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.

Latest Version of this Document
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format http://downloads.checkpoint.com/dc/download.htm?ID=32414

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 December 2020</td>
<td>Removed the Configuring the RADIUS Server Using Cisco ACS section due to end of support</td>
</tr>
<tr>
<td>06 December 2020</td>
<td>Updated Users and Privileges (on page 16)</td>
</tr>
<tr>
<td>18 May 2020</td>
<td>Updated for 7000 and 28000 Appliances</td>
</tr>
<tr>
<td>30 December 2019</td>
<td>Updated for 6000, 16000, and 26000 Appliances and Firmware Update (on page 34)</td>
</tr>
<tr>
<td>26 November 2017</td>
<td>Fixed Firmware Update for 21000 Series Appliances (on page 34)</td>
</tr>
<tr>
<td>6 July 2016</td>
<td>Updated for 5000,15000, and 23000 Appliances</td>
</tr>
<tr>
<td>18 November 2014</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Using Lights Out Management WebUI</td>
<td>6</td>
</tr>
<tr>
<td> Introduction</td>
<td>6</td>
</tr>
<tr>
<td> WebUI Requirements</td>
<td>7</td>
</tr>
<tr>
<td> Logging In to the WebUI</td>
<td>8</td>
</tr>
<tr>
<td> LOM First Time Wizard</td>
<td>9</td>
</tr>
<tr>
<td> WebUI Dashboard</td>
<td>10</td>
</tr>
<tr>
<td>Showing Hardware Information</td>
<td>11</td>
</tr>
<tr>
<td>Monitoring Appliance Health</td>
<td>13</td>
</tr>
<tr>
<td> Monitoring Appliance Health</td>
<td>13</td>
</tr>
<tr>
<td> Event Log</td>
<td>14</td>
</tr>
<tr>
<td>Configuring Settings</td>
<td>15</td>
</tr>
<tr>
<td> Users Settings</td>
<td>15</td>
</tr>
<tr>
<td> Configuring Users</td>
<td>15</td>
</tr>
<tr>
<td> Users and Privileges</td>
<td>16</td>
</tr>
<tr>
<td> Deleting Users</td>
<td>17</td>
</tr>
<tr>
<td> Login Block Settings</td>
<td>17</td>
</tr>
<tr>
<td> RADIUS Settings</td>
<td>18</td>
</tr>
<tr>
<td> Configuring RADIUS in LOM</td>
<td>18</td>
</tr>
<tr>
<td> Configuring FreeRADIUS and Other RADIUS Servers</td>
<td>19</td>
</tr>
<tr>
<td> LDAP and eDirectory Settings</td>
<td>19</td>
</tr>
<tr>
<td> Configuring an LDAP Server</td>
<td>20</td>
</tr>
<tr>
<td> Adding or Modifying an LDAP Group</td>
<td>22</td>
</tr>
<tr>
<td> Deleting an LDAP Group</td>
<td>23</td>
</tr>
<tr>
<td> DNS Server Settings</td>
<td>23</td>
</tr>
<tr>
<td> Network Settings</td>
<td>24</td>
</tr>
<tr>
<td> Network Link Configuration</td>
<td>24</td>
</tr>
<tr>
<td> NTP Settings</td>
<td>25</td>
</tr>
<tr>
<td> Services Settings</td>
<td>25</td>
</tr>
<tr>
<td> SSL Settings</td>
<td>26</td>
</tr>
<tr>
<td> Generating a Self Signed SSL Certificate from the WebUI</td>
<td>26</td>
</tr>
<tr>
<td> Generating a Self Signed SSL Certificate from Clish</td>
<td>27</td>
</tr>
<tr>
<td> Generating a CA Signed SSL Certificate from the Security Management Server</td>
<td>28</td>
</tr>
<tr>
<td> Uploading an SSL Certificate to LOM</td>
<td>28</td>
</tr>
<tr>
<td>Controlling the Appliance</td>
<td>29</td>
</tr>
<tr>
<td> Console Redirection</td>
<td>29</td>
</tr>
<tr>
<td> Launching the JViewer Client</td>
<td>29</td>
</tr>
<tr>
<td> Launching the Virtual Media Client</td>
<td>31</td>
</tr>
<tr>
<td> Installing an ISO Image on the Appliance</td>
<td>32</td>
</tr>
<tr>
<td> Power Control and Status</td>
<td>33</td>
</tr>
<tr>
<td>Managing the LOM Firmware</td>
<td>34</td>
</tr>
<tr>
<td> Showing the Firmware Version</td>
<td>34</td>
</tr>
<tr>
<td> Firmware Update</td>
<td>34</td>
</tr>
<tr>
<td> Preserve Configuration</td>
<td>35</td>
</tr>
<tr>
<td> Restore Factory Defaults</td>
<td>37</td>
</tr>
</tbody>
</table>
Using Lights Out Management WebUI

