Troubleshoot Issues with Lights-Out Management (LOM) on FireSIGHT Systems

Contents

Introduction

This document provides various symptoms and error messages that might appear when you configure Lights-Out-Management (LOM), and how to troubleshoot them step by step. LOM allows you to use an out-of-band Serial over LAN (SOL) management connection in order to remotely monitor or manage appliances without logging into the web interface of the appliance. You can perform limited tasks, such as view the chassis serial number or monitor such conditions as fan speed and temperature.

Prerequisites

Requirements

Cisco recommends that you have knowledge of FireSIGHT System and LOM.

Components Used

The information in this document is based on these hardware and software versions:

- FireSIGHT Management Center
- FirePOWER 7000 Series Appliances, 8000 Series Appliances
- Software Version 5.2 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Unable to Connect to LOM

You might be unable to connect to a FireSIGHT Management Center or FirePOWER Appliance with LOM. The connection requests might fail with these error messages:

```
Error: Unable to establish IPMI v2 / RMCP+ session Error

Info: cannot activate SOL payload with encryption
```

The next section describes how to verify a LOM configuration and connections to the LOM interface.

Verify Configuration

Step 1: Verify and confirm that LOM is enabled and uses a different IP address than the management interface.

Step 2: Verify with the Network team that UDP port 623 is open bidirectionally, and that the routes are configured correctly. Since LOM works over a UDP port, you cannot Telnet to the LOM IP address over port 623. However, an an alternate solution is to test if the device speaks IPMI with the IPMIPING utility. IPMIPING sends two IPMI Get Channel Authentication Capabilities calls via a Get Channel Authentication Capabilities request datagram on UDP port 623 (two requests since it uses UDP and connections are not guaranteed.)

> **Note**: For a more extensive test to confirm if the device listens on UDP port 623, use NMAP scan.

Step 3: Can you ping the IP address of LOM? If not, run this command as `root` user on the applicable appliance, and verify the settings are correct. For example,

```
ipmitool lan print

Set in Progress         : Set Complete
Auth Type Support       : NONE MD5 PASSWORD
Auth Type Enable        : Callback : NONE MD5 PASSWORD
                        : User     : NONE MD5 PASSWORD
                        : Operator : NONE MD5 PASSWORD
                        : Admin    : NONE MD5 PASSWORD
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 192.0.2.2
Subnet Mask             : 255.255.255.0
MAC Address             : 00:1e:67:0a:24:32
SNMP Community String   : INTEL
IP Header               : TTL=0x00 Flags=0x00 Precedence=0x00 TOS=0x00
BMC ARP Control         : ARP Responses Enabled, Gratuitous ARP Disabled
Gratituous ARP Intrvl   : 0.0 seconds
Default Gateway IP      : 192.0.2.1
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 1,2,3,6,7,8,11,12,0
Cipher Suite Priv Max   : XaaaXXaaaXXaaXX
                        :     X=Cipher Suite Unused
                        :     c=CALLBACK
                        :     u=USER
                        :     o=OPERATOR
                        :     a=ADMIN
                        :     O=OEM
```

Verify the Connection

Step 1: Can you connect using this command?

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx  -U admin sdr
```

Do you receive this error message?

```
Error: Unable to establish IPMI v2 / RMCP+ session
```

> **Note**: A connection to the correct IP address, but with the wrong credentials, fails with the previous error immediately. Attempts to connect to LOM at an invalid IP address time out after about 10 seconds and returns this error.

Step 2: Try to connect with this command:

```
ipmitool -I lanplus  -H xxx.xxx.xxx.xxx  -U admin sdr
```

Step 3: Do you get this error?

```
Info: cannot activate SOL payload with encryption
```

Now try to connect with this command (this specifies the cipher suite to use):

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

Step 4: Still cannot connect? Try to connect with this command:

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

In the verbose output do you see this error?

