dc=com`
Role Group Privilege	Select the LOM privilege ("Users and Privileges" on page 14) that is assigned to the users in this group.

Deleting an LDAP Group

To delete a role group:

1. Select **Configuration** > **LDAP/E-Directory**.
2. Select a role group and click **Delete Role Group**.
   A confirmation window opens.
3. Click **OK**.
   The role group is deleted.

DNS Server Settings

Use the **DNS Server Settings** window to configure the DNS settings of LOM. These settings make sure that you can use LOM on the network.

To configure the DNS settings:

1. Select **Configuration** > **DNS**.
   The **DNS Server Settings** window opens.
2. Configure the settings for the DNS server.
3. Click **Save**.

Host Configuration	
Host Settings	• **Automatic** - The DHCP server gives the DNS host name • **Manual** - Enter the **Host Name** in the field
Host Name	Host name of the appliance
Domain Name Configuration	
Domain Settings	• **Automatic** - The DHCP server gives the DNS domain name • **Manual** - Enter the host name in the field
Domain Name	Domain name for LOM
IPv4 Domain Name Server Configuration	
DNS Server Settings	• **Automatic** - The DHCP server gives the IPv4 DNS server address • **Manual** - Enter the IPv4 DNS server address in the field
Preferred DNS Server	The IPv4 address of the primary DNS server **Note -** Enter 0.0.0.0 to clear an IPv4 field. You cannot use empty strings for IPv4 addresses
Alternate DNS Server	The IPv4 address of the secondary DNS server

Network Settings

Use the **Network Settings** window to configure the settings for the LOM interface on the appliance.

To configure the network settings:

1. Select **Configuration > Network**.
   The **Network Settings** window opens.
2. Configure the settings for LOM interface.
3. Click **Save**.

Field	Description
LAN Interface	Shows the interface that is used to connect to LOM
LAN Settings	Enables the LOM interface
MAC Address	Shows the MAC address of the LOM interface
IPv4 Configuration	
Obtain an IP address automatically	• When **Use DHCP** is selected, LOM gets an IPv4 address from the DHCP server • When **Use DHCP** is cleared, enter the following settings for the LOM interface
IPv4 Address	Configures the IPv4 address for the LOM interface
Subnet Mask	Configures the subnet mask value for the LOM interface
Default Gateway	Configures the IPv4 address for the default gateway

Network Link Configuration

Use the **Network Link Configuration** window to configure the network link settings for the LOM physical interface on the appliance.

To configure the network settings:

1. Select **Configuration > Network Link**.
   The **Network Link Configuration** window opens.
2. Configure the network link settings for the LOM interface.
3. Click **Save**.

Field	Description
LAN Interface	Shows the interface that is used to connect to LOM.
Auto Negotiation	When enabled, the **Link Speed** and **Duplex Mode** are set automatically. In order to operate LOM at 1 Gb, you must enable **Auto Negotiation**.
Link Speed	Toggles the link speed to 10Mb or 100Mb to match your network environment. This option applies only in dedicated NIC mode, and is not available if **Auto Negotiation** is set to **On**.
Duplex Mode	Sets the **Duplex Mode** to **Full** or **Half**. This setting is not available if **Auto Negotiation** is set to **On**.

NTP Settings

Configure the **NTP Settings** for LOM. The time settings for LOM are automatically synchronized with the Security Gateway operating system (on 21000 appliances) or the BIOS (on 5000, 13000, 15000, 23000, and Smart-1 appliances) when the appliance is turned on. You can also manually enter the date and time settings, or configure the settings for an NTP server to automatically update them.

When you use an NTP server, LOM can keep the time settings when you update the LOM firmware or reset to factory settings. Use the Preserve Configuration window ("Preserve Configuration" on page 37) to keep the NTP settings after you update or reset LOM.

To use an NTP server:

1. Select **Configuration > Time**.
   The **Time Settings** window opens where you can configure the NTP settings.
2. Select **Automatically synchronize Date & Time with NTP server**.
3. Enter the settings for the **NTP Server**.
4. Click **Save**.

Services Settings

Use the **Services** window to show and configure the services on LOM.