In This Section:

Introduction .....................................................................................................................6
WebUI Requirements .....................................................................................................7
Logging In to the WebUI .................................................................................................8
LOM First Time Wizard ...................................................................................................9
WebUI Dashboard .........................................................................................................10
Showing Hardware Information ...................................................................................11

Introduction

This document applies to these appliances:

- Smart-1 225/3050/3150
- 5000 Appliances
- 6000 Appliances
- 7000 Appliances
- 13000 Appliances
- 15000 Appliances
- 16000 Appliances
- 21000 Appliances
- 23000 Appliances
- 26000 Appliances
- 28000 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.

Note:

- 6000, 7000, 16000, 26000, and 28000 appliances follow the same rules as 5000, 13000 and 23000 appliances.
- The 16000, 26000, and 28000 LOM have a different form factor than other appliances so they are not interchangeable.
### LOM port

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Link on Smart-1, 13000, and 21000 series appliances</td>
</tr>
<tr>
<td></td>
<td>• OFF - No Link</td>
</tr>
<tr>
<td></td>
<td>• ON (Amber) - Link is established</td>
</tr>
<tr>
<td></td>
<td>• Blink (Amber) - Link is active</td>
</tr>
<tr>
<td></td>
<td>Link on 5000, 6000, 7000, 15000, 16000, 23000, 26000, and 28000 series appliances</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 on Smart-1, 5000, 6000, 7000, 13000, 15000, 16000, 23000, 26000, and 28000 series appliances</td>
</tr>
<tr>
<td></td>
<td>• OFF - 10 Mbps data rate is used</td>
</tr>
<tr>
<td></td>
<td>• ON (Green) - 100 Mbps data rate used</td>
</tr>
<tr>
<td></td>
<td>• ON (Amber) - 1 Gbps data rate is used</td>
</tr>
<tr>
<td></td>
<td>Activity/Speed on 21000 series appliances</td>
</tr>
<tr>
<td></td>
<td>• OFF - 10 Mbps data rate is used</td>
</tr>
<tr>
<td></td>
<td>• ON (Green) - 1 Gbps data rate is used</td>
</tr>
<tr>
<td></td>
<td>• ON (Amber) - 100 Mbps data rate is used</td>
</tr>
</tbody>
</table>

### WebUI Requirements

- A supported web browser
- Java™ software installed on the local computer (minimum version 6.20)

These web browsers are supported:

- Microsoft Internet Explorer
- Microsoft Edge
- 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 (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:
   - 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.
   - The password requirements:
     - 8 - 16 characters
     - Do not include the username
     - No spaces
     - Must contain characters from three of these four categories: English uppercase characters (A through Z), English lowercase characters (a through z), base 10 digits (0 through 9), and non-alphanumeric characters (~!@#$%^&*).
8. Click Login.
   - The First Time Wizard window opens when you change the password for the first time.
   - The Dashboard window opens afterward.
LOM First Time Wizard

The First Time Wizard appears in the Welcome screen.

1. Click Next.

2. On the Configure Network screen:
   a) Set a Host Name for the appliance’s LOM.
   b) Choose the IP source as DHCP or a static IP setting.
      
      Note – If you choose a static IP setting, you may enter the desired LOM IP address, its NetMask, default Gateway address and DNS Server. The default Gateway and DNS Server values are optional.
   c) Click Next.

3. On the Configure Service screen, choose access permissions for the KVM and Virtual Media services from these options:
   a) Only to subnet – Grants access to IP addresses that are part of the subnet[s] to access the service.
   b) To all – Grants access to all IP addresses.
   c) Disabled – Does not grant access to any IP address.
Click **Next**.

4. In the last page, wait for the enabled **Finish** button. Click **Finish**.

**Note:**
- The LOM device will restart and apply the new settings from this wizard. Go to the new IP address to access the LOM WebUI.
- The Web-UI requires another user login to bring the user to the Dashboard page.

**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

![Lights Out Management WebUI](image)

**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
- Manufacturer name

Each component installed in the machine shows another node with this information:

- Part number
- Serial number
- Version (revision)

**To show the hardware information:**

From the menu bar, click **Hardware Inventory**.
**Note** - This example is a 21700. Different platforms may show less information.
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 substantially below the operational range. The system will fail.
  Recommendation: Contact Check Point support.