```
RAKP 2 HMAC is invalid
```

Step 5: Change the Admin password via the GUI, and try again.

Still cannot connect? Try to connect with this command:

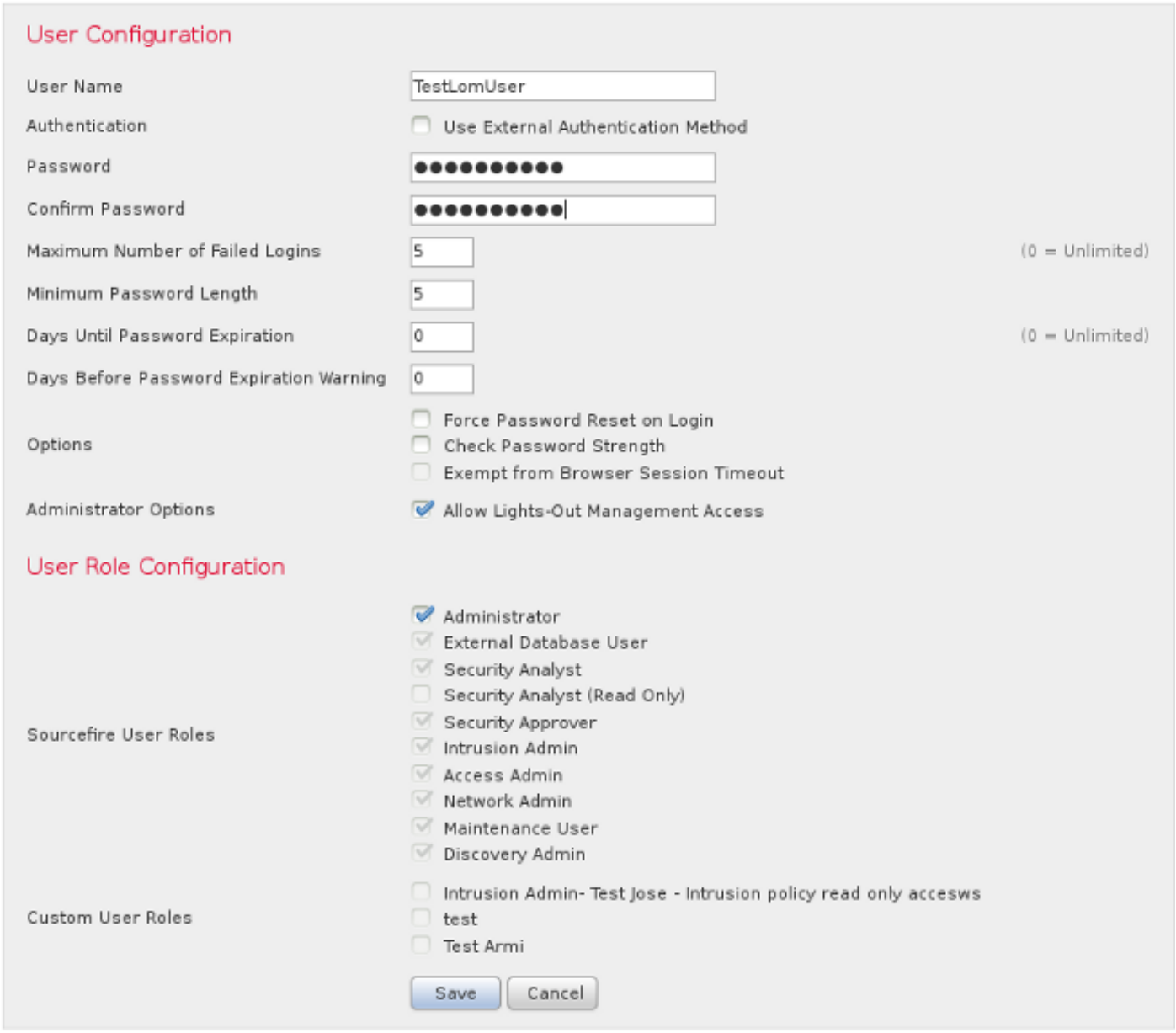
```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

In the verbose output do you see this error?

```
RAKP 2 message indicates an error : unauthorized name
```