To configure a service:

1. Select **Configuration > Services**.
   The **Services** window opens.
2. Select a service and then click **Modify**.
   The **Modify Service** window opens.
3. Configure the settings for the service.
4. Click **Modify**.
   These are the settings for the LOM services:

Field Name	Description
Service Name	Read-only field that shows the name of the service.
Current State	Select **Active** to enable the service.
Interfaces	Select an interface for the service. **LOM** is the LOM port on the appliance.
Nonsecure Port	Port that the service uses for unencrypted traffic.
Secure Port	Port that the service uses for encrypted traffic.
Timeout	Duration, in seconds, of service inactivity, after which the session closes (for Web service only).

SSL Settings

The default, pre-installed, LOM certificate is privately signed. As a result, the browser does not trust it. After initial login, you can replace the SSL certificate with one of these certificates:

- Self signed SSL certificates from the LOM WebUI - Must be set as trusted on the client browser
- Self signed SSL certificates from Clish - Must be set as trusted on the client browser
- CA signed SSL certificates from the Security Management Server

Generating a Self Signed SSL Certificate from the WebUI

After you create the certificate you must upload the certificate manually ("Uploading an SSL Certificate to LOM" on page 29).

To generate a new self signed SSL certificate from the LOM WebUI:

1. Select **Configuration > SSL**.

   The **SSL Certificate Configuration** window opens.
2. Click **Generate SSL**.
3. Enter the information for the certificate and the key:

   Note - Use only alphanumeric characters, hyphens, underscores, and periods. Do not use spaces. For **Email Address** field use any characters.
   - **Common Name (CN)** - The exact name being certified (usually the Web server's domain name)
   - **Organization (O)** - Name of the organization
   - **Organization Unit (OU)** - Name of the section in the organization
   - **City or Locality (L)** - City or location of the organization (required)
   - **State or Province (ST)** - State or province of the organization (required)
   - **Country (C)** - Country code of the organization (required)
   - **Email Address** - Email address for the organization (required)
   - **Valid For** - Number of days until the certificate expires
   - **Key Length** - Number of bits in the private key is **1024** bits
4. Click **Generate**.

To view the information on an existing SSL certificate:

1. Select **Configuration > SSL**.

   The **SSL Certificate Configuration** window opens.
2. Click **View SSL**.

Generating a Self Signed SSL Certificate from Clish

You can create an SSL certificate and a private key through CLI on Gaia and non-Gaia appliances. After you create the certificate you must upload the certificate manually ("Uploading an SSL Certificate to LOM" on page 29).

To create an SSL certificate and a private key on a Gaia appliance:

Run this command in expert mode:

```
cpopenssl req -config $CPDIR/conf/openssl.cnf -nodes -days <num_days>
-x509 -newkey rsa:<size_bits> -keyout <key_file> -out <output_file>
```

The command parameters are:

Parameter	Description
`-nodes`	Do not encrypt the output key.
`-days <num_days>`	This is optional parameter. Number of days a certificate generated by -x509 is valid for. The default is 30, the maximum is 3650, and 365 is the recommended value. **Note** - if you do not enter the `-days` parameter at all, the certificate will be valid for 30 days.
`-x509`	Output a x509 structure instead of a cert. req.
`-newkey rsa:<size_bits>`	Generate a new RSA key of `size_bits` in size. Valid values are 512, 1024, 2048, and 4096. We recommend to use 1024 or above.
`-keyout <key_file>`	Save the key in a specified `.pem` file. LOM accepts only `.pem` key file format.
`-out <output_file>`	Save the certificate in a specified `.pem` file. LOM accepts only `.pem` certificate file format.

When the command is executed, you will be asked to enter these parameters:

- Country Name - 2-letter code (for example: US)
- State or Province Name - full name (for example: New York)
- Locality Name - city (for example: Buffalo)
- Organization Name - company name (for example: My Company)
- Organizational Unit Name - section or department (for example: R&D)
- Common Name - system identifier (for example: Check Point 13500 LOM or MAC address)
- Email Address - full email address (for example: john@example.com)

Some fields have default values. If you leave them blank, the default value will be used.

Example: `cpopenssl req -config $CPDIR/conf/openssl.cnf -nodes -days 365 -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem`

To create an SSL certificate and a private key on a non-Gaia appliance:

Run this command:

```
openssl req -nodes -days <num_days> -x509 -newkey rsa:<size_bits> -keyout
<key_file> -out cert.pem
```

The command parameters are identical to the parameters for the `cpopenssl` command above.