- **LC - Lower Critical** - The sensor reading is below its minimum threshold. 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 operational.
  Recommendation: Periodically monitor the system.

- **UNC - Normal (Upper Non-Critical)** - The sensor reading is at the upper end of the normal range. The system is operational.
  Recommendation: Periodically monitor the system.

- **UC - Upper Critical** - The sensor reading is above its maximum threshold. 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 above 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 type.
   The window shows the list of all sensors or the data for the selected sensor type. Click on a sensor from the list to see its specified values on the right hand side of the screen.

**Note** - See the note on the Retrieve Hardware Sensors button for information about when to read the hardware sensors through the LOM.

### 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.

Use these drop-down menus to 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

Select one of these 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 .......................................................... 15
- Login Block Settings.................................................. 17
- RADIUS Settings ....................................................... 18
- LDAP and eDirectory Settings ...................................... 19
- DNS Server Settings .................................................. 23
- Network Settings ....................................................... 24
- Network Link Configuration ........................................ 24
- NTP Settings ............................................................ 25
- Services Settings ....................................................... 25
- SSL Settings ............................................................. 26

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.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>User ID number</td>
</tr>
<tr>
<td>Username</td>
<td>Login name of the user</td>
</tr>
<tr>
<td>User Access</td>
<td>Shows if the user is Enabled to log in to LOM</td>
</tr>
<tr>
<td>Network Privilege</td>
<td>Assigned role of the user</td>
</tr>
</tbody>
</table>

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 not in use 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) Check the Change Password check box.
b) Enter a new password in the New Password field.

**Password Requirements** - 8-16 characters, do not include the username, no spaces, and must contain characters from these four categories: English uppercase characters (A through Z), English lowercase characters (a through z), base 10 digits (0 through 9), and non-alphanumeric characters (~!@#$%^&*).

c) Re-enter the password in the Confirm New Password field to confirm.

5. Click Add or Apply.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Login name of the user</td>
</tr>
<tr>
<td>Change Password</td>
<td>When clicked, you can change the password for a user</td>
</tr>
<tr>
<td>Password Size</td>
<td>Maximum length of the password (16 or 20 characters)</td>
</tr>
<tr>
<td>New Password</td>
<td>Enter a new password</td>
</tr>
<tr>
<td>Confirm New Password</td>
<td>Enter the new password again</td>
</tr>
<tr>
<td>User Access</td>
<td>Select Enable to let the user log in to the LOM</td>
</tr>
<tr>
<td>Network Privilege</td>
<td>Assigned role of the user</td>
</tr>
<tr>
<td>Skip Complex Password Rules</td>
<td>Select Enable to choose a simple password without the enforcement rules</td>
</tr>
</tbody>
</table>

**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.
  
  **Note** - The user cannot log in to LOM in this state.
- **Operator and User** - Cannot configure LOM settings.
  - **Operator** - Can view most configurations on LOM but cannot change them. Cannot launch JViewer console.
  - **User** - Can view basic information on LOM (hardware information and sensors) but cannot look at advanced configurations. Cannot launch JViewer console.

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

<table>
<thead>
<tr>
<th>Window</th>
<th>Operator Can View</th>
<th>User Can View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Yes</td>
<td>Yes (cannot see network settings)</td>
</tr>
<tr>
<td>Hardware Inventory</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Retrieve Hardware Sensors</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>LDAP</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Network</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Network Link</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Time</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### 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 user.

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable Login Block</td>
<td>When selected, enforces the login block policy according to its settings.</td>
</tr>
<tr>
<td>Max Login Attempt</td>
<td>Sets the maximum number of login failures from a user.</td>
</tr>
<tr>
<td>Login Block Timeout</td>
<td>Sets the number of minutes that a user is blocked from logging in to LOM.</td>
</tr>
</tbody>
</table>
### Configuring Settings

#### Management Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Contains a list of all users which can be managed to include or exclude users from the Login Block policy. Determine the users to include in the Login Block by enabling or disabling the user. Select from these options for each user:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong> - Enable the Login Block policy on the user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong> - Do not enforce the Login Block policy on the user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Blocked</strong> - Immediately enforce Login Block on the user for the timeout duration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ForeverBlocked</strong> - Immediately enforce Login Block on the user for an infinite duration.</td>
</tr>
</tbody>
</table>

#### 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.

Allows configurations for up to two RADIUS servers. The second serves as a backup if the first server fails.