Step 6: Choose **User > Local Configuration > User Management**

- Create a new `TestLomUser`
- Check the **User role configuration** to **Administrator**
- Check **Allow Lights-out Management Access**



On the CLI of the applicable appliance, escalate your privileges to root and run these commands. Verify that `TestLomUser` is the user on the third line.

```
ipmitool user list 1

ID  Name         Callin  Link Auth    IPMI Msg   Channel Priv Limit
1                    false   false      true       ADMINISTRATOR
2   root             false   false      true       ADMINISTRATOR
3   TestLomUser      true    true       true       ADMINISTRATOR
```

Change the user on line three to `admin`.

```
ipmitool user set name 3 admin
```

Set an appropriate access level:

```
ipmitool channel setaccess 1 3 callin=on link=on ipmi=on privilege=4
```

Change the password of the new `admin` user

```
ipmitool user set password 3
```

Verify that the settings are correct.

```
ipmitool user list 1
```

```
ID  Name         Callin  Link Auth    IPMI Msg   Channel Priv Limit
1                    false   false      true       ADMINISTRATOR
2   root             false   false      true       ADMINISTRATOR
3   admin            true    true       true       ADMINISTRATOR
```

Make sure that SOL is enabled for the correct channel(1) and user(3).

```
ipmitool sol payload enable 1 3
```

Step 7: Ensure that the IPMI process is not in a bad state.

```
pmtool status | grep -i sfipmid
sfipmid (normal) - Running 2928 Command: /usr/local/sf/bin/sfipmid -t 180 -p power PID File:
/var/sf/run/sfipmid.pid Enable File: /etc/sf/sfipmid.run
```

Restart the service.

