

# 排除FireSIGHT系統上的無人值守管理(LOM)問題

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[無法連線到LOM](#)

[驗證設定](#)

[驗證連線](#)

[在重新啟動期間，與LOM介面的連線斷開](#)

## 簡介

本文提供在配置無人值守管理(LOM)時可能出現的各種症狀和錯誤消息，以及如何逐步對其進行故障排除。LOM允許您使用帶外Serial over LAN(SOL)管理連線，以便在不登入到裝置的Web介面的情況下遠端監控或管理裝置。您可以執行有限的任務，如檢視機箱序列號或監控風扇速度和溫度等情況。

## 必要條件

### 需求

思科建議您瞭解FireSIGHT系統和LOM。

### 採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- FireSIGHT管理中心
- FirePOWER 7000系列裝置、8000系列裝置
- 軟體版本5.2或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 無法連線到LOM

您可能無法使用LOM連線到FireSIGHT管理中心或FirePOWER裝置。連線請求可能會失敗，並顯示以下錯誤消息：

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

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

下一節介紹如何驗證LOM配置以及與LOM介面的連線。

## 驗證設定

第1步：驗證並確認LOM是否已啟用，並且使用與管理介面不同的IP地址。

第2步：向網路團隊確認UDP埠623是雙向開啟的，並且路由配置正確。由於LOM通過UDP埠工作，您無法通過623埠Telnet至LOM IP地址。但是，另一種解決方案是使用IPMIPING實用程式測試裝置是否發出IPMI訊號。IPMIPING通過UDP埠623上的Get Channel Authentication Capabilities請求資料包傳送兩個IPMI Get Channel Authentication Capabilities呼叫（兩個請求，因為它使用UDP，並且不保證連線。）

**附註：**若要進行更廣泛的測試以確認裝置是否在UDP埠623上偵聽，請使用NMAP掃描。

步驟3:是否能ping通LOM的IP地址？如果不是，請在適用的裝置上以root使用者身份運行此命令，並驗證設定是否正確。例如，

```
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
Gratuitous 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
```

## 驗證連線

第1步：是否可使用此命令連線？

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

您是否收到此錯誤消息？

Error: Unable to establish IPMI v2 / RMCP+ session

**附註：**如果連線到正確的IP地址，但憑證錯誤，則立即失敗，並出現上一個錯誤。嘗試在無效IP地址超時時連線到LOM大約需要10秒，然後返回此錯誤。

第2步：嘗試使用以下命令進行連線：

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

步驟3:是否收到此錯誤？

Info: cannot activate SOL payload with encryption

現在嘗試使用以下命令進行連線（這將指定要使用的密碼套件）：

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

第4步：仍然無法連線？嘗試使用以下命令進行連線：

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

在詳細輸出中是否看到此錯誤？

RAKP 2 HMAC is invalid

第5步：通過GUI更改管理員密碼，然後重試。

仍然無法連線？嘗試使用以下命令進行連線：

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

在詳細輸出中是否看到此錯誤？

RAKP 2 message indicates an error : unauthorized name

第6步：選擇**User > Local Configuration > User Management**

- 建立新的TestLomUser
- 將使用者角色**配置檢查**給管理員
- 選中**Allow Lights-out Management Access**

### User Configuration

User Name:

Authentication:  Use External Authentication Method

Password:

Confirm Password:

Maximum Number of Failed Logins:  (0 = Unlimited)

Minimum Password Length:

Days Until Password Expiration:  (0 = Unlimited)

Days Before Password Expiration Warning:

Options:  Force Password Reset on Login  
 Check Password Strength  
 Exempt from Browser Session Timeout

Administrator Options:  Allow Lights-Out Management Access

### User Role Configuration

Sourcefire User Roles:  Administrator  
 External Database User  
 Security Analyst  
 Security Analyst (Read Only)  
 Security Approver  
 Intrusion Admin  
 Access Admin  
 Network Admin  
 Maintenance User  
 Discovery Admin

Custom User Roles:  Intrusion Admin- Test Jose - Intrusion policy read only accesws  
 test  
 Test Armi

在適用裝置的CLI上，將您的許可權提升到root使用者並運行這些命令。驗證TestLomUser是否為第三行上的使用者。

```
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
```

將第三行的使用者更改為admin。

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

設定適當的訪問級別：

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

更改新admin使用者的密碼

```
ipmitool user set password 3
```

驗證設定是否正確。

```
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

確保為正確的通道(1)和使用者(3)啟用SOL。

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

第7步：確保IPMI進程未處於錯誤狀態。