Generating a CA Signed SSL Certificate from the Security Management Server

After you create the certificate you must upload the certificate manually ("Uploading an SSL Certificate to LOM" on page 29).

To create a CA signed SSL certificate from the Security Management Server:

1. Run this command in expert mode:
   `cpca_client create_cert -n "CN=<Common Name>" -f cert.p12 -w "" -k USER`
   Enter a value for this parameter:
   `Common Name` - system identifier (for example: Check Point 13500 LOM or MAC address)
2. Run: `cpopenssl pkcs12 -in cert.p12 -nokeys -clcerts -passin pass: -out cert.pem`
3. Run: `cpopenssl pkcs12 -in cert.p12 -nodes -nocerts -passin pass: -out key.pem`

For Example:

```
cpca_client create_cert -n "CN=FF:FF:FF:FF:FF:FF" -f cert.p12 -w "" -k USER
cpopenssl pkcs12 -in cert.p12 -nokeys -clcerts -passin pass: -out cert.pem
cpopenssl pkcs12 -in cert.p12 -nodes -nocerts -passin pass: -out key.pem
```

Uploading an SSL Certificate to LOM

To upload an SSL certificate and a private key to the LOM WebUI:

1. Select **Configuration > SSL**.
   The **SSL Certificate Configuration** window opens.
2. Click **Upload SSL**.
3. From **New Certificate**, click **Choose File** and select an SSL certificate file.
4. From **New Privacy Key**, click **Choose File** and select a private key file.
5. Click **Upload**.

Controlling the Appliance

In This Section:

Console Redirection

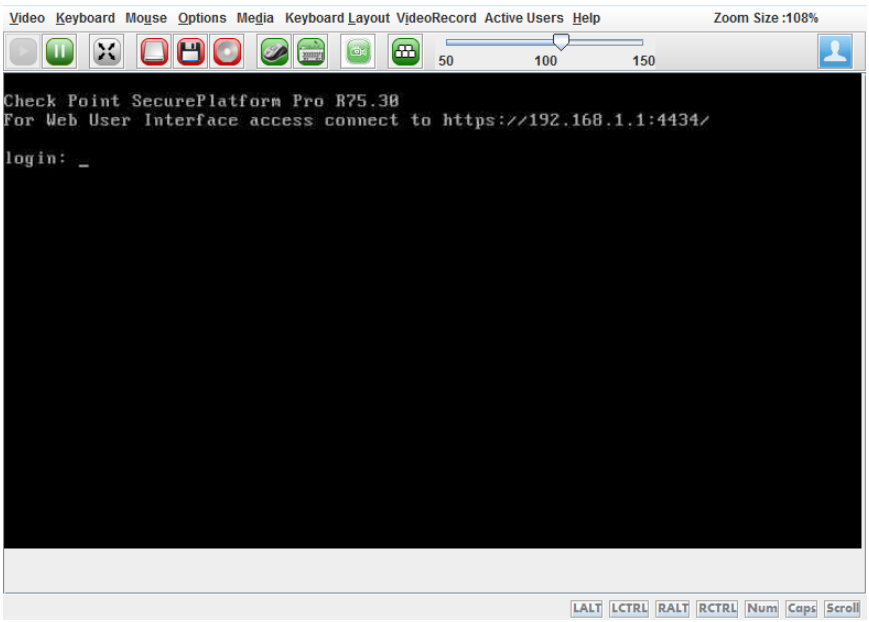
Use the **Console Redirection** window to launch the JViewer client console window. The JViewer client opens a virtual console for the appliance. You can use the Virtual Media client to access ISO images on your local computer and upload them to the appliance.

Launching the JViewer Client

Launch the JViewer client to open a console window and use the appliance CLI.

To launch the JViewer client:

1. Make sure that pop-ups are enabled in the browser.
2. Select **Remote Control > Console Redirection**.
   The **Console Redirection** window opens.
3. Click **Java Console**.
   The **jviewer.jnlp** file is downloaded.
   For Chrome, the **Save As** window opens for the **jviewer.jnlp** file.
   a) Open the file. The JViewer client opens in a new window.
   b) Java shows a security warning for the certificate.
   c) Java prompts you to run this application.