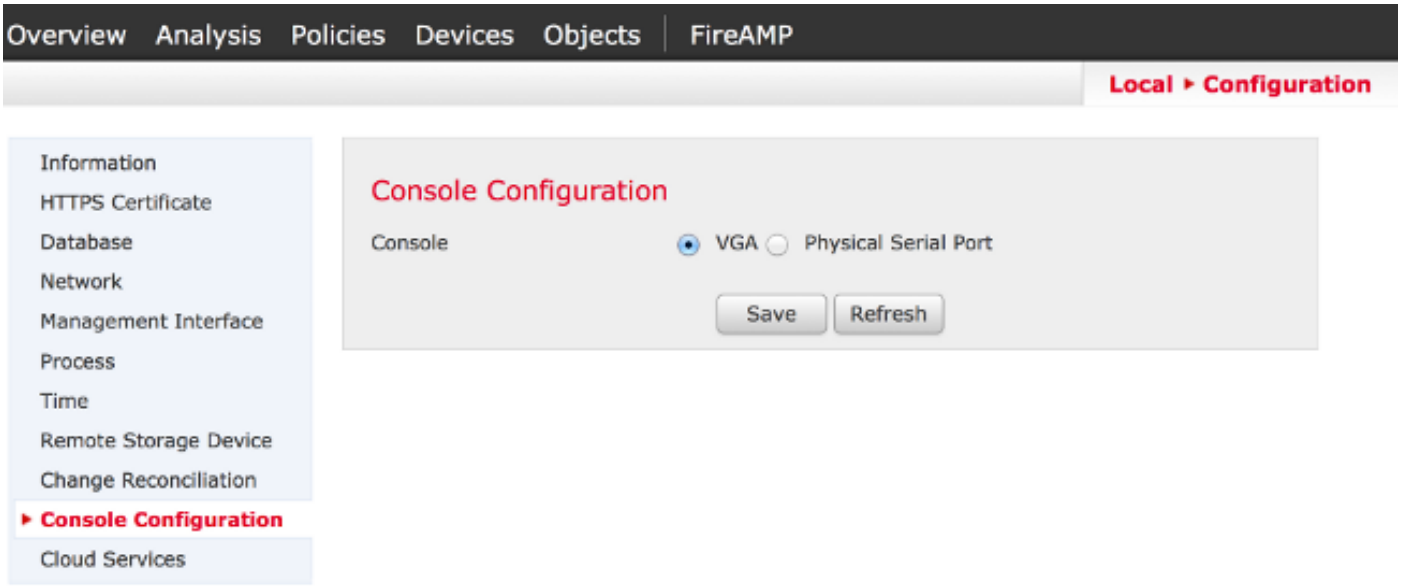
```
pmtool restartbyid sfipmid
```

Confirm that the PID has changed.

```
pmtool status | grep -i sfipmid
```

```
sfipmid (normal) - Running 20590
Command: /usr/local/sf/bin/sfipmid -t 180 -p power
PID File: /var/sf/run/sfipmid.pid
Enable File: /etc/sf/sfipmid.run
```

Step 8: Disable the LOM in the GUI, then reboot the appliance. In the appliance's GUI, choose **Local > Configuration > Console Configuration**. Select **VGA**, click **Save**, and click **OK** in order to reboot.



Afterwards, enable the LOM in the GUI, then reboot the appliance. In the appliance's GUI, choose

Local > Configuration > Console Configuration. Choose **Physical Serial Port** or LOM, click **Save**, and click **OK** to reboot.

Now, try to connect again.

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

Step 9: Shut down the device and complete a power cycle, that is, physically remove the power cable for one minute, plug it back, and then power on. After the appliance powers up fully run this command:

```
ipmitool -I lanplus -vvv -H xxx.xxx.xxx.xxx -C 3 -U admin sdr
```

Step 10: Run this command from the appliance in question. This specifically does a cold reset of the bmc:

```
ipmitool bmc reset cold
```

Step 11: Run this command from a system on the same local network as the device (that is, does not pass through any intermediate router):

```
ipmitool -I lanplus -H xxx.xxx.xxx.xxx -U admin power status
```

```
arp -an > /var/tmp/arpcache
```

Send Cisco Technical Support the resulting `/var/tmp/arpcache` file in order to determine if the BMC responds to an ARP request.

Connection to LOM Interface is Disconnected During Reboot

When you reboot a FireSIGHT Management Center or a FirePOWER Appliance, the connection to the appliance might be lost. The output when rebooting the appliance via the CLI is shown here:

```
admin@FireSIGHT:~$ sudo shutdown -r now

Broadcast message from root (ttyS0) (Tue Nov 19 19:40:30  Stopping Sourcefire 3D
Sensor 7120...nfemsg: Host ID 1 on card 0 endpoint 1 de-registering ... nfemsg: Host ID 2 on
card 0 endpoint 1 de-registering ... nfemsg: Host ID 27 on card 0 endpoint 1 de-registering
......ok Stopping Netronome Flow Manager: nfemsg: Fail callback unregistered Unregistered NFM
fail hook handler nfemsg: Card 0 Endpoint #1 messaging disabled nfemsg: Module EXIT WARNING:
Deprecanfp nfp.0: [ME] CSR access problem for ME 25 ted config file nfp nfp.0: [vPCI] Removed
virtual device 01:00.4 /etc/modprobe.conf, all config files belong into /etc/modprobe.d/.
success. No NMSB present: logging unecessary...[-10G[ OK ].. Turning off swapfile
/Volume/.swaptwo
[-10G[ OK ] other currently mounted file systems...
Unmounting fuse control filesystem.
Un
```

The highlighted output **`Unmounting fuse control filesystem. Un`** shows that the connection to the appliance is interrupted due to Spanning Tree Protocol (STP) being enabled on the switch where the FireSIGHT System is connected to. Once the managed devices reboots, this error is displayed:

```
Error sending SOL data; FAIL
```

```
SOL session closed by BMC
```

Note: Before you can connect to an appliance with LOM/SOL, you must disable Spanning Tree Protocol (STP) on any third-party switching equipment connected to the device's management interface.

A LOM connection of FireSIGHT System is shared with the management port. The link for the management port drops for a very brief time during reboot. Since the link is going down and coming back up, this could trigger a delay in the switch port (typically 30 seconds before it starts passing traffic) due to the listening or learning switch port state caused by having STP configured on the port.