### 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.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Authentication</td>
<td>When selected, enables RADIUS based authentication.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the RADIUS server (default 1812).</td>
</tr>
</tbody>
</table>
### Configuring FreeRADIUS and 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:

- Whether 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 Portal again.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP/E Directory Authentication</td>
<td>When selected, enables LDAP groups to log in to LOM.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>The default port is 389.</td>
</tr>
<tr>
<td>Bind DN</td>
<td>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: <em>cn=manager,ou=login,dc=domain,dc=com</em></td>
</tr>
<tr>
<td>Password</td>
<td>Password for the binding user.</td>
</tr>
</tbody>
</table>
| 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. |
### Field Name | Description
--- | ---
**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**.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Role Group Name</strong></td>
<td>Name for the group. Cannot contain blank spaces.</td>
</tr>
<tr>
<td><strong>Role Group Search Base</strong></td>
<td>Define the node for the search in the directory tree. You can specify to start the query from an OU, or the root. Sample for the <strong>Search Base</strong> query:</td>
</tr>
<tr>
<td><strong>Role Group Privilege</strong></td>
<td>Select the LOM privilege (on page 16) that is assigned to the users in this group.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Host Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Settings</td>
</tr>
<tr>
<td>• Automatic - The DHCP server gives the DNS host name</td>
</tr>
<tr>
<td>• Manual - Enter the Host Name in the field</td>
</tr>
<tr>
<td>Host Name</td>
</tr>
<tr>
<td>Host name of the appliance</td>
</tr>
<tr>
<td>Domain Name Configuration</td>
</tr>
<tr>
<td>Domain Settings</td>
</tr>
<tr>
<td>• Automatic - The DHCP server gives the DNS domain name</td>
</tr>
<tr>
<td>• Manual - Enter the host name in the field</td>
</tr>
<tr>
<td>Note - Not used in newer LOM F/W versions</td>
</tr>
<tr>
<td>Domain Name</td>
</tr>
<tr>
<td>Domain name for LOM</td>
</tr>
<tr>
<td>IPv4 Domain Name Server Configuration</td>
</tr>
<tr>
<td>DNS Server Settings</td>
</tr>
<tr>
<td>• Automatic - The DHCP server gives the IPv4 DNS server address</td>
</tr>
<tr>
<td>• Manual - Enter the IPv4 DNS server address in the field</td>
</tr>
<tr>
<td>Note - Not used in newer LOM F/W versions</td>
</tr>
<tr>
<td>Preferred DNS Server</td>
</tr>
<tr>
<td>The IPv4 address of the primary DNS server</td>
</tr>
<tr>
<td>Note - Enter 0.0.0.0 to clear an IPv4 field. You cannot use empty strings for IPv4 addresses</td>
</tr>
<tr>
<td>Alternate DNS Server</td>
</tr>
<tr>
<td>The IPv4 address of the secondary DNS server</td>
</tr>
</tbody>
</table>
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**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN Interface</strong></td>
<td>Shows the interface that is used to connect to LOM.</td>
</tr>
<tr>
<td><strong>LAN Settings</strong></td>
<td>Enables the LOM interface.</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>Shows the MAC address of the LOM interface.</td>
</tr>
<tr>
<td><strong>IPv4 Configuration</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **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     |

**Note** - Using DHCP or entering a different IP address manually may cause the loss of connectivity with the LOM WebUI.

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**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **LAN Interface** | Shows the interface that is used to connect to LOM.  
                      **Note** - This field does not exist in newer LOM F/W versions. |
### 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, 6000, 7000, 13000, 15000, 16000, 23000, 26000, 28000, 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.

**To update the date and time manually:**

1. Select **Configuration > Time**.
   
   The **Time Settings** window opens where you can configure the date and time manually.

2. In the **Date** drop-down lists, change the **month**, **day** and **year** of the date.

3. In the **Time** drop-down lists, change the **hours**, **minutes** and **seconds** of the time.

4. In the **Timezone** drop-down list, select the correct **time zone**.

5. Click **Save**.

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 (on page 35) 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 IP address 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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Read-only field that shows the name of the service.</td>
</tr>
<tr>
<td>Current State</td>
<td>Select <strong>Active</strong> to enable the service.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select an interface for the service. <strong>LOM</strong> is the LOM port on the appliance. Note - This is now read-only and can not be configured in any service.</td>
</tr>
<tr>
<td>Nonsecure Port</td>
<td>Port that the service uses for unencrypted traffic.</td>
</tr>
<tr>
<td>Secure Port</td>
<td>Port that the service uses for encrypted traffic.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Duration, in seconds, of service inactivity, after which the session closes (for Web service only). This can only be set between 300 and 1800.</td>
</tr>
</tbody>
</table>

**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 (on page 28).

**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 or 2048 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 (on page 28).