4. To use an on-screen keyboard, select **Keyboard Layout > SoftKeyboard > <language>**.
   The keyboard opens in a new window.
5. Use these menus to configure the console settings:
   - **Video**
   - **Keyboard**
   - **Mouse**
   - **Options**

Video

Use these menu options to configure the video settings for the JViewer client.

Menu Option	Description
Pause Redirection	Pauses the JViewer client
Resume Redirection	Resumes a paused JViewer client session
Refresh Video	Updates the console display
Compression Mode	Sets the compression algorithm, the default value is **YUV444+4ColorsVQ**
DCT Quantization Table	Sets the video quality, the default value is **4**
Host Video Output	When selected, the appliance console display is blank and the JViewer console is active
Full Screen	Shows the console display
Exit	Closes the JViewer client

Keyboard

Use these menu options to configure the keyboard settings for the JViewer client.

Menu Option	Description
Hold <ALT or CTRL> key	Sends a keystroke combination that uses the left or right ALT or CTRL key and the key that is entered
<Left or Right> Windows Key	Sends a keystroke combination that uses the left or right Windows key and the key that is entered
CTRL + ALT + DEL	Sends a keystroke combination that uses the CTRL, ALT, and DEL keys
Context menu	Selects a keystroke combination that uses the Context Menu key.

Mouse

Use these menu options to configure the mouse settings for the JViewer client.

Menu Option	Description
Show Cursor	When selected, the mouse cursor is visible in the console display
Mouse Mode	Select the settings for the mouse in the console window

Options

Use these menu options to configure settings for the JViewer client.

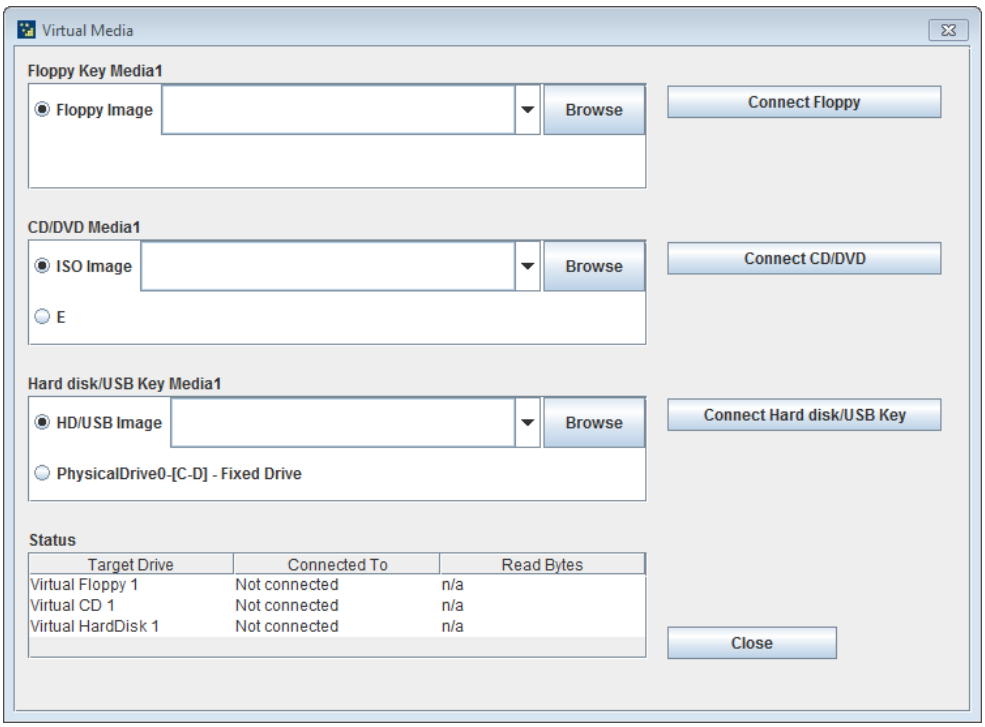
Menu Option	Description
Bandwidth	• Select **Auto Detect** to automatically configure the bandwidth for the JViewer client • Select the applicable bandwidth for the JViewer client
Keyboard/Mouse Encryption	When selected, the keystrokes and mouse movements sent to LOM are encrypted
Zoom In and **Out**	Changes the magnification of the console display

Launching the Virtual Media Client

Launch the Virtual Media client to manage virtual drives or ISO images on your local computer. You can then upload files to the appliance. You can emulate these media devices:

- Floppy disk drive
- CD/DVD drive and ISO image
- Hard disk drive and USB drive

Note - CDs, DVDs, and ISO files can only have Read Only privileges.