```
pmttool 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
```

重新啟動服務。

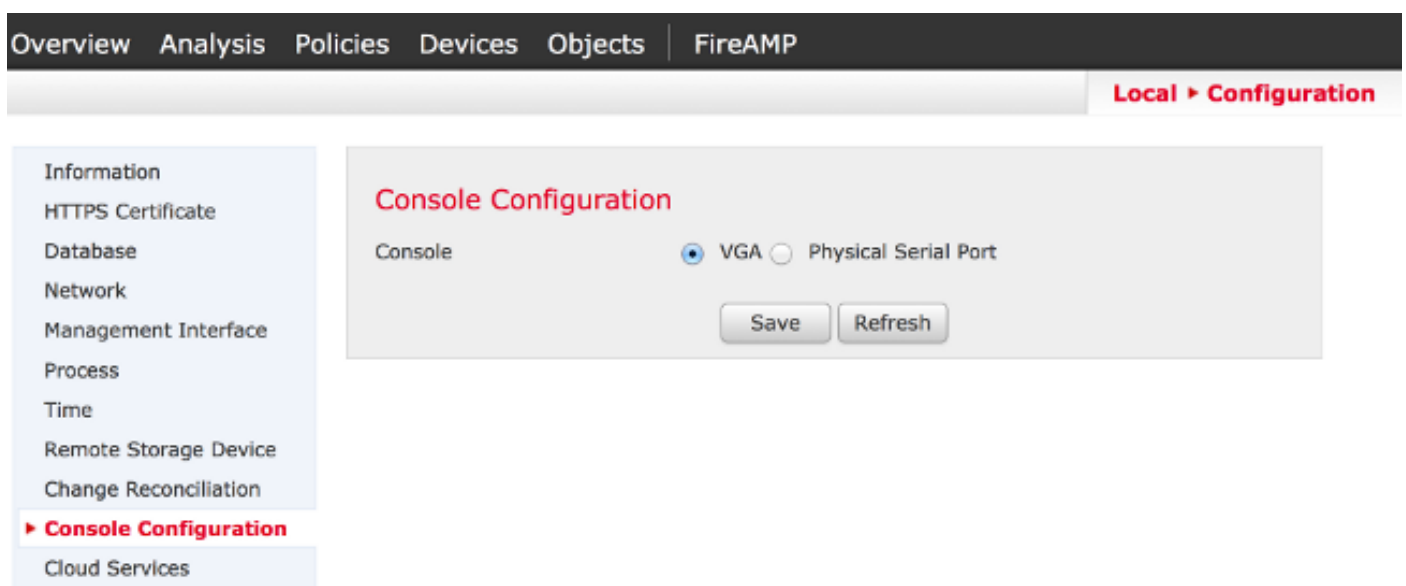
```
pmttool restartbyid sfipmid
```

確認PID已更改。

```
pmttool 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
```

第8步：在GUI中禁用LOM，然後重新啟動裝置。在裝置的GUI中，選擇Local > Configuration > Console Configuration。選擇VGA，按一下Save，然後按一下OK以重新啟動。



Overview Analysis Policies Devices Objects FireAMP

Local > Configuration

Information  
HTTPS Certificate  
Database  
Network  
Management Interface  
Process  
Time  
Remote Storage Device  
Change Reconciliation  
▶ Console Configuration  
Cloud Services

Console Configuration

Console  VGA  Physical Serial Port

Save Refresh

然後，在GUI中啟用LOM，然後重新啟動裝置。在裝置的GUI中，選擇Local > Configuration > Console Configuration。選擇Physical Serial Port或LOM，按一下Save，然後按一下OK重新啟動

。

現在，再次嘗試連線。

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

第9步：關閉裝置並完成電源循環，即物理拔下電源線一分鐘，插回電源線，然後開啟電源。在裝置電源完全開啟後，請運行以下命令：

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

步驟10:從相關裝置運行此命令。這專門對bmc執行冷重置：

```
ipmitool bmc reset cold
```

步驟11:從與裝置位於同一本地網路上的系統運行此命令（即不通過任何中間路由器）：

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

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

將/var/tmp/arpcache結果檔案傳送給思科技術支援，以確定BMC是否響應ARP請求。

## 在重新啟動期間，與LOM介面的連線斷開

重新啟動FireSIGHT管理中心或FirePOWER裝置時，與裝置的連線可能會丟失。通過CLI重新啟動裝置時的輸出如下所示：

```
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 unnecessary...[-10G[ OK ].. Turning off swapfile
/Volume/.swaptwo
[-10G[ OK ] other currently mounted file systems...
Unmounting fuse control filesystem.
Un
```

突出顯示的輸出**Unmounting fuse control filesystem**。未顯示由於與FireSIGHT系統連線的交換機上啟用了生成樹協定(STP)，與裝置的連線中斷。受管裝置重新啟動後，將顯示以下錯誤：

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

```
SOL session closed by BMC
```

**附註：**要使用LOM/SOL連線到裝置，必須在連線到裝置管理介面的所有第三方交換裝置上禁用生成樹協定(STP)。

FireSIGHT系統的LOM連線與管理埠共用。管理連線埠的連結會在重新開機期間短暫捨棄。由於鏈路正在關閉並正在恢復，這可能觸發交換機埠延遲（通常在開始傳輸流量之前為30秒），原因是在

埠上配置STP而導致交換機埠處於偵聽或學習狀態。