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

Run this command in expert mode:

```bash
copenssl 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-nodes</td>
<td>Do not encrypt the output key.</td>
</tr>
<tr>
<td>-days &lt;num_days&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>-x509</td>
<td>Output a x509 structure instead of a cert. req.</td>
</tr>
<tr>
<td>-newkey rsa:&lt;size_bits&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>-keyout &lt;key_file&gt;</td>
<td>Save the key in a specified .pem file. LOM accepts only .pem key file format.</td>
</tr>
<tr>
<td>-out &lt;output_file&gt;</td>
<td>Save the certificate in a specified .pem file. LOM accepts only .pem certificate file format.</td>
</tr>
</tbody>
</table>

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:**
copenssl 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:

copenssl 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 **copenssl** command above.

**Generating a CA Signed SSL Certificate from the Security Management Server**

After you create the certificate you must upload the certificate manually (on page 28).

**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)

**For Example:**
cpca_client create_cert -n "CN=FF:FF:FF:FF:FF:FF" -f cert.p12 -w "" -k USER

copenssl pkcs12 -in cert.p12 -nokeys -clcerts -passin pass: -out cert.pem
copenssl 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 .....................................................................................................29
Power Control and Status ............................................................................................33

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.

Note - Unlike the serial console port of the appliance, the console viewed from the JViewer client shows as a VGA connection. The output may look different as the machine boots.

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. Make sure that JAVA security configurations allows connectivity between the LOM IP address and the computer.
   The Console Redirection window opens.
4. Click Java Console.
   The jviewer.jnlp file is downloaded.
   Note - The file might appear as a potential issue as a JAVA applet. If prompted, click “Keep file” (in Chrome) to download the file and save it on your PC.
   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.
5. To use an on-screen keyboard, select **Keyboard Layout > SoftKeyboard > <language>**. The keyboard opens in a new window.

   **Note** - The keyboard layout mapping derives from the language settings in the OS system in your computer. Using a different language on the keyboard may result in key-presses to behave differently than expected.

6. 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.

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

### Keyboard

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

Menu Option | Description
---|---
Hold <ALT or CTRL> key | Holds the chosen key down until released by unselecting the option.
<Left or Right> Windows Key | Holds the left or right Windows key down until released. Alternately, allows for quick press and release.
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.
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. The power switch can only be set to On on older appliances. Newer appliances can never “set” their switch to On. The switch flicks and goes back to its initial position. When you flick the switch, the appliance turns On or Off based on the appliance’s state.

To configure the Power Control settings:

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Appliance</td>
<td>Restarts the appliance (warm boot)</td>
</tr>
<tr>
<td>Power Off Appliance-Immediate</td>
<td>Turns the appliance off without shutting down the operating system</td>
</tr>
<tr>
<td>Power Off Appliance - Orderly Shutdown</td>
<td>Shuts down the operating system and then turns off the appliance</td>
</tr>
<tr>
<td>Power On Appliance</td>
<td>Turns on the appliance when it is Off.</td>
</tr>
<tr>
<td>Power Cycle Appliance</td>
<td>Shuts down the appliance and then turns it on (cold boot).</td>
</tr>
</tbody>
</table>
Managing the LOM Firmware

In This Section:

- Showing the Firmware Version ................................................................. 34
- Firmware Update ......................................................................................... 34
- Preserve Configuration .............................................................................. 35
- Restore Factory Defaults ......................................................................... 37
- System Administrator ............................................................................. 37

Showing the Firmware Version

Before and after updating firmware, use the WebUI to look at the installed firmware version. The appliance’s CLI can also do this by running the show lom command.

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 (on page 35)
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**.

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

These settings are always saved when you upgrade the firmware.

<table>
<thead>
<tr>
<th>LOM Settings</th>
<th>LOM Portal Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>All settings for SSL certificates</td>
<td>Configuration &gt; SSL</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>LOM Settings</th>
<th>LOM Portal Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>All network link settings</td>
<td>Configuration &gt; Network Link</td>
</tr>
<tr>
<td>Current time</td>
<td>Configuration &gt; Time</td>
</tr>
<tr>
<td>All settings for SSL certificates</td>
<td>Configuration &gt; SSL</td>
</tr>
</tbody>
</table>

Managing the LOM Firmware
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 (on page 35).
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 LOM Console port on the appliance. It cannot use the Portal to configure LOM. By default, the LOM Portal 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.