To use the Virtual Media client:

1. From the JViewer client, select **Media > Virtual Media Wizard**.
   The Virtual Media client opens.
2. From the applicable media type click browse and select the file.
3. Click **Connect <media>**.
   The media is connected to the appliance.

Installing an ISO Image on the Appliance

This is a sample procedure that describes how to use LOM to boot the appliance from an ISO image.

1. From an Internet Explorer browser, log in to the URL for LOM.
2. Select **Remote Console > Console Redirection**.
   The **Console Redirection** window opens.
3. Click **Java Console**.
   The JViewer client opens.
4. From the JViewer client, select **Media > Virtual Media Wizard**.
   The Virtual Media client opens.
5. From **CD/DVD Media**, click **Browse**.
6. Select the ISO image and click **OK**.
   The file name and path are shown in the Virtual Media window.
7. Click **Connect CD/DVD**.
8. Restart the appliance.
   a) Select **Remote Control > Appliance Power Control**.
   b) Select **Reset Appliance**.
   c) Click **Perform Action**.

   The appliance restarts and loads from the ISO image.

Power Control and Status

Use the **Power Control and Status** window to restart the appliance and turn it on and off.

Note - The power switch must be turned **On** to enable the **Power Control** features.

To configure the Power Control settings:

1. Select **Remote Control** > **Appliance Power Control**.
   The **Power Control** window opens and shows the status of the appliance.
2. Select the power option.
3. Click **Perform Action**.

Field Name	Description
Reset Appliance	Restarts the appliance (warm boot)
Power Off Appliance-Immediate	Turns the appliance off without shutting down the operating system
Power Off Appliance - Orderly Shutdown	Shuts down the operating system and then turns off the appliance
Power On Appliance	Turns on the appliance when it is **Off**.
Power Cycle Appliance	Shuts down the appliance and then turns it on (cold boot).

Managing the LOM Firmware

In This Section:

Showing the Firmware Version

Before and after updating firmware, use the WebUI to look at the installed firmware version.

To show the installed firmware version:

In the **Dashboard** tab, in the **Device information** section, see the **Firmware Revision**.

Firmware Update

Use the **Firmware Update** window to update the firmware of LOM. You can select to save some or all of the LOM settings. The saved settings are applied to the card after the update.

Before you update the firmware, download the most recent firmware version and save it to the local system. You can find the latest firmware version from sk88064 in the Check Point Support Center http://supportcontent.checkpoint.com/solutions?id=sk88064.

Note - When the firmware update is in process, LOM is not available to other users.

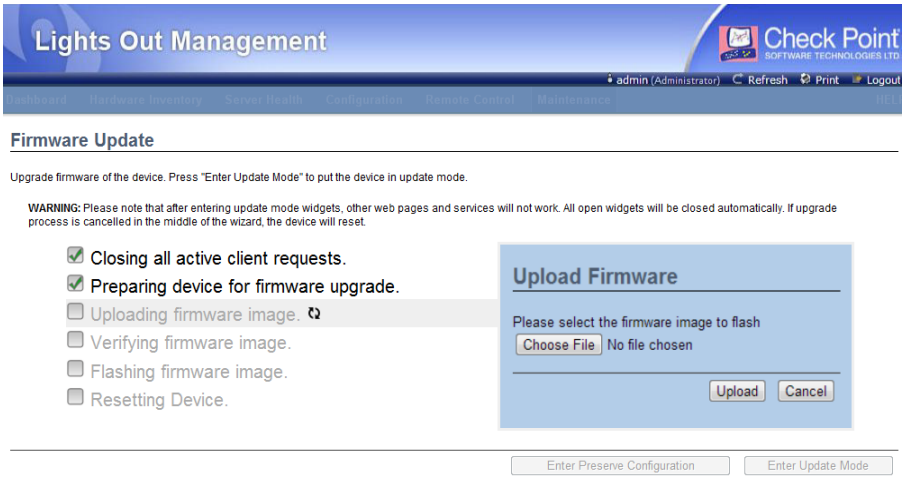
To update the LOM firmware:

1. For 21000 Appliance Series only: Make sure that the appliance power is off.
2. Select **Maintenance > Firmware Update**.

   The **Firmware Update** window opens.
3. **Recommended:** Use **Preserve All Configuration** to save all the LOM settings after the new firmware image is installed.
   - Select **Preserve all Configuration** to save all current LOM settings
   - Clear **Preserve all Configuration** to restore the LOM factory default settings
   - Click **Enter Preserve Configuration** to save some of the LOM settings ("Preserve Configuration" on page 37)
4. Click **Enter Update Mode**.

   A confirmation window opens.
5. Click **OK**.

LOM closes the active client requests and then prepares to update the firmware.



6. Click **Choose File** and select the LOM firmware image.
7. Click **Upload**.

   LOM

   - Uploads the firmware
   - Verifies the firmware image
   - Updates the firmware

   The update is complete when the **Status** is `100% Completed`, and this message shows:

```
Appliance management Firmware Image has been updated successfully
The Appliance management has been reset. You will not be able to access
the Appliance management with this browser session
Please wait and reconnect to the Appliance management using new browser
session
```

8. For 21000 Appliance Series only: We recommend that you do these steps before you use the appliance:

   a) Remove the AC or DC power supply cable.

   b) Wait for 15 seconds.

   c) Reconnect the cables.

   d) Turn on the appliance.

9. Wait a few seconds while the LOM card reboots.
10. Clear the browser cache and refresh the browser to continue using the LOM WebUI.

Preserve Configuration

Use the **Preserve Configuration** window to select the settings that are NOT reset to factory default when you update the LOM firmware.

Note - Select **IPMI** to save the settings for the LOM users that are logged in to LOM. If not, you must log in to the card using the default account.

To save LOM settings:

1. Select **Maintenance > Preserve Configuration**.
   The **Preserve Configuration** window opens.
2. For each item, select **Preserve Status** to save all the settings that are related to the item.
3. Click **Save**.

Preserve Configuration Item	LOM Settings	LOM WebUI Page
SEL	All system event logs	Appliance Health > Event Log
IPMI	Time zone	Configuration > Time
IPMI	All user settings	Configuration > User
IPMI	Password for the default admin account	Login to WebUI
KVM	All mouse mode settings	Configuration > Mouse Mode
KVM	KVM and Media Encryption settings	Configuration > Remote Session
Network	All DNS settings	Configuration > DNS
Network	All login block settings	Configuration > Login Block
Network	All network settings	Configuration > Network
NTP	NTP server setting	Configuration > Time
Services	All service settings	Configuration > Services
Authentication	All LDAP settings	Configuration > LDAP/E-Directory
Authentication	All RADIUS settings	Configuration > RADIUS
Authentication	All settings	Maintenance > System Administrator

These settings are always saved when you upgrade the firmware.

LOM Settings	LOM WebUI Page
All settings for SSL certificates	Configuration > SSL

You cannot save these settings and they are reset to factory default settings when you upgrade the firmware.

LOM Settings	LOM WebUI Page
All network link settings	Configuration > Network Link
Current time	Configuration > Time
All settings for SSL certificates	Configuration > SSL

Restore Factory Defaults

Use the **Restore Factory Defaults** window to reset the LOM settings to the factory defaults. It does **not** restore the factory default firmware version.

To restore factory default settings:

1. Select **Maintenance > Restore Factory Defaults**.

   The **Restore Factory Defaults** window opens.
2. **Optional:** Click **Enter Preserve Configuration** to save one or more of the LOM settings ("Preserve Configuration" on page 37).
3. Click **Restore Factory Defaults**.
4. Click **OK**.

System Administrator

Use the **System Administrator** window to configure the setting for the LOM system administrator account. This is the only account that can log in to the LOM console port. You cannot change the **sysadmin** user name for the system administrator account.

Note - The **sysadmin** account can only log in to the Console port on the appliance. It cannot use the WebUI to configure LOM. By default, the LOM WebUI is disabled.

To configure the system administrator account:

1. Select **Maintenance > System Administrator**.
   The **System Administrator** window opens.
2. Configure if the system administrator account is active:
   - Select **Enable** to activate the account
   - Clear **Enable** to deactivate the account
3. **Optional:** Change the password for the system administrator account.
   a) Select **Change Password**.
   b) Enter and then confirm the password.
4. Click **Save**.